Computer Standards & Interfaces 36 (2014) 501–512

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Diagnosis mechanism for accurate monitoring in critical infrastructure protection

Cristina Alcaraz *, Javier Lopez

Computer Science Department, University of Malaga, Campus de Teatinos s/n, 29071 Malaga, Spain

ARTICLE INFO

Article history:
Received 25 November 2012
Received in revised form 8 September 2013
Accepted 1 October 2013
Available online 25 October 2013

Keywords:
Critical infrastructure protection
Situational awareness
Industrial wireless sensor networks
The ISA100.11a standard
Accuracy

ABSTRACT

Wide-area situational awareness for critical infrastructure protection has become a topic of interest in recent years. As part of this interest, we propose in this paper a smart mechanism to: control real states of the observed infrastructure from anywhere and at any time, respond to emergency situations and assess the degree of accuracy of the entire control system. Particularly, the mechanism is based on a hierarchical configuration of sensors for control, the ISA100.11a standard for prioritization and alarm management, and the F-Measure technique to study the level of accuracy of a sensor inside a neighborhood.

1. Introduction

Being aware of a situation in critical contexts is currently a matter of utmost importance within the research field of Critical Infrastructure Protection (CIP). International organisations and experts are combining efforts to tackle the topic of situational awareness [1]. This is the case at the National Institute of Standards and Technology (NIST), which not only classifies this need in [2] as one of the eight priority areas for protection, but also defines it as a new concept denominated as Wide-Area Situational Awareness (WASA). WASA consists of controlling and optimizing system resources deployed over large geographic areas, as well as delivering smart solutions in charge of prevention and response before interruptions can arise within the system or between systems [2]. This means that it is necessary to address any type of instability, unforeseen event or potential fault caused by malicious actions [3] that may have a local, regional or national effect due to the existing interdependency relationships between Critical Infrastructures (CI) and their sectors [4]. According to the three latest reports of incidents in critical sectors published by the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) [5–7], these incidents (caused by failures or attacks) have become more and more prevalent in the last few years. Fig. 1, based on statistical values taken from [5–7], illustrates this increase where one of the most affected critical sectors is precisely the energy sector and its control systems, also known as Supervisory Control and Data Acquisition (SCADA) systems.

The consequences of this may be devastating with a high probability of triggering the famous cascading effect between critical systems. Therefore, Fig. 1 clearly shows why operative agents (e.g., human operators) should be made aware of these situations so as to anticipate anomalies or deliver a rapid response. Moreover, this degree of protection should be provided by standalone solutions with proactive and reactive capabilities that help the underlying system work alone, especially, at distant locations, where the control may be reduced to a few human operators in the field. Taking into account the criticality of the application context and the goals of WASA, our main contribution in this paper therefore is to provide a smart mechanism with the capability to offer interactive monitoring and protection of small control sub-domains, such as energy transmission/distribution substations. The mechanism is principally based on the technology of Industrial Wireless Sensor Networks (IWSN) as part of an observation and protection system. Nonetheless, as this technology and its sensory devices can have a significant tendency towards generating operational errors [8] caused by hardware or software failures or some type of threat [8–10], the proposed mechanism also controls the behaviour so as to determine the degree of accuracy in observation and protection tasks.

To compute this accuracy, topics relative to the accurate detection of and response to anomalous behaviour are addressed, together with aspects related to alarm management offered by current industry standards such as the ISA100.11a standard [11]. Any information produced within the observation system, has to be locally monitored by human operators in the field and remotely supervised by the SCADA Centre so as to be aware of the real state of both the underlying system and the protection system at all times. In order to validate the mechanism and show how it is able to offer an attractive way to deal with unforeseen situations and self-evaluate its functional capacities, a critical scenario is stressed (i.e., intentionally provoking emergency situations) to analyse the behaviour of the entire approach. The results show that this is a solution that could help the SCADA system know the real-state of its

* Corresponding author.
E-mail addresses: alcaraz@lcc.uma.es (C. Alcaraz), jlm@lcc.uma.es (J. Lopez).

