C. Alcaraz, L. Cazorla, and J. Lopez, "Cyber-Physical Systems for Wide-Area Situational Awareness", *Cyber-Physical Systems: Foundations, Principles and Applications*, pp. 305 - 317, 2017.
http://doi.org/http://dx.doi.org/10.1016/B978-0-12-803801-7.00020-1
NICS Lab. Publications: https://www.nics.uma.es/publications

Cyber-Physical Systems for Wide-Area Situational Awareness

Cristina Alcaraz[a*,a], Lorena Cazorla[a], Javier Lopez[a]

[a]*Computer Science Department, University of Malaga,*
Campus de Teatinos s/n, 29071, Malaga, Spain
{alcaraz,lorena,jlm}@lcc.uma.es

Abstract

Cyber-physical systems (CPSs), integrated in critical infrastructures, could provide the minimal services that traditional situational awareness (SA) systems demand. However, their application in SA solutions for the protection of large control distributions against unforeseen faults may be insufficient. Dynamic protection measures have to be provided not only to locally detect unplanned deviations but also to prevent, respond, and restore from these deviations. The provision of these services as an integral part of the SA brings about a new research field known as wide-area situational awareness (WASA), highly dependent on CPSs for control from anywhere across multiple interconnections, and at any time. Thus, we review the state-of-the art of this new paradigm, exploring the different preventive and corrective measures considering the heterogeneity of CPSs, resulting in a guideline for the construction of automated WASA systems.

Keywords: wide-area situational awareness; cyber-phsysical systems; control systems; critical infrastructure protection; detection; response; restoration

1. Introduction

Cyber-physical systems (CPSs) are collaborative systems composed of autonomous and intelligent devices capable of managing data flows and operations, and monitoring physical entities integrated as part of critical infrastructures (CIs). The interaction between cyber-physical devices (CPDs) is done through large, heterogeneous and interconnected communication infrastructures. Through these infrastructures, control systems can process and manage measurements and evidence produced in remote locations, and distribute and visualize control transactions. The interfaces that lead these activities are generally control devices that ensure the intermediation tasks between the acquisition world and the control world, such as gateways, servers or remote terminal units (RTUs). An RTU, typically working at ∼22MHz-200MHz with 256 bytes-64MB RAM, 8KB-32MB flash memory and 16KB- 256KB EEPROM, serves as a data collector or a front-end to reach remote substations equipped with sensors or actuators responsible for executing a specific action in the field.

Unfortunately, remote substations do not always envisage a holistic protection, which makes prevention from anywhere, at any time and at anyhow, a crucial issue. The vast majority of CIs are exposed daily to continuous changes, mainly from unforeseen faults, malfunctions or deliberate disturbances as published by the Industrial Control Systems Cyber Emergency Response Team in (ICS-CERT, 2015). So the technological competences of many CPSs should consist of the minimal protection services that traditional situational awareness (SA) systems

demand, such as perception of observed environment, understanding their meaning and their projection in the near future, initially introduced in (Endsley, 1995).

However, SA solutions for critical control applications deployed in large distributions can be insufficient, as local protection through "*dynamic services*" is also required to ensure one of the eight priority areas defined by the National Institute of Standards and Technology in (NIST, 2014). This area, known as wide-area situational awareness (WASA), not only focuses on monitoring critical components and their performance at all times, but also on automatically *anticipating, detecting and responding to unplanned faults*, and if necessary *restoring states* before major disruptions can arise. This means that WASA strategies should be consolidated in a methodological process that helps the underlying system extract, interpret and respond to threatening situations, as proposed in (Alcaraz and Lopez, 2013). However, this paper neglects the relevance of studying preventive and corrective measures, taking into account the properties of the context, the features of the underlying system and its technological capacities.

