C. Alcaraz, and J. Lopez, "Wide-Area Situational Awareness for Critical Infrastructure Protection", *IEEE Computer*, vol. 46, pp. 30-37, 2013.
http://doi.org/10.1109/MC.2013.72
NICS Lab. Publications: https://www.nics.uma.es/publications

Wide-Area Situational Awareness for Critical Infrastructure Protection

Cristina Alcaraz, *Member IEEE*, and Javier Lopez, *Senior Member IEEE*

Abstract—Despite successive attempts to protect critical infrastructures against incidents and malicious threats by using traditional situational awareness solutions, the complex and critical nature of these infrastructures makes this adaptation difficult. For this reason, experts are reconsidering the topic of Wide-Area Situational Awareness (WASA) to provide monitoring of performance at all times from anywhere while ensuring dynamic prevention and response services. Given the novelty of this new research field, a WASA methodological framework together with a set of requirements for awareness construction are presented in this paper in order to help in the development and commissioning of future WASA defense solutions.

Index Terms—Situational Awareness, Context-Awareness, Critical Infrastructure Protection

1 Introduction

Situational awareness (SA) has become one of the most cutting-edge research areas in recent years by being a transversal field to other investigation areas, such as Critical Infrastructure Protection (CIP). Through SA, control systems responsible for monitoring other Critical Infrastructures (CIs), such as Supervisory Control and Data Acquisition (SCADA) systems, could be able to understand events occurring within the observed infrastructure at any time. These events can be of different natures with very specific goals within the infrastructure that can become significant for protection. This means that the monitoring should focus not only on supervising normal states of a CI but also on monitoring the welfare of the infrastructure itself to prevent, detect and respond to internal failures (hardware (HW)/ software (SW) malfunctions) and/or deliberate actions in a timely and efficient manner.

Unfortunately, existing SA solutions are not good enough to address the protection of CIs. The vast majority of these infrastructures are extensively distributed in different locations where their control may be reduced to the minimum (perhaps none) number of human operators. Because of this fact and the need to drive SA in these systems, experts in CIP are combining efforts to start a new era of protection towards Wide-Area Situational Awareness (WASA) [1]. This new defense aims to provide dynamic solutions that help the control system prevent any intrusive or threatening presence that puts the security of the entire system/s at risk. In order to help drive new WASA initiatives, this paper deals with the development of a methodological framework in which a set of requirements of awareness construction for critical environments is addressed. In addition, the feasibility of the framework is validated through a threat analysis on critical resources and information, and applied in different types of threatening scenarios.

The paper is organized as follows. Section 2 analyzes the need of awareness for critical scenarios and the importance of the technique when faced with threatening situations. Section 3 identifies the construction requirements for awareness that are necessary to introduce the methodological framework in Section 4 and its applicability in Section 5.

2 Awareness Paradigm

SA in application domains based on human-machine is still an immature concept that can be confused with the concept of context-awareness, which was introduced by Schilit in 1994 as a term of ubiquitous computing [2]. The differentiation between SA and context-awareness can be found in the abstraction level of their models and in the level granularity and representation of a context [3]. A. Dey defines context as "*any information that can be used to characterize the situation of an entity*". An entity is a person, place or object that is considered relevant for the interaction between a user and an application [4]. This characterization is used by context-aware computing systems to deliver relevant information to a low-level representation and services to the end-user. Its value is dependent on the characteristics (physical events; e.g., level of voltage) associated with the application domain (e.g., energy substations) within which the CI (e.g., electrical generators) is being developed.

Physical events, generally perceived by sensory devices, can be subject to a primary structure of information related to *location* (where), *identity* (who), *activity* (what, a problem) and *time* (when) that are normally used to determine the why of a given situation [4]. Any additional information would simply attempt to offer a more accurate picture of such a situation. In contrast, SA is concerned with a state of knowledge (high-level information) that explains what an application domain is experiencing at a given moment. It corresponds to the outcome given by a set of strategic processes.