0920-5489/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.csi.2013.10.002

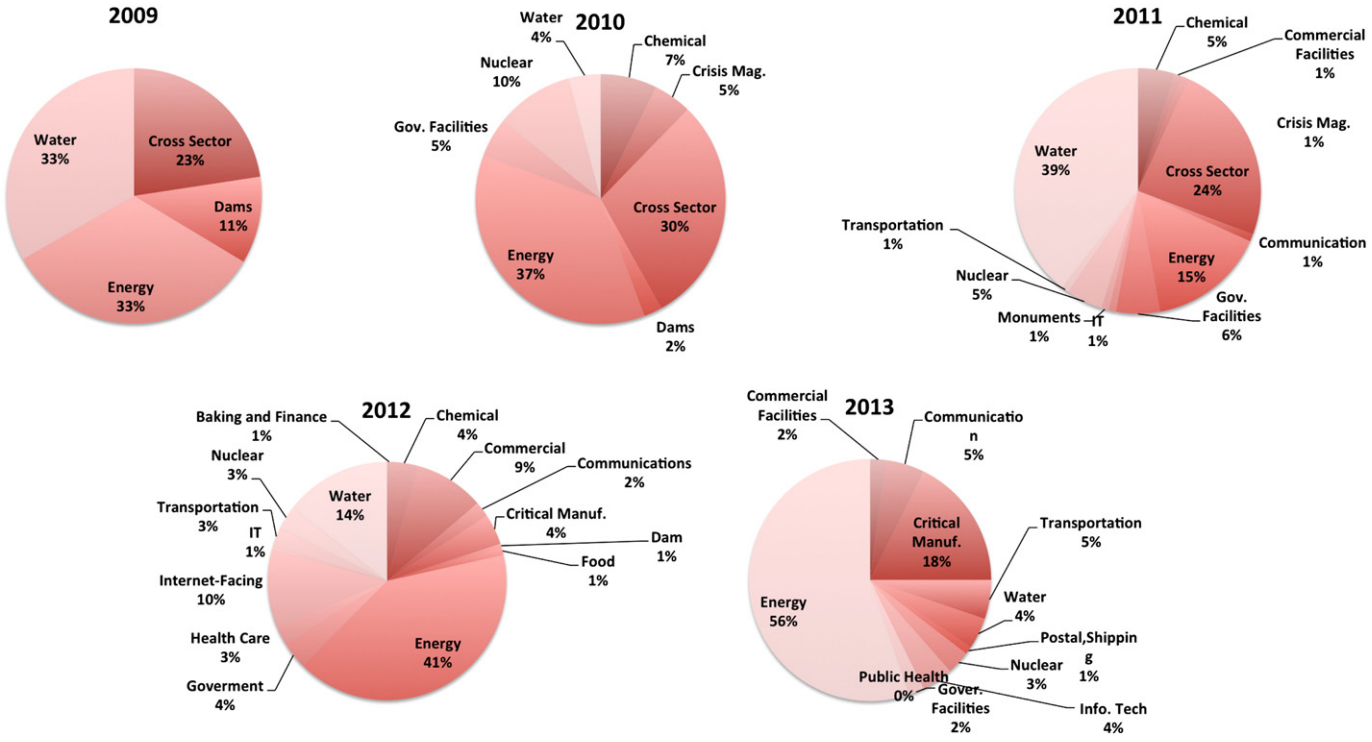

Fig. 1. Incidents reported by the ICS-CERT in [5–7].

components, and even improve its governance, risk management, auditing and maintenance as stated in [12].

The paper is organised as follows. Section 2 introduces related work, and Section 3 presents the general architecture and the functional goals of the WASA mechanism together with the technologies described above. Then, we introduce the solution in Section 4, describing the prevention method applied to control the reliability in the observation tasks. Section 5 analyses a use case based on the results obtained from the simulation where a software application is also introduced. Section 6 concludes the paper and outlines future work.

2. Related work

There are some experts in the CIP field that are currently developing attractive solutions [13–15] for CIP based on situational awareness. Most of these solutions follow similar architectural designs based on

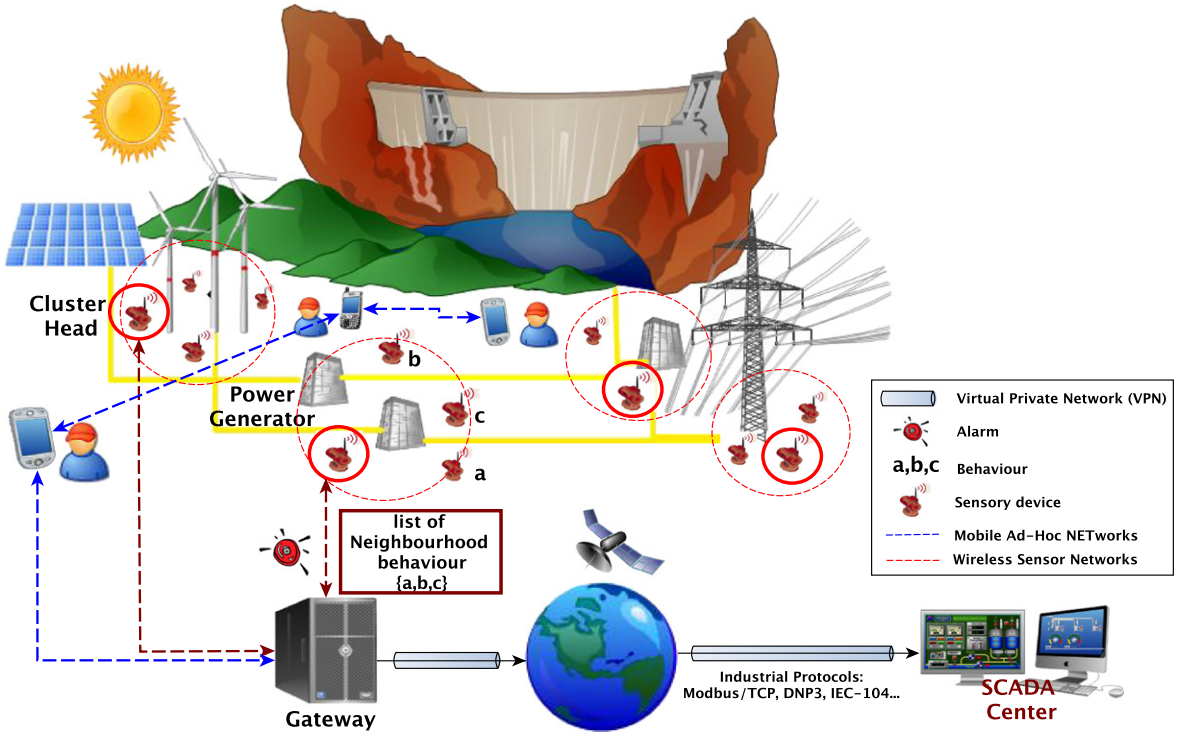

Fig. 2. General architecture of the WASA solution.