Generally, CPDs can be categorized according to their functional capacities: *weak, heavy-duty* and *powerful-duty* (Roman et al., 2007). Within the class weak, are extremely constrained devices but with sufficient competences to run simple operations, such as ∼4MHz, 1KB RAM and 4KB-16KB ROM. (e.g., home-appliances, sensors). Devices belonging to the heavy-duty category are relatively expensive devices (e.g., handled-devices, smartphones) that are able to execute any simple or complex critical action. Their microprocessors are quite potent, working at around 13MHz-180MHz, 256KB-512KB RAM and 4MB-32MB ROM, and within this category, we highlight the role of the RTUs, smart meters (∼8-50MHz, 4KB-32KB RAM and 32-512KB flash memory) or industrial wireless sensor networks (WSNs). Industrial sensors usually have slightly greater capacities than conventional ones, equipped with a ∼4MHz- 32MHz, 8KB-128KB RAM, 128KB-192KB ROM, and can protect the observed infrastructure through their sensorial modules and manage data streams. Finally, the powerful-duty class contains all those devices with significant capacity to address any action or application, such as servers, proxies or gateways. Considering this taxonomy, the main contribution here is to offer the necessary guidelines to build effective WASA solutions, which should rely on automatic and lightweight protection services that do not jeopardize the functions of the primary systems.

The chapter is organized as follows: Section 2 introduces the current prevention, response and restoration solutions, examining all those features make them suitable for devices deployed in cyber-physical contexts, thus promoting their applicability for future WASA applications. The exploration of the capacities that the different models can demand, and their ability to encourage accurate awareness and response to faults (Byzantines, transient or fail-stop faults (Treaster, 2005)), are given in Section 3 together with the conclusions and future work.

2. Wide-Area Situational Awareness: Automated Prevention, Response and Restoration

2.1. Prevention and Detection

Within the field of prevention, it is important to consider detection techniques as specified in (Chandola et al., 2009; Gyanchandani et al., 2012; Kotsiantis et al., 2007). Five groups of detectors are stressed: *Data mining-based*, where the techniques directly depend on a set of data to find behavior pattern sequences; *statistical-based* composed of interference tests to verify whether a specific instance data belongs to a statistical model; *knowledge-based* which progressively acquire knowledge about specific threats; *information and spectral theory-based* focused on the data itself, its order and its meaning; and all those other well-known *machine learning-based* techniques such as artificial neural networks (ANNs), Bayesian networks (BNs), support vector machines (SVMs), rule-based, nearest neighbor-based, fuzzy logic and genetic algorithms.

For each of the aforementioned classes, there is a set of machine learning sub-classes. Within the data-mining category are the *classification-based* techniques; a set of classifiers capable of assigning data instances to normal/anomalous collections such as *classification and regression trees*. These structures are composed of tree-like constructions of fast computation by comparing their data instances against a pre-computed model. *Association rule*

learning is another sub-class of data mining, which identifies the relationships between categorical variables using rules and thresholds to prune. The effectiveness of the approach depends on the parameters that configure the pruning operations and their algorithms. Likewise, *Clustering-based algorithms* group data instances in clusters through an unsupervised/semi-supervised method where computing distances between data points, is required, like the k-means algorithm.

The statistical-based group contains the *parametric and non-parametric-based* models, such as Gaussian-based models or histogram-based techniques, which control interfering data points according to the data observed. These models are generally accurate and tolerant to noise and missing values, providing a better picture about the confidential interval associated with the anomaly, but the accuracy relies heavily on the complexity and length of their datasets. This class also comprises the operational models based on computing counters whose values are bounded to predefined thresholds. This constrained feature restricts their use to those dynamic scenarios in which their contexts are subject to continuous changes and their values are not predefined properly. *Time series* and *Markov -based* models are two further subclasses of this group. The former predicts behaviors through successive and uniform time series, such as smoothing techniques based on weighted data instances and their variant exponential smoothing models. Although they are generally accurate and tolerant to insignificant changes and missing values, they tend to produce weak models for medium and long-range forecasting with a heavy dependence on past evidence and on the smoothing factor to forecast. Markov models are, to the contrary, a mathematical representation whose quantitative values and operations are closely related to a state transition (probabilistic) matrix. This matrix contains all the activity transactions without having to have knowledge of the situation, where the operational difficulty varies according to the complexity and dimensionality of the situation, and its precision depends on the variations in the activity sequence.

The techniques in knowledge-based detection progressively acquire knowledge about specific threats, guaranteeing high accuracy with a low false positive rate (FPR), flexibility and scalability for expanding the detection engine with new knowledge. Gyanchandani et al. in (Gyanchandani et al., 2012) identify three types of approaches in this field, *state transactions* through state transaction diagrams; *Petri nets* using directed bipartite graphs restricted to conditions and events; and rule-based *expert systems* capable of reasoning about provided knowledge. But despite the potential to autonomously recognize anomalies, their intelligent implementations depend on the degree of granularity and maintenance of their knowledge. Regarding the information and spectral theory-based class, their statistical approaches are planned in accordance with the irregularities in the data. For example, through the entropy it is possible to identify anomalies whose feasibility is subject to the size of the dataset; and through spectral schemes it is also possible to obtain time series and the characteristics of the communication channel whose effectiveness is related to the degree of handling high dimensional data and the complexity of their approaches.

