Studies in Computational Intelligence 565

Elias Kyriakides
Marios Polycarpou *Editors*

Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems

cost
EUROPEAN COOPERATION IN SCIENCE AND TECHNOLOGY

Springer

Elias Kyriakides · Marios Polycarpou
Editors

Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems

Springer

Editors
Elias Kyriakides
Marios Polycarpou
KIOS Research Center for Intelligent
Systems and Networks
Department of Electrical and Computer
Engineering
University of Cyprus
Nicosia
Cyprus

ISSN 1860-949X
ISBN 978-3-662-44159-6
DOI 10.1007/978-3-662-44160-2

ISSN 1860-9503 (electronic)
ISBN 978-3-662-44160-2 (eBook)

Library of Congress Control Number: 2014948739

Springer Heidelberg New York Dordrecht London

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Studies in Computational Intelligence

Volume 565

Series editor

Janusz Kacprzyk, Polish Academy of Sciences, Warsaw, Poland
e-mail: kacprzyk@ibspan.waw.pl

About this Series

The series "Studies in Computational Intelligence" (SCI) publishes new developments and advances in the various areas of computational intelligence—quickly and with a high quality. The intent is to cover the theory, applications, and design methods of computational intelligence, as embedded in the fields of engineering, computer science, physics and life sciences, as well as the methodologies behind them. The series contains monographs, lecture notes and edited volumes in computational intelligence spanning the areas of neural networks, connectionist systems, genetic algorithms, evolutionary computation, artificial intelligence, cellular automata, self-organizing systems, soft computing, fuzzy systems, and hybrid intelligent systems. Of particular value to both the contributors and the readership are the short publication timeframe and the world-wide distribution, which enable both wide and rapid dissemination of research output.

More information about this series at http://www.springer.com/series/7092

COST Information

COST—the acronym for European Cooperation in Science and Technology—is the oldest and widest European intergovernmental network for cooperation in research. Established by the Ministerial Conference in November 1971, COST is presently used by the scientific communities of 35 European countries to cooperate in common research projects supported by national funds.

The funds provided by COST—less than 1% of the total value of the projects—support the COST cooperation networks (COST Actions) through which, with €30 million per year, more than 30,000 European scientists are involved in research having a total value which exceeds €2 billion per year. This is the financial worth of the European added value which COST achieves.

A "bottom up approach" (the initiative of launching a COST Action comes from the European scientists themselves), "à la carte participation" (only countries interested in the Action participate), "equality of access" (participation is open also to the scientific communities of countries not belonging to the European Union) and "flexible structure" (easy implementation and light management of the research initiatives) are the main characteristics of COST.

As a precursor of advanced multidisciplinary research COST has a very important role for the realization of the European Research Area (ERA) anticipating and complementing the activities of the Framework Programs, constituting a "bridge" toward the scientific communities of emerging countries, increasing the mobility of researchers across Europe, and fostering the establishment of "Networks of Excellence" in many key scientific domains such as: Biomedicine and Molecular Biosciences; Food and Agriculture; Forests, their Products and Services; Materials, Physical and Nanosciences; Chemistry and Molecular Sciences and Technologies; Earth System Science and Environmental Management; Information and Communication Technologies; Transport and Urban Development; Individuals, Societies, Cultures and Health. It covers basic and more applied research and also addresses issues of pre-normative nature or of societal importance.

Web: http://www.cost.eu

Preface

Modern society relies on the availability and smooth operation of a variety of complex engineering systems. These systems are termed *Critical Infrastructure Systems*. Some of the most prominent examples of critical infrastructure systems are electric power systems, telecommunication networks, water distribution systems, transportation systems, wastewater and sanitation systems, financial and banking systems, food production and distribution, health, security services, and oil/natural gas pipelines. Our everyday life and well-being depend heavily on the reliable operation and efficient management of these critical infrastructures.

