Available online at www.sciencedirect.com

SciVerse ScienceDirect

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

Computers & Security

Smart control of operational threats in control substations

Javier Lopez [a], Cristina Alcaraz [a,*], Rodrigo Roman [b]

[a] Computer Science Department, University of Malaga, Campus de Teatinos s/n, 29071 Malaga, Spain
[b] Institute for Infocomm Research, 1 Fusionopolis Way, #19-01 Connexis, South Tower, Singapore 138632, Singapore

ARTICLE INFO

Article history:
Received 17 November 2012
Received in revised form
16 February 2013
Accepted 12 March 2013

Keywords:
Smart Grids
Energy control systems
Wireless sensor networks
Reputation
Digital economy
Security

ABSTRACT

Any deliberate or unsuitable operational action in control tasks of critical infrastructures, such as energy generation, transmission and distribution systems that comprise subdomains 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 reliability 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.

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 (Tapscott, 1996). 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) (Tanaka, 2009). 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 and McNulty, 2001).

It is precisely because of their importance in keeping the digital economy alive, this paper focuses on energy systems.

* *Corresponding author*. Tel.: +34 649130337.
E-mail addresses: jlm@lcc.uma.es (J. Lopez), alcaraz@lcc.uma.es, c.alcaraz@ieee.org (C. Alcaraz), rroman@i2r.a-star.edu.sg (R. Roman).
0167-4048/$ – see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.cose.2013.03.013

More specifically, on energy systems belonging to the 21st century known as Smart Grids. According to the National Institute of Standards and Technology (NIST) conceptual model (NIST Special Publication 1108R2, 2012), 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 (Alcaraz and Lopez, 2012; Kotzanikolaou et al., 2013). Moreover, errors can result in a cascading effect with a high probability of a more catastrophic system breakdown (Reaves and Morris, 2012; Peerenboom and Fisher, 2007) 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 Fig. 1, makes these infrastructures an attractive target where adversaries could hamper the normal execution of critical services. In fact, various studies (cf. Nicholson et al., 2012) 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 Special Publication 1108R2, 2012; Federal Energy Regulatory Commission, 2009). 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 (Joo et al., 2009), 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 (Alcaraz and Lopez, 2012; Reaves and Morris, 2012), 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 (ISA, 2009, 2012). 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

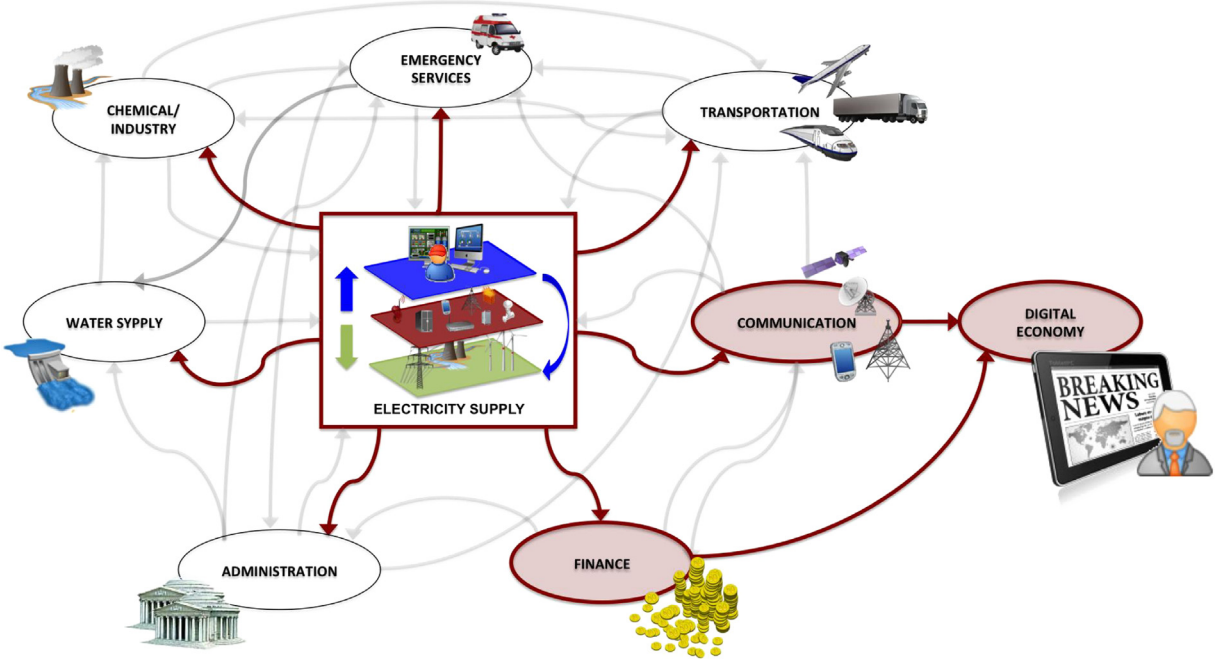

Fig. 1 – Interdependence relationships and impact on the digital economy.