The intrinsic features of all these techniques are summarized in Table 2.1, and can be incorporated as detection engines within intrusion detection systems (IDSs) to constantly monitor and evaluate evidence. They can be classified into three categories: *anomaly-based* so as to detect unforeseen deviations from normal behaviors; *signature-based* to perceive abnormal behaviors by matching each instance to an updated database containing the threat models; and *specification-based* to detect behaviors according to the legitimate specifications of the system. These detection features are also analyzed in (Jokar, 2012) stating that anomaly-based IDSs usually provide high FPRs with the ability to predict unknown threats, but require complex training and tuning time. In contrast, signature-based IDSs have low FPR but more difficulty to ensure the detection of unknown threats; whereas specification-based IDSs also guarantee low FPRs with the ability to notice new threats/vulnerabilities within a given system. However, this detection mode has high computational costs to implement predefined threat models, which are closely linked to the functional capacities of their devices.

Table 2.1 Classification and characteristics of the preventive techniques

			Low complexity	Speed of classification	Speed of learning	Handles parameters	Compressibility	Accuracy	Learning from observation	Control – interdep. data	Control – missing data	Control - redundancy	Control - noise	Control – subtle changes	Control – drastic changes	Incremental learning
Data mining-based	Classification-based	Classification trees	✓	✓	✓	✓	✓			×		×				
		Regression trees	✓			✓			✓	×	✓	×				✓
	Association rule-learning based	Apriori, FP-growth, etc.	×		✓	×	✓		✓	✓		✓	×			×
	Clustering-based	K-means, Hierarchical Clustering, etc.	✓	×	×	×	✓	×	✓	×	✓	✓	×			✓
Statistical-based	Parametric and non-parametric	In general	✓		×	×	×	✓			✓		✓	×		
		Operational models	✓			×	×	×							×	
	Time series	Smoothing	×			×	×	✓			✓		✓	✓	×	
	Markov chains	Markov models, HMMs, Hierarchical Markov models, etc.	×		×	×	×	✓	✓				×		×	
Knowledge detection-based			✓			✓		✓								✓
Information and spectral theory-based						×	×					✓	×	✓		
Other machine learning-based	ANN		×	✓	×	×	×	✓	✓	✓	×	×	×			
	BN	In general	×	✓		✓	✓		✓		✓	×	✓			
		Naïve Bayes networks		✓	✓	✓	✓	×	✓	×	✓	×				
	SVM		✓	✓	×	×	×	✓	✓	✓		✓	×			×
	Ruled-based		✓			✓	✓	✓					×			×
	Rule learners		✓	✓	×	✓	✓	×	✓	×	×	×	×			×
	Nearest neighbor	K-nearest		×	✓	✓	×	×	✓	×	×	×	×			✓
	Fuzzy algorithm		✓	✓	✓	✓	✓	×			✓		✓			
	Genetic algorithm		×			✓		×								

2.2. Response

Although IDSs help detect the existence of faults, it is also imperative to take evasive and/or corrective actions to prevent the propagation of secondary effects caused by these faults (Stakhanova et al., 2007). Intrusion Response Systems (IRSs) are systems that have all the IDS capabilities but with the necessary support to stop incidents (Scarfone and Mell, 2007). Since, CPSs are characterized by complex interconnected systems, the avoidance of faults and consequent cascading effects through these preventive systems is of paramount importance. Traditionally, the response to a threat was manual and required a high degree of expertise, but the increasing complexity and speed of cyber-attacks, and the ramifications of faults show the acute need for complex intelligent dynamic IRSs (Stakhanova et al., 2007).