The citizens expect that critical infrastructure systems will always be available, 24 hours a day, 7 days a week, and at the same time, they will be managed efficiently so that the services are provided at a low cost. Experience has shown that this is most often true. Nevertheless, critical infrastructure systems fail occasionally. Their failure may be due to natural disasters (e.g., earthquakes and floods), accidental failures (e.g., equipment failures, software bugs, and human errors), or malicious attacks (either direct or remote). When critical infrastructures fail, the consequences are tremendous. These consequences may be classified into societal, health, and economic. For example, if a large geographical area experiences a blackout for an extended period of time, that may result in huge economic costs, as well as societal costs. In November 2006, a local fault in Germany's power grid cascaded through large areas of Europe, resulting in 10 million people left in the dark in Germany, France, Austria, Italy, Belgium, and Spain. Severe cascading blackouts have taken place in North America as well. Similarly, there may be significant health hazards when there is a serious fault in the water supply, especially if it is not detected and accommodated quickly. When the telecommunication networks are down, many businesses can no longer operate. In the case of faults or unexpected events in transportation systems, we witness the effect of traffic congestion quite often in metropolitan areas of Europe and around the world. In general, failures in critical infrastructure systems are low probability events, which however may have a huge impact on everyday life and well-being.

Technological advances in sensing devices, real-time computation and the development of intelligent systems, have instigated the need to improve the

performance of critical infrastructure systems in terms of security, accuracy, efficiency, reliability, and fault tolerance. Consequently, there is a strong effort in developing new algorithms for monitoring, control, and security of critical infrastructure systems, typically based on computational intelligence techniques and the real time processing of data received by networked embedded systems and sensor/actuator networks, dispersed throughout the system. Depending on the application, such data may have different characteristics: multidimensional, multiscale, spatially distributed, time series, event-triggered, etc. Furthermore, the data values may be influenced by controlled variables, as well as by external environmental factors. However, in some cases the collected data may be incomplete, or it may be faulty due to sensing or communication problems, thus compromising the sensor-environment interaction and possibly affecting the ability to manage and control key variables of the environment.

Despite the technological advances in sensing/actuation design and data processing techniques, there is still an urgent need to intensify the efforts towards intelligent monitoring, control, and security of critical infrastructure systems. The problem of managing critical infrastructure systems is becoming more complicated since they were not designed to be so large in size and geographical distribution; instead, they evolved due to the growing demand, while new technologies have been combined with outdated infrastructures in a single system that is required to perform new and more complex tasks. Furthermore, deregulation and the new market structure in several of these infrastructures has resulted in more heterogeneous and distributed infrastructures, which make them more vulnerable to failures and attacks. The introduction of renewable energy sources and environmental issues have incorporated new objectives to be met and new challenges in the operation and economics of some of these infrastructures (for example, power systems, telecommunication, water distribution networks, and transportation).

Two important notions that captivate the attention of researchers and of the industry are the concepts of *cyber-physical systems* and *system of systems*. Cyber-physical systems are the result of the interconnection and interaction of the cyber (computation) and the physical elements in a system. Embedded sensors, computers, and networks monitor and collect data from the physical processes; in turn, it is possible to control the physical processes through the analysis and use of the data collected to take appropriate actions for retaining the stability and security of the system.

The system of systems concept arose from the interconnection of independent systems in a larger, more complex system. These formerly independent systems may now be interacting or be interdependent. There are dependencies between infrastructures (e.g., a fault in the power system removes the supply to a water pump and thus, the water supply to an area), or in some cases interdependencies (e.g., a fault in the power system causes the oil/natural gas pipeline pumping stations to stop working, and as a consequence the supply of fuel to the power station is interrupted). Critical infrastructure dependencies and interdependencies pose an even higher degree of complexity, particularly on the appropriate modeling and simulation of the effects that one infrastructure has on another

infrastructure. The fact that fewer people nowadays understand how these networks operate and the interactions between all the components, creates a necessity for further research and in-depth analysis of the various infrastructures.