- *C. Alcaraz is with the Computer Science Department, University of Malaga, ES, 29071 Spain, e-mail: alcaraz@lcc.uma.es (http://www.nics.uma.es/alcaraz)*
- *J. Lopez is with the Computer Science Department, University of Malaga, ES, 29071 Spain, e-mail: jlm@lcc.uma.es (http://www.nics.uma.es/jlm).*

There are currently several ways of addressing a state of knowledge and these will depend on the degree of user interactivity within an application domain and on the conceptual perspective taken by experts. Some believe the SA field for dynamic and complex systems can be associated with the cognitive model defined by R. Endsley in 1995 [5]. The model is based on perception of physical events from an environment, the comprehension of their meaning, and the projection of their status in the near future. Other experts who defend the observer theory rebuff this way of identifying behavior. This theory relies on those objections made by humans who actively interact with the application domain. There are other experts who believe in the need to combine both previous perspectives to offer hybrid models able to objectify cognitive interpretations through the observations made by an observer [6].

It is only now that international standard organizations and relevant companies working on CIs are recognizing the need for situational awareness. This is the case of the National Institute of Standards and Technology (NIST), which in [7] classifies *situational awareness* as one of the eight priority areas to be taken into account when protecting CIs such as Smart Grids. This priority area, known as WASA, not only focuses on monitoring critical system components and their performance at all times, but also *anticipate, detect and respond to unforeseen situations* (failures or attacks) before they can cause disruptions.

2.1 Importance of Awareness in Critical Infrastructures

Technological convergence for modernization and interconnection of critical systems is bringing about numerous security problems. New vulnerabilities and threats from information technologies are being added to existing vulnerabilities of the underlying system [8]. According to the incident report published by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [9], the rate of incidents (caused by failures and attacks) in CIs has become more significant in all the different critical sectors and in their control systems; e.g., 9 incidents were registered in 2009, 41 in 2010 and 198 in 2011. As in conventional information systems, the adversary's goal is to try to bypass the security mechanisms to penetrate inside the system, and once inside to carry out further attacks.

Security mechanisms are generally implemented according to the security priorities given and the level of criticality of a system. For example, industry and SCADA systems demand a specific security order: *Availability*, *Integrity* and *Confidentiality* (AIC) [10] since the unavailability of data (e.g., alarms, measurements, commands) or resources (e.g., servers, sensors, actuators) or the variation of their content may trigger a major security risk other than merely a threat to confidentiality.

In order to differentiate HW/SW resources and information, we subdivide availability into *Resource Availability* (RA) and *Information Availability* (IA). A threat to availability is normally exploited by Denial-of-Service (DoS) attacks to disrupt or reduce functionalities. A threat to integrity is associated with the adversary's ability to manipulate or destroy the integrity of a resource (*Resource Integrity* (RI)) or information (*Information Integrity* (II)), and could be carried out through malware such as trojans, viruses or worms. This security property can also be related to the manipulation of security credentials, permissions and roles so as to impersonate a user's identity (*User Integrity* (UI)) such as the administrator of the system (*Host-User Integrity* (HUI)). A threat to confidentiality concerns the adversary's ability to eavesdrop or deliberately expose sensitive information relative to configurations (*Resource Confidentiality* (RC)) or critical data such as credentials, commands, alarms or measurements (*Information Confidentiality* (IC)). The frequent tracking of RC/IC could even help attackers gain more knowledge of vulnerabilities in order to modify/disrupt critical sections of the system.