Countermeasures applicable by an IRS can be divided into: *passive* and *active* responses (see Table 2.2). Passive reactions are usually included in the normal operation of some IDSs (Stakhanova et al., 2007), and can be implemented in almost all CPDs according to their capacities (i.e., powerful devices would be able to implement

sophisticated mechanisms; whereas weak devices would implement simpler methods). Within passive reactions, there are two main categories: *administrator notification* and *prevention measures*. The first logs the system's information and state and alerts the system's administrator to control the situation. Notifications to administrators are the most common operations implemented in deployed IDS/IRS solutions. Alert systems do not require high computational power, thus they can be implemented by any CPD.

The presence of prevention measures depends on the computational capabilities of the devices. We have distinguished six chief kinds of preventive solutions: *cryptography* is an effective approach to prevent attackers from understanding captured data (Xing et al., 2010); it is usually used in normal to powerful-duty devices. *Security policies* are the security measures taken by the organizations and they should be implemented by all the devices in the CPS regardless of their computational power; IRSs can follow these guidelines to identify violations in the security policies of the surveilled system (Scarfone and Mell, 2007). *Monitoring* tools (e.g., IDSs) supervise the local (host or network) operations and state in search for intrusive behaviors; IDSs range from heavy-duty to lightweight solutions, thus monitoring could be present in all types of devices in the CPSs.

Protective/defensive infrastructure comprises devices or system configurations designed for protection tasks (e.g., firewalls, demilitarized zones and proxies) (Byres et al., 2005); this infrastructure is compatible with CPDs of all ranges of computational power. *Low-level preventive mechanisms* are physical security measures implemented at the lower layers of the communication systems to prevent intrusions (e.g., directional antennas in wireless devices, or synchronized clocks (Xing et al., 2010)); ideal for weak-duty devices. *Session/communication measures* are techniques that add security at the session or communications levels, (e.g., packet leashes or cookies (Gollmann, 2008)); these protective methods are useful for powerful devices that have to deal with remote connections and queries via the Internet.

Concerning the *active reaction mechanisms*, we can divide them into two groups (Stakhanova et al., 2007): *host-based* and *network-based* response actions. Host-based responses refer to those local operations, which modify parameters or processes within the affected CPDs, e.g., operations on files, operations on user accounts, and operations on processes and services. Here, trust-based mechanisms such as reputation, credit-based trust or token-based trust, are effective information protection methods in communication networks that can be implemented at different levels in the CPSs (Meghdadi et al., 2011). Network-based response, conversely, corresponds to those activities performed in the communications network which affect its services and parameters, e.g., disabling or blocking network operations (Ingols et al., 2009), isolating segments of the network (Meghdadi et al., 2011), modifying routing parameters (Karlof and Wagner, 2003) or setting up deceiver devices (Specht and Lee, 2004). These responses can be implemented in the CPS regardless of the computational power of its devices, since they focus on the network's operation.

Table 2.2 Classification and characteristics of the response mechanisms

			Low complexity	Easy to Implement	Low Use of Resources	Requires additional HW	Adaptable to Changes	Low Impact of Response	Low-risk Automation
Passive	Administrator Notification	Generate System Logs	✓	✓		*	✓	✓	✓
		Generate Alarm	✓	✓	✓		✓	✓	✓
		Generate Report	✓	✓	✓		✓	✓	✓
	Prevention Measures	Cryptography	*		*			✓	✓
		Security Policies	✓	✓	✓			✓	✓

		Monitoring	✓			*	✓	✓	✓
		Protective/Defensive Infrastructure	✓	✓	✓	✓		✓	✓
		Low-level Preventive Mechanisms	✓	✓	✓	*		✓	✓
		Session/Communication Measures		✓				✓	✓
Active	Host-Based	Operations on Files		✓	*				
		Operations on User Accounts		✓	*				
		Operations on Processes and Services			*		✓		
		Trust Mechanisms			*		✓		*
	Network-Based	Disable/Block Operations		✓	✓				
		Isolation Actions	✓	✓	✓				
		Routing	✓	✓	✓		✓		
		Deceiver Devices				✓	✓	✓	*

Table 2.2 overviews the main active and passive response measures that IRSs can implement. For each identified method, we have analyzed several characteristics that determine the environment in which it can be deployed in terms of required resources, adaptability and performance. Parameters such as complexity of the solution and the implementation, the consumption of the resources of the infrastructure, the adaptability and impact of the responses, and the automation capabilities are of paramount importance to determine the applicability of given countermeasures (hence, IRSs) to critical systems such as CPSs. In Table 2.2, we analyze these characteristics for each of the main sets of responses and indicate the strengths of each mechanism (note that * indicates the dependence on the implementation of the countermeasure).

