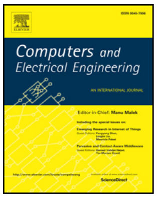
Computers and Electrical Engineering 000 (2017) 1–13

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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



Monitoring system reaction in cyber-physical testbed under cyber-attacks☆

Giuseppe Bernieri[a,*], Estefanía Etchevés Miciolino[b], Federica Pascucci[a], Roberto Setola[b]

[a] *Department of Engineering, Università degli Studi Roma Tre, Italy*
[b] *Complex Systems & Security Lab, University Campus Bio-Medico of Rome, Italy*

ARTICLE INFO

Article history:
Received 3 May 2016
Revised 12 February 2017
Accepted 13 February 2017
Available online xxx

Keywords:
Cyber-physical systems
SCADA system
Fault diagnosis
Networked control system
Communication network
IDS

ABSTRACT

In this paper, we exploit the cyber-physical testbed developed within the EU Project FACIES to analyze how monitor systems, typically used in Industrial Control Systems, may be prone to fail when facing cyber-attacks. Specifically, through several experimental trials, we test the poor ability of a Fault Diagnosis module to correctly manage cyber-attacks, which generally turn to be considered physical faults, forcing operators to perform erroneous countermeasures. To conclude, we outline how the presence of a cyber Intrusion Detection System improves the effectiveness and the reliability of the protection schema. The experimental validation has been carried out on an emulated water distribution system.

1. Introduction

In recent years, the Information and Communications Technology (ICT) evolution joined the Industrial Control Systems (ICSs) development, leading to new significant enhancements. After the first Supervisory Control And Data Acquisition (SCADA) *monolithic* systems, conceived in the 60s, the *networked* generation was born, which exploits TCP/IP (Transmission Control Protocol/Internet Protocol) infrastructure for remote monitoring and control [1]. Even though the benefits of the interaction of these two worlds are noticeable, new security challenges concerning industrial facilities arisen: typical vulnerabilities of the cyber domain emerged in ICSs. The classic cyber-security tools [2,3] are ineffective, since ICSs are designed to operate in standalone or isolated configurations and are characterized by hard real-time and bandwidth constraints. In the last decade, Critical Infrastructures (CIs) have experienced a large number of cyber-attacks, as reported by the ICS–CERT (Industrial Control System – Cyber Emergency Response Team) for the US [4]. The most famous example is *Stuxnet*, the first Programmable Logic Controller (PLC) rootkit targeting specific devices ever [5]. More recently, a serious cyber-event occurred in Ukraine in December 2015, when several power grids were exposed to organized cyber-attacks leading to diffuse power loss [6]. Despite the impact of such "alarms", the paramount importance of the information traveling in the SCADA system networks and its protection is still underestimated. As narrated in "Blackout" [7], cyber-attacks, successful in misleading the monitoring modules, may induce erroneous reactions from the operators.

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. J. Joaquin Garcia-Alfaro.

[*] Corresponding author.

E-mail addresses: giuseppe.bernieri@uniroma3.it (G. Bernieri), e.etcheves@unicampus.it (E. Etchevés Miciolino), federica.pascucci@uniroma3.it (F. Pascucci), r.setola@unicampus.it (R. Setola).

http://dx.doi.org/10.1016/j.compeleceng.2017.02.010
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

In literature, many works have demonstrated that the security of SCADA systems may benefit from the fusion of control engineering and ICT security. In this work, an analysis of the impact of cyber-attacks on the monitoring systems generally used for managing ICSs is presented. To this aim, several cyber-attacks against a realistic water system emulator, designed within the EU Project FACIES [8], are implemented. The impact of these attacks on a classical model-based Fault Diagnosis (FD) module supported by an Intrusion Detection System (IDS) is evaluated.

The remainder of the paper is structured as follows. Initially, a brief introduction of the related works is addressed in Section 2. In Section 3, the general model representing the dynamic behavior of Cyber-Physical Systems (CPS) is described, highlighting the interaction between the SCADA system and the monitored plant. The testbed employed as case study is introduced in Section 4, where its structure and its control architecture are detailed. Thereafter, the FD problem is addressed in Section 5, where the analytical model for the testbed and the FD module are shown. In Section 6, the cyber aspects are investigated, introducing models for the cyber-threats that have been developed according to the Control Theory perspective. Section 7 examines the methodology behind the experimental tests and analyzes the FD system response under cyber-attacks. Moreover, the role of a specific IDS is studied. Conclusions and future developments are discussed in Section 8.