Cyber-Attacks	Threat on AIC	Impact on AIC
Industrial Sector		
Siberian PipeLine Explosion (1982)	RI via a trojan	II
Chevron Alert System (1992)	RI*, UI*	II
Gazprom (1999)	UI* via a trojan	UI
Maroochy Water System (2000)	RI*, UI*	UI
California System Operator (2001)	HUI	Unknown
Davis-Besse Nuclear Plant (2003)	RI via a worm	UI
Zotob (2005)	RI via a worm	RI
Electricity Grid in U.S. (2009)	RI via malware tools	RI, IC
Mariposa (2009)	RI via a bonet	RA, UI, II
Stuxnet (2010)	HUI, RI via a worm, trojan	IU, II
Night Dragon (2011)	UI, HUI	IC
DUQU (2011)	RI via a virus	IC
Flame (2012)	RI via a worm	IC, UI
Governmental and Public Sector		
Salt River (1994)	UHI, RI via a trojan	IC, II
Conficker (2011)	RI via a worm	Unkown
Transport Sector		
Worcester Airport (1997)	RA, HUI	UI
CSX Corporation, Sobig (2003)	RI via a virus	UI
Financial Sector		
Gauss (2012)	RI via a virus	IC, UI

Table 1 Relevant Cyber-Attacks in CIs, Retrieved from [8], [9] and Using the Threat Taxonomy AIC

Considering this security taxonomy, Table 1 illustrates how threats to AIC can have a serious impact on critical systems. This table illustrates in detail the nature of each threat, most of which targeted the integrity of control resources, databases, critical information and users. Although these threats normally come from external entities

with specific goals such as cyber-espionage (represented in Table 1 with a dark background), it is also possible to find threats sparked by internal malicious entities who maintain a close relationship with the observed system (represented in Table 1 with `*'). This is the case of the Maroochy water system where a disgruntled operator gained access to wireless network to execute false commands [8].

Although Table 1 clearly justifies why operative entities (e.g., human operators) should be made aware of these situations so as to deliver a rapid response, the efficiency of such an action relies on the information received from the context and the degree of interpretation of such a context. In fact, an improper action could also bring about unexpected security problems that could have serious or irreparable consequences for the safety-critical of the system/s [8]. Safety-critical is a security property, which concerns the ability of the system to operate under adverse, accidental and unplanned conditions. This property is closely related to the cascading effect, the propagation of which may lead to serious economic and social crisis to a nation/s [10].

3 Requirements for Building Awareness

The integration of existing and new awareness models inside critical control systems should not consist of a trivial and single step. Rather, it must follow a gradual process to ensure compliance with the prerequisites of the application domain [10] and integrate a set of further high-level functionalities according to these prerequisites. This means that experts in CIP have to thoroughly study the inherent characteristics of each infrastructure to identify those functional services required for their protection such as automatic incident management or dynamic response. This analysis can also assume a larger study of functional complexities in order to achieve a trade-off between performance and protection. These requirements are stated below.

3.1 Technological Decoupling

WASA solutions must be supported by technologies able to work properly irrespective of their location and environmental conditions. This technological deployment can range from large communication infrastructures, such as the Internet and cloud-computing, to small and constrained objects (e.g., sensors) installed close to the CI under observation. However, this technological coupling together with the protocols could imply important architectural complexities that may involve incompatibilities, conflicts or operational delays. If in addition, the SA approach is not configured or implemented properly, any security threat to AIC or malfunction within the CI could have an impact on its survivability of malicious actions and dependability when faced with internal incidents [10].

3.2 Availability and Redundancy

SA components are normally configured inside the main interfaces between the supervisory world (i.e., the control center) and the acquisition world (i.e., the observation system). These main interfaces, working as gateways, should always be active and their observation systems together with their critical information should always be available. This means that any malfunction or threat to the availability of these interfaces may leave areas isolated and unprotected. These situations may have a significant impact on the security and the safety-critical of the system or systems involved. A way of mitigating these situations would be the design and implementation of redundant solutions.