2.3. Restoration

Recovery mechanisms comprise all those actions related to resilience and fault-tolerance that help the underlying system to return to its natural state and operating configuration (Treaster, 2005; Bansal et al., 2012). *Replication-based* techniques are one of the most popular fault-tolerance techniques, which replicate functionalities and add redundancy to the system. The type of data consistency (linearizability, sequential and casual) and the replication mode, *active* or *passive* are important. Passive replication activates the backup systems only when needed, where primary devices are the only ones that can manage replicas. In contrast, active replication constantly replicates evidence and configurations of the primary entity to preserve assets and maintain the backup elements updated at all times.

Although the active mode individually manages evidence in multicast mode to favor the response, the redundancy management causes complexities. When replicas need to be compared to identify Byzantine faults, a voting process in distributed networks is normally required to manage consensus according to detected events. Process level redundancy (PLR) is another example of active replication. It detects transient faults, which are less severe than Byzantines but harder to diagnose. For detection, their algorithms demand software-centric approaches to detect transient faults, resources to reduce overhead and redundant processes to schedule the processes across all system assets.

Rollback is another well-known recovery approach. It includes a *checkpoint-based rollback* with dependency on storage points containing current information, and a *log-based rollback* (also known as a message logging protocol) comprising checkpoints and a record of non-deterministic events. Within the checkpoint class, there are coordinated and uncoordinated approaches. The former synchronizes checkpoints to restrict the rollback propagation, but hampers the recovery time and their functionality in critical contexts. Uncoordinated checkpoints, to the contrary, individually execute checkpoints to later combine them with a message logging protocol, thereby guaranteeing a

complete picture of the process's execution. According to Treaster (Treaster, 2005), there are three main log-based techniques: pessimistic/synchronous, optimistic/asynchronous and causal. Pessimistic logging techniques consist in registering each message received by an entity to be subsequently re-sent, but only if necessary, during the rollback stages; whereas optimistic protocols register events to a volatile memory to later (only periodically) store them in disk. Although this protocol can simplify storage complexities in disk, the recovery process can become much more complex when the logs have not been stored properly over time. Finally, causal protocols log non-deterministic events in a casual manner, but they add the problem of optimistic protocols in which temporarily registered events may be lost unexpectedly.

As the checkpoints can be costly, experts (Ruchika 2013; Veronese and Lung 2009) recommend applying heterogeneous replication-based checkpoints to enhance performance and guarantee tamper-resistance for faults. But their implementation can bring about complexities in the recovery processes due to redundancy, a characteristic that has also been considered in *fusion-based* techniques. These techniques address the problem by relying on fewer backup devices as fusion points, instead of actively configuring replication-based approaches in all the devices. Nonetheless, this characteristic also tends to increase implementation costs and complexities for recovery by maintaining the fusion points up to date.

Table 2.3 Classification and characteristics of the restoration techniques

			Low complexity	Capacity for storage	Performance	Consistency	Accuracy	Responsiveness	Adaptability	High rate of redundancy	Configurability	Handles N-faults	Handles Byzantine faults	Handles transient faults
Replication-based	Active	In general	×	✓	*	✓	✓	✓	✓	✓		✓		
		Voting	×	✓	*	✓	✓	✓	✓	✓		✓	✓	
		PLR		✓	*	✓	✓	×	×	✓	×			✓
	Passive			✓	*	✓		×	✓	×		✓		
Rollback-based	Checkpoints	Coordinated	×	✓	*	✓		×		✓		✓		
		Uncoordinated	×	✓	*			×		×		✓		
		Replication-based	×	✓	*	✓	✓	✓		✓		✓		
	Message logging	Pessimistic	×	✓	*			✓	✓			✓		
		Optimistic	×	✓	*		×	×	×			✓		
		Casual	×	✓	*	✓	×	×	×			✓		
Fusion-based			×	✓	*	✓				×		✓		

Table 2.3 encompasses all the aforementioned properties, which are also sustained by Bansal et al. (Bansal et al., 2012). These authors stress that the performance of each approach (denoted with * in Table 2.3) depends on a set of factors. Replication-based schemes vary according to the number of replicas produced within the system (the performance decreases as the number of replicas increases); checkpoints and rollback depend on the frequency and size of the checkpoints; fusion-based on the rate of faults (low rate of faults improves the recovery); and PRL on the set of faults. If in addition, the approaches are equipped to incorporate multiple fault detectors, the level of reliability, accuracy and adaptation can become quite noteworthy, thereby favoring their use for cyber-physical contexts.

