Annual Reviews in Control 38 (2014) 47–70

Contents lists available at ScienceDirect

Annual Reviews in Control

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

Integrated monitoring, control and security of Critical Infrastructure Systems

Mietek A. Brdys *

Department of Electronic, Electrical and Computer Engineering, College of Engineering and Physical Sciences, University of Birmingham, Edgbaston, Birmingham B15 2TT, UK
Department of Control Systems Engineering, Gdansk University of Technology, ul. G. Narutowicza 11/12, 80-233 Gdansk, Poland

ARTICLE INFO

Article history:
Received 18 September 2013
Accepted 15 February 2014
Available online 18 April 2014

ABSTRACT

Modern societies have reached a point where everyday life relies heavily on desired operation of critical infrastructures, in spite of accidental failures and/or deliberate attacks. The issue of desired performance operation of CIS at high security level receives considerable attention worldwide. The pioneering generic methodologies and methods are presented in the paper project for designing systems capable of achieving these objectives in the cost effective manner at existing CIS and also in the future. A control systems engineering approach to integrated monitoring, control and security of critical infrastructure systems (CIS) is applied. A multilayer structure for an intelligent autonomous reconfigurable agent operating within a single region of a CIS is derived first. Methods and algorithms for synthesising the layers are proposed so that the agent can autonomously perform required control activities under wide range of operating conditions. The required ability of the system to meet the desired operational objectives under a wide range of the operating conditions is achieved by supervised reconfiguration of the agents. Recently proposed robustly feasible model predictive control technology with soft switching mechanisms between different control strategies is applied to implement the soft and robustly feasible agent reconfiguration, which is adequate to current operational conditions. Next developing the multiagent structures, which are suitable for monitoring, control and security of an overall CIS is discussed. It is based on the distributed structuring the agent layers. The proposals are illustrated by applications to the integrated wastewater treatment case-study system and drinking water distribution system.

1. Introduction

Control and operational management of CIS must secure their reliable and sustainable functioning in achieving the required operational objectives under *wide range* of operational conditions, which include accidental seriously unfavourable events such as sensor and or actuator faults, failures of communication links or anomalies occurring in technological operation of the CIS physical processes. A *monitoring system* is needed in order to deliver information. The CIS are subject to deliberate attacks. The inputs resulting from these attacks can seriously deteriorate required functioning of the CIS. The early detection of such disturbance inputs, compensation/rejection of their impact and restoration of the CIS back to its normal operation requires actions from a dedicated *security system*. The security system can be viewed as a dedicated control system to handle the special type of the disturbance inputs. This is depicted in Fig. 1.

Utilising and integrating the monitoring and control facilities, which are adequate to maintain a desired performance of CIS operating under normal conditions to support the monitoring and control security facilities is vital for achieving desired high operational and cost effective performance of the security system under the failures and deliberate attacks.

The CIS are spatially distributed and of a network structure. The dynamics is nonlinear, uncertain and with several time scales. There is large number of variables involved in the dynamics model which is heterogeneous. Not only the inputs but also states/outputs are constrained. The latter requires robust feasibility of the control actions generated by control units. Hence, the CIS are large scales complex systems with variety of different objective to be met under wide range of operational conditions (see Fig. 2).

The CIS are typically distributed over a large geographical area and a centralised system for performing the monitoring, control and security functions would not be viable. Therefore, the area is decomposed into the regions as shown in Fig. 3. Performing the integrated monitoring, control and security functions over the

* Address: Department of Electronic, Electrical and Computer Engineering, College of Engineering and Physical Sciences, University of Birmingham, Edgbaston, Birmingham B15 2TT, UK.

E-mail addresses: m.brdys@bham.ac.uk, mbrdys@ely.pg.gda.pl

http://dx.doi.org/10.1016/j.arcontrol.2014.03.006
1367-5788/© 2014 Elsevier Ltd. All rights reserved.

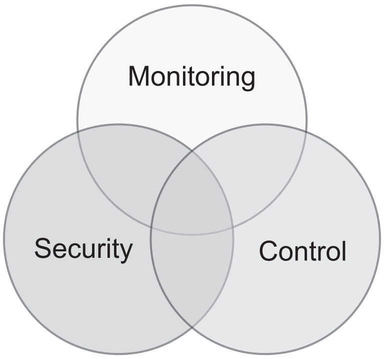

Fig. 1. Key interacting components of the system maintaining operation of CIS.

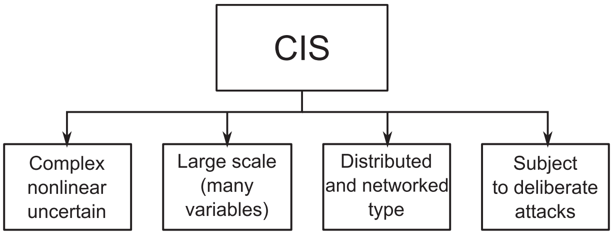
CIS
Complex nonlinear uncertain
Large scale (many variables)
Distributed and networked type
Subject to deliberate attacks

Fig. 2. CIS are large scale complex systems.

regions is conducted by the regional agents. These are the intelligent units of high autonomy interacting directly or/and through the CIS as illustrated in Fig. 4.