3.3 Anticipation, Dynamism and Autonomy

Efficiency of operative actions normally relies on the degree of prevention of anomalies. An anomaly is something that deviates from what is standard, normal, or expected; and it is normally associated with recognized symptoms (based on rules/patterns) by an organization. A symptom is a characterization or indication of the existence of something, and it can be categorized as follows:

- *Infrastructural anomalies*: Control of physical events of the observed infrastructure. Such a control may focus on checking whether a physical event is within its permitted thresholds as defined by the security policies of an organization/country.
- *Anomaly control*: Detect HW/SW malfunctions within the control network.
- *Intrusion control*: Detect suspected activities in AIC (see Section 2.1).
- *Combination*. A mixture of the previous categories.

The more intelligent, accurate and autonomous the WASA approach is for managing these types of symptoms, the greater the probability that operative entities can respond to emergency situations in a timely and efficient manner. Moreover, this response should be as automatic as possible when parts of the system are to be found at distant locations with minimal (or null) local control, such as substations; and in the worst scenario be able to offer dynamic recovery techniques of states and critical information.

3.4 Transparency, Coexistence and Reliability

When different observation systems and communication networks need to cooperate with each other to monitor and protect CIs, their interconnections should be transparent to operative entities. This transparency should be mainly provided through powerful gateways that connect different types of networks and technologies. However, the degree of heterogeneity and the nature of the application domain (e.g., industrial noise) may affect the reliability of the communication. For this reason, recent industrial communication protocols, such as ISA100.11a [11], include within their standards, the hopping and blacklisting methods to facilitate the change of radio frequency channel, as well as the design of mesh topology networks for link redundancy.

3.5 Sustainability and Accountability

In order to accomplish sustainability, WASA solutions should ensure four other chief requirements: Scalability, extensibility, interoperability and maintainability [10]. Scalability concerns the capacity of a network to increase/decrease its hardware capabilities and its ability to manage them. Extensibility is, to the contrary, associated with the ability to improve the functional capabilities with new/modified services (e.g., new rules/patterns). However, and unfortunately, the integration of new services or resources inside complex systems could also bring about serious compatibility problems when aspects of interoperability are not properly addressed.

On the other hand, maintainability is also essential to not only enhance scalability and extensibility but also to enable reliability when errors and vulnerabilities appear within the system. Moreover, accountability aspects should be considered to offer not only the input necessary for reparation/upgrade tasks of existing deficiencies, but also to facilitate forensic and correlation tasks to clarify the causes of such deficiencies.

3.6 Security and Safety-Critical

Guaranteeing security in the different processes of a WASA solution is a matter of utmost importance. If this security is not fully addressed, any problem that has an impact on the integrity of the elements that comprise the WASA solution will potentially affect the performance of the underlying system, with a high probability of affecting the normal execution of operations (safety-critical). In this regard, knowledge of different taxonomies of threats according to the observation system and protection of the communication channels between the elements that composed the observation system are required. The protection can include cryptographic services, security services offered by the great majority of communication protocols, virtual private networks, in addition to boundary services for intrusion detection, access control, authentication and authorization. As for the control of anomalies that can cause a cascading effect, the WASA solution also has to configure proactive services for the anticipation of faults, reactive services to minimize security risks, as well as recovery and/or restoration services to return to normal states.

4 A Methodological Framework for Awareness

A WASA methodological framework for constructing future SA solutions is proposed in this section. The framework is based on the combination of two theories (cf. Section 2): (i) *The hybrid perspective* to objectify observations where a human presence and his/her decisions are relevant to address emergency situations; and (ii) the concept of *context-awareness* for the deliberation of functional services [3].

Indeed, context-awareness is based on three main phases: The acquisition of a type of context, the understanding and representation of such a context, as well as the deliberation of services according to the recognized context. Depending on the level of development of these phases, the resulting model could display different kinds of contexts and manage a set of suitable functional and/or automatic services for an application domain. Given that these functional services can become the foundation for the construction of essential proactive and reactive solutions required for WASA, the core of the framework is therefore based on context-awareness so as to not only offer high-level information but also protection. Apart from this, the framework also needs to be able to adapt heterogeneous technologies with the capability to control CIs from anywhere, anyhow, at any time. The selection of these technologies should be subject to the potential capacities of each of them.