Given the current challenges faced by critical infrastructures and given that it is not realistic to consider rebuilding them from scratch, it is necessary to derive approaches and develop methods to transform and optimize these infrastructures through the use of instrumentation, embedded software, and "smart" algorithms. In the global effort towards developing a more systematic and efficient approach for all critical infrastructures, it is useful to consider that these systems have some common characteristics. Critical infrastructure systems are safety critical systems that are complex in operation, spatially distributed, dynamic, time-varying, and uncertain. There is a wealth of data that can be obtained from various parts of these systems. Their dynamics have significant similarities in their analysis, while the effects of faults or disturbances can be modeled in similar ways.

This book was motivated by the European Science Foundation COST Action *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems* IC0806 (IntelliCIS) and is supported by the COST (European Cooperation in Science and Technology) Office. The book aims at presenting the basic principles as well as new research directions for intelligent monitoring, control, and security of critical infrastructure systems. Several critical infrastructure application domains are presented, while discussing the key challenges that each is facing. Appropriate state-of-the-art algorithms and tools are described that allow the monitoring and control of these infrastructures, based on computational intelligence and learning techniques. Some of the book chapters describe key terminology in the field of critical infrastructure systems: risk evaluation, intelligent control, interdependencies, fault diagnosis, and system of systems.

The Chapter "Critical Infrastructure Systems—Basic Principles of Monitoring, Control, and Security" provides an overview of critical infrastructure systems. It describes the basic principles of monitoring, control, and security and sets the stage for the rest of the book chapters. Chapters "Electric Power Systems", "Telecommunication Networks", "Water Distribution Networks", and "Transportation Systems: Monitoring, Control, and Security" concentrate on four key critical infrastructure systems: electric power systems, telecommunication networks, water distribution networks, and transportation systems. Their basic principles and key challenges are described.

Chapters "Algorithms and Tools for Intelligent Monitoring of Critical Infrastructure Systems", "Algorithms and Tools for Intelligent Control of Critical Infrastructure Systems", and "Algorithms and Tools for Risk/Impact Evaluation in Critical Infrastructures" focus on algorithms and associated tools for intelligent monitoring, control, and security of critical infrastructure systems, as well as risk/impact evaluation. The chapters provide the necessary theory, but also provide real life examples in the application of these tools and methodologies.

The Chapter "Infrastructure Interdependencies—Modeling and Analysis" presents several approaches for modeling critical infrastructure interdependencies. The Chapter "Fault Diagnosis and Fault Tolerant Control in Critical Infrastructure

Systems" provides a theory-based overview of fault diagnosis and fault tolerant control in critical infrastructure systems and illustrates the application of these methodologies in the case of water distribution networks.

The Chapter "Wireless Sensor Network Based Technologies for Critical Infrastructure Systems" examines the role of telecommunication networks in supporting the monitoring and control of critical infrastructure applications. The physical network is examined, as well as reliability and security issues. The Chapter "System-of-Systems Approach" concentrates on the reliability, security, risk, and smart self-healing issues in critical infrastructures, viewed from a system of systems perspective. The interdependencies between systems are examined with a focus on the electric power grid. Finally, the Chapter "Conclusions" discusses the main attributes that a future critical infrastructure system is expected to have and provides some potential future research directions in the areas of intelligent monitoring, control, and security of critical infrastructure systems.

Contents

Critical Infrastructure Systems: Basic Principles of Monitoring, Control, and Security

Georgios Ellinas, Christos Panayiotou, Elias Kyriakides and Marios Polycarpou

Abstract Critical Infrastructures have become an essential asset in modern societies and our everyday tasks are heavily depended on their reliable and secure operation. Critical Infrastructures are systems and assets, whether physical or virtual, so vital to the countries that their incapacity or destruction would have a debilitating impact on security, national economy, national public health or safety, or any combination of these matters. Thus, monitoring, control, and security of these infrastructures are extremely important in order to avoid the disruption of their normal operation (either due to attacks, component faults, or natural disasters) or to ensure that the infrastructure continues to function after a failure event. This chapter aims at presenting the basic principles and new research directions for the intelligent monitoring, control, and security of critical infrastructure systems.