2. Related work

The challenges of securing ICSs have been addressed in [9], where it is foreseen the development of innovative solutions encompassing both cyber and physical threats. One of the most important components of any SCADA system is the *Alarm Module*, which shows to the operator the presence of anomalous values in the monitored variables. As a result of the complexity of the system, operators are unable to continuously verify the consistence of the collected data. Hence, the *Alarm Module* is designed to compare the values acquired by the sensors with fixed thresholds, and to report back to the operator when the observed values exceed them. In some cases, several thresholds are associated with different levels of criticality, to provide information related to the entity of the detected anomaly.

As exposed in [10], the authors believe that the fusion between control engineering and ICT security could enforce the development of more sophisticated detection and reaction approaches against cyber-threats affecting ICSs. They have shown that by exploiting the physical model of the system it is possible to identify attacks. Due to the high level of automation of ICSs and the different faults/errors that physical components may encounter, more sophisticated tools, as Bad Data Detector (BDD) and FD systems, need to be implemented to automatically detect anomalous events and provide decision support to the operators. An essential asset of this analysis is the importance of investigating in which ways a model-based FD system reacts to cyber-attacks in real experimental stages. Such technology is becoming a priority in the design of intelligent and autonomous control systems, as it guarantees enhanced reliability, security, and availability for the systems. Both BDD and FD systems are designed to emphasize the presence of anomalies, having a global overview of all data acquired from the field rather than analyzing each single value. To this end, BDD and FD systems exploit the knowledge about the plant/infrastructure to reveal incoherent and inconsistent values. The main difference between them is that the first one is static, while the second one explicitly considers the system dynamics. On the one side, BDD systems exploit a state-observation model of the plant/infrastructure to infer the coherence of acquired measurements. On the other side, FD uses a dynamic model of the plant/infrastructure to identify operation anomalies.

In the literature, there are several studies aimed at analyzing the possible impact of cyber-attacks against BDD systems. In [11,12], it is shown how to design a cyber-attack that is no-detectable from the BDD systems (i.e., realizing a stealth attack). Conversely, less attention has been posed to detect cyber-attacks using FD modules. Cyber threats, indeed, are typically identified by modules such as IDSs, which passively analyze the network traffic [13].

3. General analytic model of a cyber-physical system

ICSs are CPSs characterized by being geographically distributed. In fact, an ICS system can be considered composed of a physical and a cyber structure, as schematically represented in Fig. 1. Specifically, the physical structure consists of the infrastructure/plant to be managed (e.g., all in-field devices), while the cyber structure encompasses the communication infrastructure and the elements used to supervise and manage the physical structure (e.g., the Human-Machine Interface – HMI). The physical structure can be generally modeled as a nonlinear uncertain discrete-time system, where physical and anomalous cyber-events are represented as disturbances to the state and output functions, formalized as:

$$\begin{aligned} x(k+1) &= f(x(k), \tilde{u}(k)) + \eta(x(k), d(k), \tilde{u}(k)) + w_s(k) \\ y(k) &= h(x(k)) + \Phi(x(k), d(k)) + w_o(k) \end{aligned}$$

where $k \in \mathbb{N}$ is the time instant, $x \in \mathbb{R}^n$ represents the state vector, $\tilde{u} \in \mathbb{Q}^m$ is the input vector (i.e., m is the number of actuators), in which the effects of malicious inputs injected by cyber-attacks are also considered, $f : \mathbb{R}^n \times \mathbb{Q}^m \to \mathbb{R}^n$ models the nominal dynamics, $d \in \mathbb{R}^p$ are the physical faults that can affect the system, $\eta : \mathbb{R}^n \times \mathbb{R}^p \times \mathbb{Q}^m \to \mathbb{R}^n$ is the cyber-physical attack/fault function affecting the state, $y \in \mathbb{R}^\nu$ is the output vector (i.e., ν is the number of sensors), $h : \mathbb{R}^n \to \mathbb{R}^\nu$ is the nominal output map, $\Phi : \mathbb{R}^n \times \mathbb{R}^p \to \mathbb{R}^\nu$ is the physical attack map affecting the output and $w_s \in \mathbb{R}^n$ and $w_o \in \mathbb{R}^\nu$ represent the model uncertainties and the noise vectors, respectively.

The plant, interacting with the SCADA/HMI, allows to perform control and monitoring actions. The general model of cyber actions generated by the SCADA can be expressed as: $u(k) = \beta(\tilde{y}(k), y_{ref}(k))$, where $\tilde{y} \in \mathbb{R}^\nu$ is the input vector for the