3. Guidelines for WASA: Analysis and Discussion

To assess the applicability of each of the aforementioned methods for CPSs, it is necessary to take into account their computational features and the sensitive nature of the application context. Control systems generally demand (Alcaraz and Lopez, 2012): operational performance, reliability and integrity, resilience and security, and safety-critical. However, guaranteeing these requirements also implies considering the complexities and characteristics of the different approaches (see Tables 2.1, 2.2, 2.3) and their suitability for support by the different CPDs.

For prevention, we consider parameters related to the complexity, the accuracy and the general performance of the models, understanding that vised techniques have a better general performance for real-life problems than unsupervised ones (Sadoddin and Ghorbani, 2007). Solutions such as BNs are difficult to implement successfully in a complex constrained environment, since their computational cost and complexity of implementation increase with the complexity of the system being modeled. Whenever it is necessary to evaluate the correctness of a model, or to add a certain degree of expert knowledge, ANNs and SVMs are more restrictive methods; e.g., SVMs have low complexity models but the learning process's low speed adds implementation overhead. Thus the methods that are better suited for IDSs in constrained scenarios are those based on logic, such as decision trees, optimized rule learners and fuzzy logic, and on simplified computation models such as operational or rule-based models. Decision trees have well-balanced characteristics for this specific context, while rule learners have several drawbacks (e.g., accuracy) that can be easily overcome (e.g., implementing boosting algorithms), but they provide several capabilities (performance, comprehensibility, and easiness of introducing rules by experts), that are vital and really useful in critical contexts. An example of such a system is available in the framework proposed in (D'Antonio et al., 2006), where the IDS component has a classifier engine fed from the knowledge taken from other artificial intelligence modules such as processors and pattern recognition algorithms.

Knowledge-based and rule-based systems, optimized SVN and statistical methods are suitable for integration inside heavy-duty devices because of their accuracy. Depending on the regularity of the traffic, the application context and its capacity for change, optimized parametric or non-parametric solutions, with the exception of the operational models, can be effective approaches since they are moderately complex and have a high efficiency for detection. Similarly, powerful-duty devices can also adopt the knowledge-based schemes and statistical methods because they can autonomously detect slight or abrupt anomalies with a high accuracy. Hidden Markov Models (HMMs) are potential tools for detecting hidden dynamics and extracting knowledge where there may be obfuscation in the traffic received. An example of the use of HMMs in an IRS can be found in (Haslum et al., 2007), where the HMM is used to represent the interaction between the attacker and the system's network. Nonetheless, other methods could be equally applicable for powerful-duty environments, although there are methods (e.g., SVN, rule learners, ANNs, genetic algorithms, etc.) with costly training processes that are less appropriate for dynamic networks with irregular traffic. Although they are present in traditional networks, as in (Fessi et al., 2014) where the authors present an IRS using genetic algorithms for response selection, the frequent occurrence of asynchronous disturbances in the CPS dynamic scenarios may make the IDSs trigger the learning mechanisms more frequently, increasing the overhead in the underlying systems.

These restrictions can be translated to the IRSs, since the applicability of given countermeasures heavily depends on the characteristics of the environment where the response is launched. Currently, IRSs, designed specifically for critical systems, implement some of the response mechanisms mentioned in Section 2.2, particularly passive methods. However, most systems still lack important passive prevention mechanisms because of the legacy equipment, the proprietary protocols and components traditionally present in these environments (Alcaraz and Lopez, 2012). Nevertheless, (see Table 2.2) most passive and preventive mechanisms are easy to implement and introduce few overheads. They are effective and suitable for application in CPSs regardless of the computational power of the environment, but are especially indicated for constrained contexts.

Active reaction solutions, however, are rarely present in these scenarios, since active responses usually imply the introduction of sophisticated mechanisms, implying a higher use of computational resources and equipment. Methods that modify the behavior of the system or the network are only suitable for those sections of the CPSs containing powerful equipment capable of devoting sufficient computational power to the IRS. Additionally, other methods that require extra hardware or need to run powerful intelligent algorithms are only applicable to powerful-

duty environments of the CPS, since they need to perform complex operations with high requirements on computational power.