The framework is composed of two main phases (see Fig. 1). The first phase, called here the *setup and commissioning phase*, focuses on initializing the context and configuring the entire approach. The second phase corresponds to the *development phase*, which is based on a set of high-level services that must be active throughout the life-cycle of the approach. For the sake of clarity, these two phases are described in detail in the following sections.

4.1 Setup and Commissioning Phase

Any network designer's first task should be the specification of the context. The definition should include at least the primary structure, commented on in Section 2, where four particular attributes were highlighted: *Location* (Lc), *identity* (Id), *activity* (Ac) and *time* (Tm) [4]. This primary structure can increase its information by adding secondary attributes such as the *level of criticality* (LC). This new attribute is in charge of explaining the current state of the observed infrastructure at a given moment, the values of which can be tagged by objects of the observation system.

The criticality range of LC depends on both the security policies of the organization and on the characteristics associated with the alarm management systems applied for the WASA solution, where aspects of prioritization establish an order for attending to situations. For example, ISA100.11a handles five levels of priority for alarms: *Urgent* (U'), *high* (H'), *medium* (M'), *low* (L'), *journal* (J'). These alarms are managed by each network device, but only one of them (generally, the gateway) is responsible for buffering them, using organized queues according to their levels of priority.

Considering the analysis of context in [4], specification of attributes for CIs should be dependent on the type of observation (cf. Section 3.3). For example, observations for a particular attack on the AIC may not necessarily

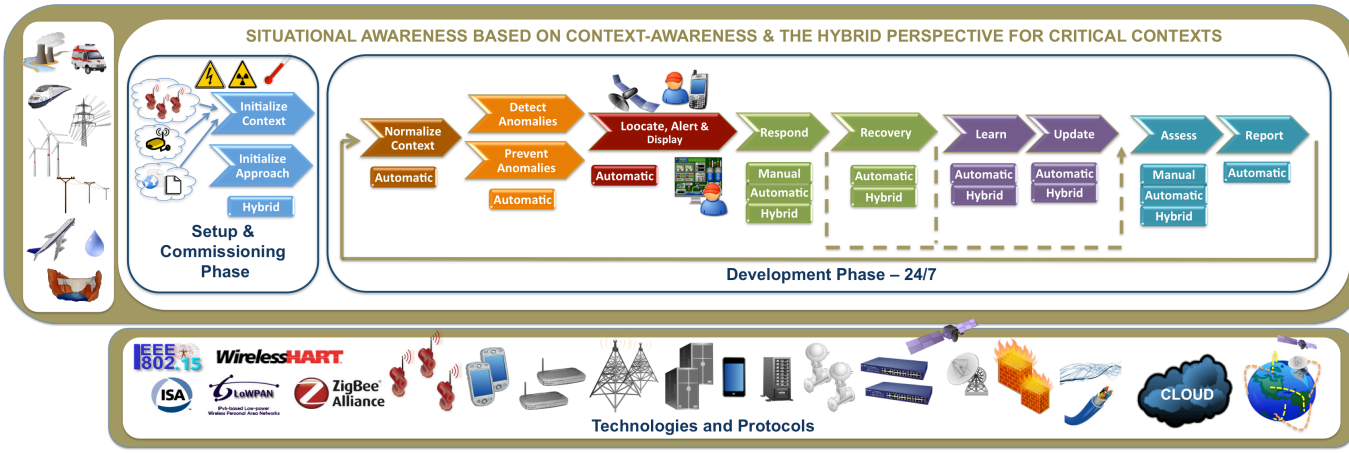

Fig. 1. Methodological Framework for WASA

require all of the attributes for the context. Perhaps, a minimal part of the set of attributes would be sufficient to identify such a threat. To understand this, an analysis of threats in AIC (cf. Section 2.1) is analyzed and summarized in the first three columns of Table 2. This table clarifies the importance of the definition and classification of the context according to what the control system wants to observe and protect.