Keywords Control systems · Critical infrastructure systems · Electric power systems · Fault diagnosis · Monitoring · Security · Telecommunication networks · Transportation systems · Water distribution networks

G. Ellinas (✉) · C. Panayiotou · E. Kyriakides · M. Polycarpou
KIOS Research Center for Intelligent Systems and Networks, Department of Electrical and Computer Engineering, University of Cyprus, 1678 Nicosia, Cyprus
e-mail: gellinas@ucy.ac.cy

C. Panayiotou
e-mail: christosp@ucy.ac.cy

E. Kyriakides
e-mail: elias@ucy.ac.cy

M. Polycarpou
e-mail: mpolycar@ucy.ac.cy

E. Kyriakides and M. Polycarpou (eds.), *Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems*, Studies in Computational Intelligence 565,
DOI 10.1007/978-3-662-44160-2_1

1 Introduction

Everyday life relies heavily on the reliable and secure operation and intelligent management of large-scale critical infrastructures and any destruction or disruption of these infrastructures would cause tremendous consequences and will have a debilitating impact on security, national economy, national public health or safety, or any combination of these matters [1]. Specifically, critical infrastructures are defined as "*assets, systems, or parts thereof, essential for the maintenance of vital societal functions, health, safety, security, economic, or social well-being*" [2]. Thus, citizens nowadays expect that critical infrastructures will always be available and that they will be managed efficiently (with low cost).

Examples of Critical Infrastructures (CIs) include, amongst others, the electrical power plants and the national electrical grid, oil and natural gas systems, telecommunication and information networks, transportation networks, water distribution systems, banking and financial systems, healthcare services, and security services. Figure 1 shows the South East Asia—Middle East—Western Europe 4 (SEA-ME-WE 4) undersea fiber-optic transport network as an example of a (telecommunications) critical infrastructure. SEA-ME-WE 4 is a fiber-optic cable system approximately 19,000 km long that is used to carry information (providing the primary Internet backbone) between South East Asia, the Indian subcontinent, the Middle East, and Europe. This cable connects a large number of countries and is used to carry telephone, Internet, multimedia, and various broadband data applications utilizing a data transmission rate of 1.28 Tbps.

The monitoring, control, and security of critical infrastructure systems are becoming increasingly more challenging as their size, complexity, and interactions are steadily growing. Moreover, these critical infrastructures are susceptible to natural disasters (such as earthquakes, fires, and flooding), frequent faults (e.g., equipment faults, human error, software errors), as well as malicious attacks (directly or remotely) (Figure 2 shows possible threats to critical infrastructures).

There is thus an urgent need to develop a common framework for modeling the behavior of critical infrastructure systems and for designing algorithms for intelligent monitoring, control, and security of such systems. This chapter aims at presenting the basic principles and new research directions for the intelligent monitoring, control, and security of critical infrastructure systems. Subsequent chapters in this book provide more specific information on the monitoring and control of particular infrastructures such as Electric Power Systems (Chapter "Electric Power Systems"), Telecommunication Networks (Chapter "Telecommunication Networks"), Water Distribution Networks (Chapter "Water Distribution Networks"), and Transportation Systems (Chapter "Transportation Systems: Monitoring, Control, and Security"). Additional information on algorithms and tools for CI monitoring and control, as well as on critical infrastructure interdependencies are included in later chapters. In particular, Chapters "Algorithms and Tools for Intelligent Monitoring of Critical Infrastructure Systems," "Algorithms and Tools for Intelligent Control of Critical Infrastructure Systems," and "Algorithms and Tools for Risk/Impact Evaluation in Critical