Regarding restoration, it is possible to note from Table 2.3 that the vast majority of techniques have significant computational and spatial complexities since they require high rates of redundancy. Logging events in an optimistic or casual manner, specification of multicast protocols and configuration of hybrid networks, in which the handling of replicas and checkpoints could be concentrated in some heavy-duty or powerful-duty nodes (RTUs, gateways, servers), could resolve the implicit overheads of the models built in constrained environments such as the decentralized architecture for CPS contexts described in (Pradhan et al., 2014). External storage systems could benefit the data storage and the restoration phases in those nodes classified as weak. The nodes could connect to the cloud and leave backup instances of critical evidence favoring accountability and audits (Alcaraz and Lopez, 2014).

In less restrictive, distributed scenarios, where the rate of redundancy can be higher, more complex reparation mechanisms can be adapted such as the save-point, trees-based rollback presented in (Koldehofe et al., 2013) for distributed environments. Even so, the provision of lightweight and dynamic fault tolerance systems composed of adaptive models in this type of application context is still required. Responsiveness, adaptability, accuracy and performance of the models are fundamental criteria when developing methods, without forgetting the need to launch optimized strategies that provide satisfactory average-time and with linear approximations as stated in (Alcaraz and Wolthusen, 2014).

Table 3.1 Adapting WASA techniques to cyber-physical environments

	Weak	**Heavy-duty**	**Powerful-duty**
Prevention	Decision tress Rule learners Operational models Knowledge-based Rule-based Fuzzy logic	Knowledge-based SVN Rule-based Statistical-based	Knowledge-based Statistical-based
Response	Administrator notification (logs, alarms, reports) Security policies Low-level prevention Cryptography	Monitoring Session/communication measures Modification operations (files, accounts, processes) Routing (isolation, blocking)	Monitoring Operations on processes and services Deceiver techniques Trust mechanisms
Restoration	Passive replication Message logging (optimistic, casual)	Active replication Checkpoint replication-based Message logging (pessimistic, optimistic)	

Table 3.1 summarizes the analysis done in this section and concludes the chapter. The analysis has determined that it is still necessary to continue exploring new strategies that help simplify the implicit overheads in awareness and response tasks, providing more dynamic lightweight solutions where the rate of redundancy reaches minimum values, and the degree of accuracy and responsiveness reach high values. These goals should be part of future work where experts in the field of CI protection should combine efforts to foster the concept of WASA in all those sections that include a CI, without degrading the existing cyber-physical interdependencies and guaranteeing a suitable tradeoff between operational performance and protection (Alcaraz and Lopez, 2012).

Acknowledgements

C. Alcaraz is supported by the “Ramón y Cajal” (RYC-2014-1631) research programme financed by the Ministerio de Economía y Competitividad, and L. Cazorla is supported by a FPI fellowship from the Junta de Andalucía through the project FISICCO (P11-TIC-07223). Additionally, this work has been partially supported by the project PERSIST (TIN2013-41739-R) financed by the Ministerio de Economía y Competitividad.

References

Alcaraz, C., Lopez, J., 2012. Analysis of requirements for critical control systems. International Journal of Critical Infrastructure Protection, Elsevier, 2(3-4), 137-145.

Alcaraz, C., Lopez, J., 2013. Wide-area situational awareness for critical infrastructure protection. IEEE Computer, 46(4), 30-37.

Alcaraz C., Lopez J., 2014. WASAM: a dynamic wide-area situational awareness model for critical domains in smart grids. Future Generation Computer Systems, Elsevier, 30, 146-154.

Alcaraz, C., Wolthusen, S., 2014. Recovery of Structural Controllability for Control Systems. Eighth IFIP WG 11.10 International Conference on Critical Infrastructure Protection, 441, 47-63.

Bansal, S., Sharma, S., Trivedi, I., 2012. A detailed review of fault tolerance techniques in distributed systems. International Journal on Internet and Distributed Computing Systems, 1(1), 33-39.

Bessani, A., Veronese, G., Correia M., Lung., L., 2009. Highly-resilient services for critical infrastructures. In Proceedings of the Embedded Systems and Communications Security Workshop.

