Journal of Process Control 24 (2014) 621–639

Contents lists available at ScienceDirect

Journal of Process Control

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

Experimental validation of a resilient monitoring and control system

Wen-Chiao Lin[a,1], Kris R.E. Villez[b], Humberto E. Garcia[a,*]

[a] Dynamic Systems Integration, Optimization, and Resilient Controls Group, Idaho National Laboratory, Idaho Falls, ID 83415-3570, USA
[b] Eawag Process Engineering, Überlandstrasse 133, P.O. Box 611, 8600 Dübendorf, Switzerland

ARTICLE INFO

Article history:
Received 24 October 2013
Received in revised form 7 March 2014
Accepted 7 March 2014
Available online 26 April 2014

Keywords:
Resilient monitoring and control systems
Experimental validation
Cyber-physical attacks
Health condition assessment
Hardware-in-the-loop
Adaptive supervisory controls
Fault detection
Identification
Accommodation

ABSTRACT

Complex, high performance, engineering systems have to be closely monitored and controlled to ensure safe operation and protect public from potential hazards. One of the main challenges in designing monitoring and control algorithms for these systems is that sensors and actuators may be malfunctioning due to malicious or natural causes. To address this challenge, this paper addresses a resilient monitoring and control (ReMAC) system by expanding previously developed resilient condition assessment monitoring systems and Kalman filter-based diagnostic methods and integrating them with a supervisory controller developed here. While the monitoring and diagnostic algorithms assess plant cyber and physical health conditions, the supervisory controller selects, from a set of candidates, the best controller based on the current plant health assessments. To experimentally demonstrate its enhanced performance, the developed ReMAC system is then used for monitoring and control of a chemical reactor with a water cooling system in a hardware-in-the-loop setting, where the reactor is computer simulated and the water cooling system is implemented by a machine condition monitoring testbed at Idaho National Laboratory. Results show that the ReMAC system is able to make correct plant health assessments despite sensor malfunctioning due to cyber attacks and make decisions that achieve best control actions despite possible actuator malfunctioning. Monitoring challenges caused by mismatches between assumed system component models and actual measurements are also identified for future work.

Published by Elsevier Ltd.

1. Introduction

1.1. Motivation

Complex high performance systems, such as chemical production plants, refineries, and power generation and transportation systems have to be closely *monitored* and *controlled* to ensure safe operation and protect the public from potential hazards. One of the main challenges in designing monitoring and control algorithms for these systems is that sensors and actuators may be malfunctioning due to natural or malicious causes. For example, if the monitoring system is connected to the some information network, false data may be injected to sensor measurements via cyber attacks. Likewise, valves regulating fluid flows in a cooling system may be stuck due to accumulation of deposits, corrosion, or other forms of wear-and-tear. This paper aims to develop a resilient monitoring and control (ReMAC) system, whose performance degrades gracefully under natural or malicious malfunctioning of sensors and actuators. In particular, we expand previously developed resilient condition assessment monitoring systems [1] and Kalman filter-based diagnosis algorithms [2] and integrate them with a supervisory control mechanism developed here. While the monitoring and diagnostic algorithms assess plant (cyber and physical) health conditions, the supervisory controller selects, from a set of candidates, the best controller based on these health assessments. The developed ReMAC system is then experimentally demonstrated on a chemical reactor with a water cooling system in a hardware-in-the-loop (HiL) setting, where the reactor is computer simulated and the water cooling system is implemented by a machine condition monitoring (MCM) testbed at Idaho National Laboratory (INL).

1.2. Review of related work

Research on resilient systems is a relatively new subject and recent work on resilient systems can be found in [3–14,1,15–19,2]. In particular, [3] provides collections of papers that treat resilience engineering as a paradigm for safety management that focuses on “how to help people cope with complexity under pressure to achieve success.” These papers explore different facets of resilience as “the ability to anticipate and adapt to the potential for surprise and failure.” Based on these work, [5] further identifies four

[*] Corresponding author. Tel.: +1 2085267769; fax: +1 2085263150.
[1] W.-C. Lin has moved to General Motors Company.

http://dx.doi.org/10.1016/j.jprocont.2014.03.006
0959-1524/Published by Elsevier Ltd.

cornerstones of resilience as knowing "what to do," "what to look for," "what to expect," and "what has happened."

Relations between resilience and robustness have been investigated. For example, [6] addresses different fire-prone ecological systems and suggests that robustness tradeoffs in these systems demonstrate resilience. In [7], resilient control systems that emphasize control design in an adversarial and uncertain cyber environment (as opposed to physical disturbances) are developed. This control design is viewed as pivoting on the tradeoff between robustness and resilience. Optimality criteria are proposed for tradeoff between robustness and resilience in modern industrial control systems.

Further developments of resilient systems with uncertain cyber environments can be found in [8,9]. Specifically, [8] provides a conceptual framework and brief overview of the architectural considerations for designing systems that operate in hostile cyber environment with uncertainties in complex networks and human interactions. The work in [9] develops an intelligent resilient control algorithm for a wireless networked control system based on quantification of the concept of resiliency in terms of quality of control. Here, resiliency maintains normal operations in the face of wireless interference incidents. Ref. [10] further uses the quality of control for designing resilient control strategies for model-based building control, improving building automation systems.