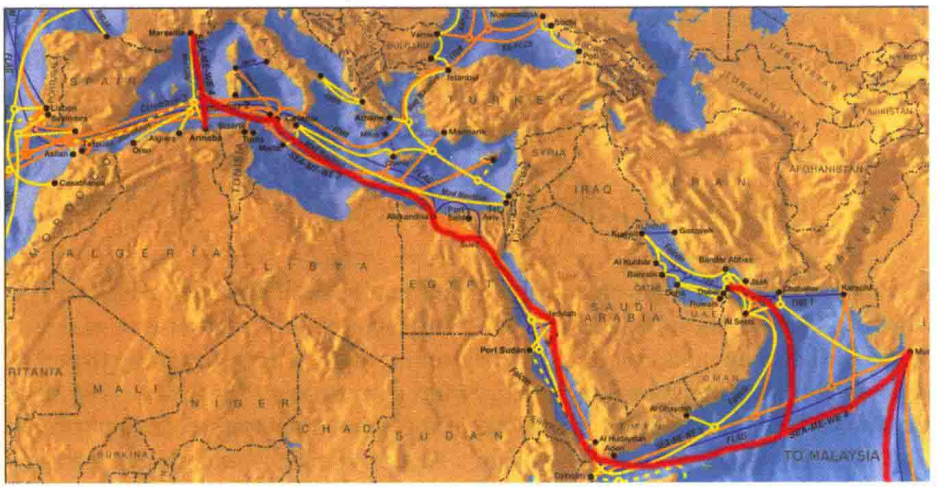

Fig. 1 SEA-ME-WE 4 undersea fiber-optic cable system (in *bold*) as an example of a (telecommunications) critical infrastructure

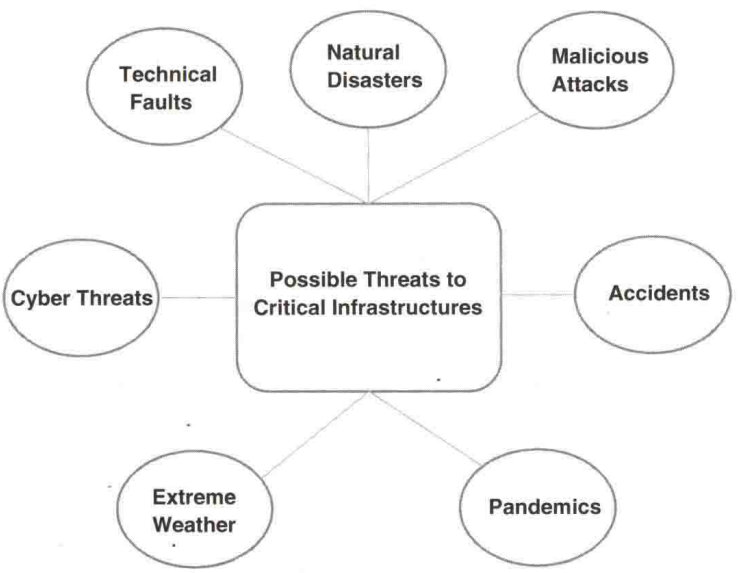

Fig. 2 Threats to critical infrastructures

Infrastructures" describe different algorithms and tools for intelligent monitoring and control and for risk/impact evaluation of CIs, while Chapter "Fault Diagnosis and Fault Tolerant Control in Critical Infrastructure Systems" addresses specifically the problems of fault diagnosis and fault tolerance control in critical infrastructure systems. In addition, Chapter "Infrastructure Interdependencies: Modeling and Analysis" discusses modeling and analysis of infrastructure interdependencies, Chapter "Wireless Sensor Network Based Technologies for Critical Infrastructure Systems"

describes wireless sensor network based technologies for CIs and Chapter "System-of-Systems Approach" presents a system-of-systems approach for the intelligent monitoring, control, and security of critical infrastructures.