4.2 Development Phase

In this second phase, a further six phases are stated: *Normalization* (N), *prediction and detection* (Pr/Dt), *location, alerting and display* (Lct/Al/Ds), *response and recovery* (Rs/Rc), *learning and updating* (Ln/Up), and *assessment and reporting* (Ass/Rp). The three first phases are closely related to situational awareness based on context-awareness (i.e., primary actions), and the rest of the phases comprise a set of actions to ensure dynamic protection, performance and maintenance at all times (i.e, secondary actions). The methodological process basically follows a sequential scheme, which is illustrated in Fig. 1 and is thoroughly discussed in the following sections.

1) *Normalization*: The underlying system has to be controlled 24/7 without losing the monitoring of its states, where different context formats are received from different technological sources. Because of this heterogeneity, the incoming context has to be normalized to abstract the semantic value that has to be later interpreted by the rest of the modules that comprise the approach.

2) *Prediction and detection*: Both prevention techniques focus on the interpretation of the normalized context to determine the nature of an environment at a given moment. Still, there is a notable difference between the two techniques. The prediction works at an earlier stage than the detection so as to anticipate anomalies through forecasting models, which are based on predictive and statistical models. According to [12], there are three ways of analyzing states for prevention: (i) *Threat observation* methods (Bayesian predictors, non-parametric methods, counting/threshold), (ii) *symptom monitoring* methods (stochastic models, control theory, machine learning, classifiers, time series analysis), and (iii) *error detection* methods (frequency of occurrence, rule-based system (data-mining, fault trees) or pattern recognition through Markov models).

In order to control the accuracy of these prevention techniques, rates of False Positives (FPs, false warning), False Negatives (FNs, missed warning), True Positives (TPs, correct warning) and True Negatives (TNs, correctly no warning) should be taken into consideration. The relevance of these rates can be better understood by looking at an example. Let us suppose that the observation system is suffering a Sybil attack, where a malicious sensor of the system is impersonating several legitimate identities at different locations, to intentionally make the system believe an unreal situation. As a result, the rates of FPs/FNs in the prevention tasks could become unreal values and therefore unreliable. In order to avoid this situation and detect this attack, the detection techniques should analyze the discrepancies between the attributes of *identity* and *location* with respect to the entire observation system (see Table 2).

3) *Location, alerting and display*: Depending on the location of the CI, the system has to endow the WASA solution with location capacities to offer a rapid response. These capacities can optionally (denoted in this paper with the symbol `+') rely on geospatial technologies or databases with information of operators' availability according to their contracts. When the underlying system is faced with a threatening or anomalous situation, the WASA solution has to locate and warn those human operators nearest to the affected area. The representation of the warning, mainly based on attributes, should be sufficiently complete so as to provide a clearer picture of the situation.

4) *Response and/or recovery*: A response in CIs can be addressed through a *manual* (M) action (taken by a human operator), an *automatic* (A) action (taken by the