Resilient systems have also been considered regarding security issues in, for example, [11,12]. While [11] describes experiences and success in cyber security programs leading to more robust, secure, and resilient monitoring and control systems in industrial assets, [12] discusses security-related definitions for resilience, which includes integrity and confidentiality in addition to availability.

Developments of resilient systems for computer systems and for monitoring critical infrastructures can be found, for instance, in [13,14]. In particular, in [13], metadata-based resilience policies are enforced to design computing systems that can dynamically adapt in a predictable way to unexpected events. In [14], basic paradigms are proposed for integration of diverse fault detection and identification methods and control methods for achieving resilience in critical infrastructures.

This work builds on the resilient monitoring systems developed in [4,1,15–19] and Kalman filter-based diagnosis methods in [2]. In [4,1], it is assumed that a set of sensors observing process variables are deployed throughout a monitored plant, which is subject to process disturbances (e.g., unplanned, random process anomalies and deliberate, non-random physical attacks). Likewise, the sensors are subject to disturbances (e.g., unplanned, random sensor faults and failures and cyber-attacks), which cause them to project false data/observations. Although [4] and [1] developed similar monitoring architectures, the design approaches for the components are different. In particular, the monitoring system designed in [1] aims at selecting sensors to make plant health assessments within desired time periods despite cyber attacks, while that in [4] focuses on selecting sensor configurations to maximize plant health assessment confidence. Moreover, some advantages are also afforded by the approach considered in [1], such as faster computations of the monitored plant assessments. Following this line of work, [15] developed an active probing method for sensor data quality assessment. Integration of the active probing method into the resilient monitoring structure is documented in [16], while [17,18] consider application of the developed monitoring system to simplified power plants consisting of a boiler and a turbine. Reference [19], extending the work in [1], developed game-theoretic formulations for resilient monitoring systems that improve monitoring performance when natural or malicious sensor malfunctioning is incorrectly characterized.

The Kalman-filter based fault detection identification (FDI) method as applied here was first presented in [2]. In essence, this method is based on the key observation that the expected values of one-step ahead prediction residuals obtained by means of the Kalman filter are unique for fault type (e.g., bias, drift), fault location (affected actuator, process or sensor), and magnitude (e.g., bias magnitude). To obtain high sensitivity and specificity, the method requires that a reliable model is available. Alternative diagnostic methods are available when this is a challenging requirement, either based on data mining tools (e.g., [20] or on course-grained system and/or data representations (e.g., [21,22]).

This paper integrates the work in [1,2] with a supervisory control algorithm for developing a resilient monitoring and control algorithm. Note that, while the work in [1] aims at assessing the overall monitored plant conditions, the algorithms in [2] determine the health of monitored plant components. Hence, in the following, we will refer to methods in [1,2] as systems- and component-centric, respectively.

1.3. Main contributions and organization of paper

The main contributions of this paper include the following.

- Development of a resilient monitoring and control (ReMAC) system that combines previously developed systems- and component-centric monitoring algorithms [1,2] with supervisory control methods.
- Application of the developed ReMAC system to a chemical reactor with a water cooling system in an HiL setting, where the reactor is computer simulated and the water cooling system is implemented by an MCM testbed at INL.

As this paper is on experimental verification of the developed algorithms, we focus more on describing the background knowledge, experimental setups, scenarios considered, and simulation results. Whenever appropriate, references are given for readers who wish to read the theory and analysis in more detail. The rest of this paper is organized as follows. Section 2 introduces the overall architecture of the developed ReMAC system, while Section 3 describes the algorithms implementing constituent components of it. The monitored plant considered is detailed in Section 4. Implementation of the ReMAC system for the monitored plant considered and simulation results are given in Sections 5 and 6, respectively. Finally, Section 7 concludes the paper and describes future work.

2. Monitoring architecture

This section describes the architecture of the developed resilient monitoring and control (ReMAC) system, shown in Fig. 1.

In particular, we consider a monitored plant, which is subject to physical disturbances (e.g., process anomalies). A set of sensors are deployed to observe the plant process variables, while a set of regulatory controllers regulate the plant via actuators. The sensors and actuators are subject to natural or malicious disturbances, such as cyber attacks (e.g., injecting false data to the sensors) or physical disturbances (e.g., decreased efficiency due to aging in a pump). In view of sensor disturbances, a scalar, referred to as the data quality (DQ), is dynamically assigned to quantify the trustworthiness of its reported measurement. While recent work has developed active methodologies for assigning sensor DQs [15–17], this paper does not address this particular element. Instead, the monitoring systems considered in this work assume that sensor DQs are computed by a watch dog system, which assign sensor data qualities based on, e.g., cyber attack assessments, sensor data traffic, or state estimation comparisons. The sensor signals are used in a Kalman