The paper is organised as follows. In Section 2 the CIS operational states are introduced in order to capture different operational conditions including activities of the attacking agents. Then they are mapped into the control strategies, suitable to pursue the control objectives, which can realistically be achieved at these states. The model predictive control (MPC) technology is applied to design the control strategies. The robustly feasible strategies (RFMPC) are outlined in Section 3. A reconfiguration of an agent in order to adapt the control strategy to a current operational state of the CIS is discussed in Section 4. A soft switching mechanism between different RFMPC strategies is proposed to produce the softly switched robustly feasible MPC (SFRFMPC) that implements soft reconfiguration of the agent. An approach to derive a multiagent control system over an overall CIS based on the derived architecture and algorithms for a regional agent is briefly discussed in Section 5. An application to the integrated wastewater treatment system case study CIS is presented in Section 6. An application to quality control in the case study example of drinking water distribution network is described in the Sections 7 and 8. The conclusions in Section 9 complete the paper.

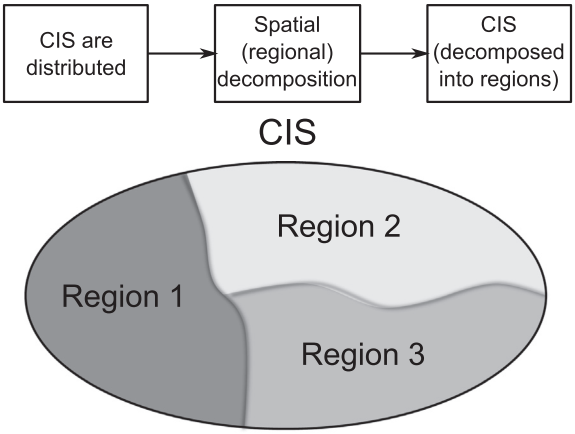
CIS are distributed
Spatial (regional) decomposition
CIS (decomposed into regions)
CIS
Region 1
Region 2
Region 3

Fig. 3. Spatial decomposition of CIS into regions.

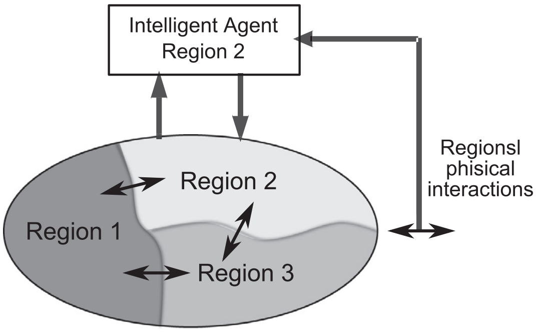

Fig. 4. Regional agents.

2. Operational states and control strategies

2.1. Approach

A current *operational state* (OS) of a CIS is determined by the states of all the factors which influence its ability to achieve prescribed control objectives. These include: states of the CIS processes; states of the sensors, actuators and communication channels (e.g., faults), states of process anomalies, technical faults, current operating ranges of the processes, states of the disturbance inputs. The OS without security content (not security OS) are robustly estimated/predicted by using conventional state estimation algorithm (data driven, model based) and fault detection and diagnosis algorithms (FDD) (Duzinkiewicz et al., 2008; Gertler, 1998). The typical operational states are Brdys, Grochowski, Gminski, Konarczak, and Drewa (2008): *normal*, *disturbed* and *emergency*. Not all control objectives can be satisfactorily achieved at a specific OS. This is identified by performing a suitable a prior analysis. Given the control objectives a control strategy suitable to achieve these objectives is designed or chosen from the set of strategies designed a prior. In this way a mapping between the operational states and suitable control strategies to be applied at these OS is produced (see Fig, 5). It should be pointed out that there can be more than one normal, disturbed and emergency operational state and they constitute the separated clusters in the OS space equipped with the links indicating transfer between the specific operational states. In a triple of ordered and linked of the normal, perturbed and emergency operational states, a deterioration of CIS operational conditions forces the CIS to move into the perturbed operational state. The control system is expected to adapt its current control strategy to the new operational state as otherwise the CIS with not adequate control strategy in place can be further forced to move into the emergency operational state. Being safely

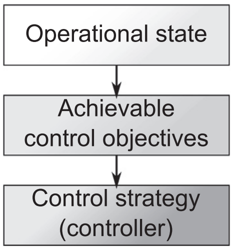

Fig. 5. Mapping operational states into control strategies.