Byres, E., Karsch, J. and Carter, J., 2005. NISCC good practice guide on firewall deployment for SCADA and process control networks. National Infrastructure Security Co-Ordination Centre.

Chandola, V., Banerjee, A., Kumar, V., 2009. Anomaly detection: a survey. ACM Computing Surveys, 41(3), 15, 15-58.

D'Antonio, S., Oliviero, F. and Setola, R., 2009. High-Speed Intrusion Detection in Support of Critical Infrastructure Protection. Critical Information Infrastructures Security, Springer, pp. 222-234.

Endsley, R., 1995. Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(33), 32-64.

Fessi, B. A., Benabdallah, S., Boudriga, N. and Hamdi, M., 2014. A Multi-Attribute Decision Model for Intrusion Response System. Information Sciences (270), Elsevier, pp. 237--254.

Gollmann, D., 2008. Securing web applications. Information Security Technical Report 13(1), 1-9.

Gyanchandani, M., Rana, J., Yadav, R., 2012. Taxonomy of anomaly based intrusion detection system: a review. Neural Networks, 2(43), 1-14.

Haslum, K., Abraham, A. and Knapskog, S., 2007. DIPS: A Framework for Distributed Intrusion Prediction and Prevention Using Hidden Markov Models and Online Fuzzy Risk Assessment. International Symposium on Information Assurance and Security, IEEE, pp. 183-190.
ICS-CERT, 2015. Years in Review 2009-2014. <https://ics-cert.us-cert.gov/Other-Reports> (accessed 24.06.15.).

Ingols, K., Chu, M., Lippmann, R., Webster, S. and Boyer, S., 2009. Modeling modern network attacks and countermeasures using attack graphs. Computer Security Applications Conference, IEEE, 117-126.

Jokar, P., 2012. Model-based intrusion detection for home area networks in Smart Grids. University of Bristol, 1-19.

Karlof, C. and Wagner, D., 2003. Secure routing in wireless sensor networks: attacks and countermeasures. Ad Hoc Networks 1(2), 293-315.

Koldehofe B., Mayer R., Ramachandran U., Rothermel K., Völz M., 2013. Rollback-recovery without checkpoints in distributed event processing systems. 7th ACM international conference on Distributed event-based systems, ACM, 27-38.

Kotsiantis, S., Zaharakis, I., Pintelas, P., 2007. Supervised machine learning: a review of classification techniques. Frontiers in Artificial Intelligence and Applications, 249-268.

Meghdadi, M., Ozdemir, S. and Güler, I., 2011. A survey of wormhole-based attacks and their countermeasures in wireless sensor networks. IETE Technical Review 28(2).

NIST, 2014. Guidelines for Smart Grid Cybersecurity - Volume 1 - Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements. NISTIR 7628 Rev 1.

Pradhan S., Otte W., Abhishek D., Gokhale A., Gabor K., 2014. Towards a self-adaptive deployment and configuration infrastructure for cyber-physical systems. ISIS-14-102, 1-8.

Roman, R., Alcaraz, C., Lopez, J., 2007. A survey of cryptographic primitives and implementations for hardware-constrained sensor network nodes. Mobile Networks and Applications 12 (4), 231–244.

Ruchika, M., 2013. Schemes for surviving advanced persistent threats. Diss. Faculty of the Graduate School of the University at Buffalo, State University of New York.

Sadoddin R. and Ghorbani A., 2007. A comparative study of unsupervised machine learning and data mining techniques for intrusion detection. Machine Learning and Data Mining in Pattern Recognition, Springer, 404-418.

Scarfone, K. and Mell, P., 2007. Guide to intrusion detection and prevention systems. NIST Special Publication (800), 94.

Specht, S. M. and Lee, R. B., 2004. Distributed denial of service: taxonomies of attacks, tools, and countermeasures. ISCA PDCS, 543-550.

Stakhanova, N., Basu, S. and Wong, J., 2007. A taxonomy of intrusion response systems. International Journal of Information and Computer Security (1), 169-184.

Treaster, M., 2005. A survery of fault-tolerance and fault-recovery techniques in parallel systems. ACM Computing Research Repository, vol. 501002, 1-11.

Xing, K., Srinivasan, S. S. R., Jose, M., Li, J. and Cheng, X., 2010. Attacks and countermeasures in sensor networks: a survey, Network Security, Springer, 251-272.