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.

http://www.springer.com/978-3-662-44159-6

Intelligent Monitoring, Control, and Security of Critical Infrastructure Systems

Kyriakides, E.; Polycarpou, M. (Eds.)
2015, XII, 359 p. 144 illus., 31 illus. in color., Hardcover
ISBN: 978-3-662-44159-6