Threat on AIC	Use Case	Context					Actions of the WASA Solution											
		Primary Attributes				Sec. Attr	Primary Actions							Secondary Actions				
		Lc	*Id*	*Ac*	*Tm*	*Lc*	*N*	*Pr*	*Dt*	*Lct*	*Al*	*Ds*	*Rs*	*Rc*	*Ln*	*Up*	*Ass*	*Rp*
Infrastructural Anomalies																		
RA	*Unavailability of electrical service*	✓		✓	✓	U′	A	A	A	A+	A	A	M/A/H	(A/H)+	(A/H)+	(A/H)+	M/A/H	A
RI	*Voltage is not inside [Vmin, Vmax]*	✓	✓	✓	✓	L′/M′/H′/U′	A	A	A	A+	A	A	M/A/H	(A/H)+	(A/H)+	(A/H)+	M/A/H	A
Control Anomalies																		
RA (sensor)	*No battery*	✓	✓	✓		H′/U′	A	A	A	A+	A	A	M				M/A/H	A
RI (sensor/ gateway)	*HW/SW configuration error*	✓	✓	✓	✓	H′/U′	A	A	A	A+	A	A	M/A/H	A/H	(A/H)+	(A/H)+	M/A/H	A
Infrastructural Anomalies																		
RA (sensor)	*Physical attack*	✓	✓	✓		H′/U′	A	A	A	A+	A	A	M		(A/H)+	(A/H)+	M/A/H	A
IA/RI (sensor/ gateway)	*DoS attack/ Desconf. of parameters*	✓	✓	✓	✓	H′/U′	A	A	A	A+	A	A	A/H	A/H	(A/H)+	(A/H)+	M/A/H	A
II (sensor)	*Information manipulation*		✓	✓		H′/U′	A	A	A	A+	A	A	A/H	(A/H)+	(A/H)+	(A/H)+	M/A/H	A
UI (sensor)	*Sybil attack*	✓	✓			H′/U′	A	A	A	A+	A	A	A/H	(A/H)+	(A/H)+	(A/H)+	M/A/H	A
RC/IC (sensor)	*Routing table/ Sniffing*		✓	✓		J′/L′/M′	A	A	A	A+	A	A	A/H		(A/H)+	(A/H)+	M/A/H	A

Table 2 Analysis of Threats in AIC for Energy Control Substations Based on [4] and ISA100.11a

WASA solution) or a *hybrid* (H) action (automatic execution under a human supervision). In order to dynamically protect those areas with minimal supervision, automatic response systems (using decision and action trees) should be considered. However, it is quite logical to think that full delegation in automatic response systems in critical environments may create major security risks if the response system is not updated properly or is not able to find an appropriate action according to the context. Therefore, there may be certain situations that force the organization of the application domain to prefer a M/H response instead of relying entirely on dynamic mechanisms to assist in emergency situations.

Moreover, the WASA solution could also be optionally customizable to offer support for recovering of or restoring missed states/information in an A/H manner. This recovery can be subject to controllability (manipulation of parameters to drive the system to a particular configuration) or the use of redundant systems with the capability to massively store data. An example is the cloud-computing services, which offer a suite of advantages for data availability and redundancy at a low cost. In this way, if the system loses control of itself, a great part of its configuration and information is centralized inside the cloud.

4) *Learning and updating*: These two services focus on providing dynamic learning solutions that facilitate the automatic update of behavior rules/patterns for providing security and protection at all times. The learning phase could include incremental learning techniques (decision trees, neural networks, or Bayesian networks) or data-mining for sequential patterns, time series and statistical analysis [12]. Although these techniques can be useful for WASA approaches, there is still a necessity to progress in lightweight methods using a set of relevant parameters, such as: The LC of a context, past experience, or the impact and scope of an adverse effect. When the learning module generates new rules/patterns, the WASA solution should also (automatically or in hybrid) update the entire approach to contemplate this new knowledge in the near future.

5) *Assessment and reporting*: Once incidents have been solved, the system waits to receive a feedback value from operative entities to evaluate the efficiency of the entire approach through out the updating of the rates associated with FP, FN, TP and TN. For the accuracy evaluation, threshold values are needed to determine when to send a warning. The warning should include information about the current state of the observed system and the efficiency of its observation devices. This way, it is possible to detect

strange behavior throughout the approach and identify whether the prevention techniques hamper other protection tasks (i.e., a bad detection could affect the prediction) and their rates of accuracy. For the control of the FN rate, the system has to be flexible in order to receive a manual feedback from operative entities. The penalization in this case should be more notable using much more restrictive thresholds given that existing anomalies have not been detected correctly.

5 Further Discussion

Table 2 summarizes the purposes of the framework for different types of contexts and critical scenarios. In particular, it shows how primary actions should automatically be executed as an integral part of the approach, thereby complying with the concept of SA; whereas most of the secondary actions can optionally be customizable. For example, although it is highly recommended for CIP to create hybrid solutions under supervision, it is also advisable to consider the automatic option when the environment is practically isolated. This also means that the design of WASA approaches is directly proportional to the nature of the application domain.