2 Disruption of Critical Infrastructures

A *failure event* in CIs (accidental or intentional) is defined as a negative event which influences the *inoperability* of infrastructures and subsystems, where the inoperability of an infrastructure or subsystem is defined as the inability to perform its intended function. An example of a failure event in the CI shown in Fig. 1 was the January 2008 accidental destruction of the submarine system's fiber-optic link (speculated to have happened by a ship's anchor outside Alexandria's port). As a result of this accident, Internet services were widely disrupted in the Middle East and in the Indian subcontinent, including more than 50 % disruption on Internet services in some of the countries affected.

Note that throughout this chapter the term "failure" denotes infrastructure failures while the term "fault" denotes component faults that even though cannot be avoided they can be dealt with by utilizing redundancy, such that, even under some component faults, the infrastructure continues to operate. Thus, an overall system requirement is that the system should continue to operate (perhaps suboptimally) even when one or more of its constituent components have failed. However, when a system operates at a suboptimal point it could potentially waste energy and other resources, or operate at a high risk region. This creates a false sense of security for the entire system. Thus, autonomous ways for quickly detecting, isolating, and recovering the faults are needed for the successful deployment of critical infrastructures as it is discussed in detail in the sections that follow. This is because a fault that goes unattended for a long period of time can cause both tangible and intangible losses for the company/organization that provides the service, as well as for its clients. Therefore, the current trend is for more and more CIs to provide services that are virtually uninterruptible.

Table 1, for example, shows examples of monetary losses (per hour) incurred by various industries when even simple IT outages occur in their networks [3]. On average, businesses lose between $84,000 and $108,000 (US) for every hour of IT system downtime, according to estimates from studies and surveys performed by IT industry analyst firms. Losses in these industries can be tangible or intangible. Tangible/direct financial losses include such things as lost transaction revenue, lost wages, lost inventory, and legal penalties from not delivering on service level agreements. Conversely, intangible/indirect financial losses may include lost business opportunities, loss of customer/partner goodwill, brand damage, and bad publicity/press.

One important aspect of CIs related to their management is that they consist of various autonomous systems due to deregulation. This makes coordination and protection more difficult, since each autonomous system may have its own

Table 1 Projected losses/hour for various industries during IT outages [3]

Industry	Typical hourly cost of downtime (in US dollars)
Brokerage service	6.48 million
Energy	2.8 million
Telecom	2.0 million
Manufacturing	1.6 million
Retail	1.1 million
Health care	636,000
Media	90,000

objectives. A failure event can also be propagated or propagate its effects to other interdependent infrastructures, according to specific concepts of proximity (e.g., geographical, physical, cyber, etc.). This is due to the interdependencies that exist between infrastructures. These interdependencies are mostly highlighted when infrastructures are experiencing catastrophic natural disasters or are under terrorist attacks and there is an attempt to respond and recover from severe disruptions in the infrastructures [4]. Because of the interdependencies between critical infrastructures, potential failures in one infrastructure may lead to unexpected cascade failures to other infrastructures that may have severe consequences.

Specifically, over the last few years, several efforts have been undertaken in the literature on how to take measures aimed at preventing/reducing risks, preparing for, and protecting citizens and critical infrastructures from accidental faults, terrorist attacks, and other security related incidents. These measures entail (i) identifying critical infrastructures and interdependencies and developing risk assessment tools and methodological models for the critical infrastructures, (ii) developing monitoring, control, and security strategies for these infrastructures based on the risk assessment tools, (iii) developing contingency planning, stress tests, awareness raising, training, incident reporting, etc., as part of the prevention and preparedness strategy, and (iv) developing protection mechanisms, as part of the response strategy, that can enable the infrastructure to recover from the failure/attack.

3 Modeling of Critical Infrastructures

The problem of controlling and managing critical infrastructures is becoming more and more difficult as CIs are becoming very large due mainly to the growing demand for the services they provide. Furthermore, deregulation has resulted in more heterogeneous and distributed infrastructures, and has created more interdependencies between them, which make them more vulnerable to failures and attacks. As these infrastructures become larger and more complex, fewer people understand how these networks work and the interactions between all the components. Thus, models are created in order to represent these infrastructures and try to predict their behavior under failure/attack scenarios.