Some threat scenarios in AIC are also illustrated in Table 2, where specific failures and attacks are analyzed. A typical attack on control systems is for example a false data injection attack (threat to II). The presence of this attack can be detected by analyzing irregular variations of states together with information (*identity* and *activity*) received from different sources (sensors, agents). Warning of this threat is urgent given the criticality of the context and a rapid A/H response is necessary to isolate critical sections from the threat (e.g., closing of ports), as well as to recover missed parameters, using for example controllability. Given the relevance of this framework for protection, it is now the moment to provide effective, dynamic and lightweight solutions that consider this methodology as the guideline for the protection and the foundation for their constructions.

Acknowledgment

This work has been partially supported by the European Commission through the research project NESSOS (IST-256980) and by the Spanish Ministry of Science through the research project ARES (CSD2007-00004). Additionally, the Marie Curie COFUND programme "U-Mobility" co-financed by the University of Malaga and the European Commission under GA No. 246550 has funded the work of the first author.

References

[1] A. Mavridou, M. Papa, "A situational awareness architecture for the Smart Grid", Global Security, Safety and Sustainability & e-Democracy, LNCS 99, pp. 229-236, 2012.

[2] B. Schilit, M. Theimer, "Disseminating active map information to mobile hosts", IEEE Network, vol. 8, issue 5, pp. 22-32, 1994.

[3] N. Nwiabu, I. Allison, P. Holt, P. Lowit, B. Oyeneyin, Situation awareness in context-aware case-based decision support, IEEE Conference on CogSIMA, pp. 9-16, 2011.

[4] A. Dey, K. Anind, P. Brown, N. Davies, M. Smith, P. Steggles, "Towards a better understanding of context and context-awareness", Symposium on Hand-held and Ubiquitous Computing, Springer-Verlag, pp. 304-307, 1999.

[5] R. Endsley, "Toward a theory of situation awareness in dynamic systems", Human Factors: The Journal of the Human Factors and Ergonomics Society, vol. 37, issue 33, pp. 32-64, 1995.

[6] C. Sandom, "Operator situational awareness and system safety", IEEE System Dependency on Humans, pp. 5/1-5/8, 2000.

[7] NIST, "NIST framework and roadmap for Smart Grid interoperability standards", release 2.0, NIST special publication 1108R2, 2012.

[8] B. Miller, D. Rowe, "A survey of SCADA and critical infrastructure incidents", Conference on Information Technology Education, pp. 1-6, 2012.

[9] ICS-CERT, "ICS-CERT incident response summary report", pp. 1-17, 2009-2011, http://www.us-cert.gov. Accessed on January 2013.

[10] C. Alcaraz, J. Lopez, "Analysis of requirements for critical control systems", International Journal of Critical Infrastructure Protection, Elsevier, vol. 2, no. 3-4, pp. 137-145, 2012.

[11] ISA-100, "An ISA standard wireless systems for industrial automation: Process control and related application", ISA-100.11a-2009, pp. 1-817, 2009.

[12] F. Salfner, "Event-based failure prediction an extended hidden Markov model approach", Doctoral Thesis, pp. 1-301, Humboldt-Universittzu, Berlin, 2008.

Cristina Alcaraz is a Postdoctoral Researcher of the Network, Information and Security (NICS) Laboratory who received her PhD in Computer Science in 2011 from the University of Malaga. Her main research activities focus on CIP, security of SCADA systems and Smart Grids.

Javier Lopez is Full Professor in the Computer Science Department at the University of Malaga, and Head of NICS Lab. His research activities are mainly focused on information security and CIP, and has lead several international research projects in those areas. Prof Lopez is Co-Editor in Chief of IJIS journal and the Spanish representative in the IFIP TC-11 on Security and Privacy Protection in Information Systems.