Chapter 6

Hierarchical Architectures of Resilient Control Systems: Concepts, Metrics, and Design Principles

Quanyan Zhu

Department of Electrical and Computer Engineering, New York University

Dong Wei

Corporate Technology, Siemens Corporation

Kun Ji

Corporate Technology, Siemens Corporation

CONTENTS

6.1 Introduction

System resilience is the intrinsic ability of a system to adjust its functioning prior to, during, or following changes and disturbances, so that it can sustain required operations under conditions created by both expected and unexpected causes, such as human errors, system faults, adversarial attacks, and natural disasters. The concept of resilience is related to but also distinct from other system attributes, such as reliability, robustness, security, and fault tolerance. Resilience engineering can be understood as the science of managing multiple system properties in an integrative multilayer and multiagent fashion. Resilience has been studied in many fields, such as psychology, ecology, and organizational behavior.

Critical infrastructure refers to those systems and assets that are essential for the functioning of a society and economy. The incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Resilience is a desirable property of critical infrastructure. As it is mentioned in [6],

> resilience has become an important dimension of the critical infrastructure protection mission, and a key element of the value proposition for partnership with the government because it recognizes both the need for security and the reliability of business operations.

Control systems are typically used in industries such as electric generation, transmission and distribution, gas and oil plants, water and wastewater treatment, and manufacturing for monitoring and controlling physical and chemical processes in critical infrastructures [5, 8]. Therefore, it is important to ask the following questions: What does resilience mean to control systems? How do we measure or estimate it? What applications can deploy resilient control technologies? To answer the above-mentioned questions, this chapter describes a big picture of fundamental principles and applications of resilient control systems by

- Defining the scope of resilient control systems
- Developing a hierarchical viewpoint toward resilient control systems
- Defining the resilience of control systems quantitatively
- Discussing the relationship between resilience properties of a control system and other properties, such as robustness, fault tolerance, flexibility, survivability, and adaptiveness
- Proposing metrics to measure or estimate control system resiliency
- Developing design and operation principles
- Discussing applications and guidelines in the smart grid that deal with extreme events
- Disclosing related research fields, such as prognostic technologies and data fusion technologies

This chapter is organized as follows: Section 6.2 discusses the related research works conducted in the area of system resilience. In Section 6.3, we present a hierarchical viewpoint toward resilient control systems. Section 6.4 presents major performance indices that quantify the resilience of control systems. Design and operation principles are discussed in Section 6.5. An example of the power grid is used to illustrated the principles of resilient control systems in Section 6.6. We conclude the chapter with Section 6.7, discussing potential applications of resilient control systems and further research topics.

6.2 Related Work

Originally, the term *resilience* was studied in the fields of ecology and psychology. The concept of resilience in ecological systems was first described by the Canadian ecologist C. S. Holling [9] to draw attention to trade-offs between efficiency, on the one hand, and persistence, on the other, or between constancy and change, or between predictability and unpredictability. Emmy Werner was one of the first scientists to use the term *resilience* in psychology, which refers to the ability to recover from trauma or crisis. She studied children who grew up with alcoholic or mentally ill parents in the 1970s [30].

In recent years, the term *resilience* has been used to describe a movement among entities such as businesses, communities, and governments to improve their ability to respond to and quickly recover from catastrophic events such as natural disasters and terrorist attacks. The concept is gaining credence among public and private sector leaders who argue that resilience should be given equal weight to preventing terrorist attacks in U.S. homeland security policy. The study of resilience from the perspective of organizations includes business organizations [3, 16, 21, 25, 31] and government organizations [6, 7, 11].

Resilience has been studied in the field of communication networks in the past few years. Resilient communication networks [2, 4, 18] aim to provide and maintain acceptable service to the following applications in the face of faults and challenges to normal operation:

- Enable users and applications to access information when needed, such as web browsing, distributed database access, and sensor monitoring
- Maintain end-to-end communication association, such as computer-supported cooperative work, videoconference, and teleconference
- Provide distributed processing and networked storage

The major topics include resilient network structure [10, 14], intrusion resilient network [26, 27], denial-of-service (DoS) resilient network [1, 24], and resilient network coding [12].

Literature on resilience study can also be found in the fields of economics, aviation industry, disaster response, nuclear power plants, oil and gas industry, emergency health care, and transportation engineering.

The area of resilient control systems (RCSs) is a new paradigm that encompasses control design for cyber security, physical security, process efficiency and stability, and process compliance in large-scale, complex systems. In [23], RCS is defined as a control system that maintains state awareness and an accepted level of operational normalcy in response to disturbances, including threats of an unexpected and malicious nature. While one might say that resilient design is primarily dependable computing coupled with fault-tolerant control, it has been argued in [23] that dependable computing views malicious faults as a source of failure, but does not consider the effect of these faults on the underlying physical processes in a large-scale complex system.

Recent literature on RCS has studied many aspects of resilience in control systems. In [22], notional examples are used to discuss fundamental aspects of resilient control systems. It has been pointed out that current research philosophies lack the depth or the focus on the control system application to satisfy many aspects of requirements of resilience, including graceful degradation of hierarchical control while under cyber attack. In [37], a hierarchical viewpoint is used to address security concerns at each level of complex systems. The paper emphasizes a holistic cross-layer philosophy for developing security solutions and provides a game-theoretical approach to model cross-layer security problems in cyber-physical systems. In [36], the authors have proposed a game-theoretic framework to analyze and design, in a quantitative and holistic way, robust and resilient control systems that can be subject to different types of disturbances at different layers of the system. In [34], a hybrid system model is used to address physical layer control design and cyber-level security policy making for cyber-physical systems that are subject to cascading effects from cyber attacks and physical disturbances. In [28], metrics for resilient control systems are developed for analyzing and designing resilient systems. In this work, we extend the concepts developed in [28] for hierarchical cyber-physical systems.

Cyber security is an essential component of the resilience of control systems. Few works have provided quantitative methods of modeling of device configurations and evaluating trade-offs among defense options. In [15], the authors have made a comprehensive survey on game-theoretic methods for different problems of network security and privacy. It has been pointed out that the quantitive methods discussed in the survey can be integrated with cyber-physical systems for analyzing and designing resilient control systems. The literature on device configurations can be found in [33, 35, 38]. In [33], a cooperative game approach has been used to address the static configuration of security devices, such as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), in the face of adversarial attacks. In [35], the authors address the dynamic counterpart of the configuration problem. The equilibrium cyber policy can be obtained from a game-theoretic analysis of a dynamic zero-sum Markov game, which has taken into account the trade-offs between different defense mechanisms. In [38], a network-level configuration of security devices has been addressed by considering the interdependence of devices in the network.

6.3 Hierarchical Resilient Control Systems

An industrial control system (ICS) is one electronic device or a set of electronic devices to monitor, manage, control, and regulate the behavior of other devices

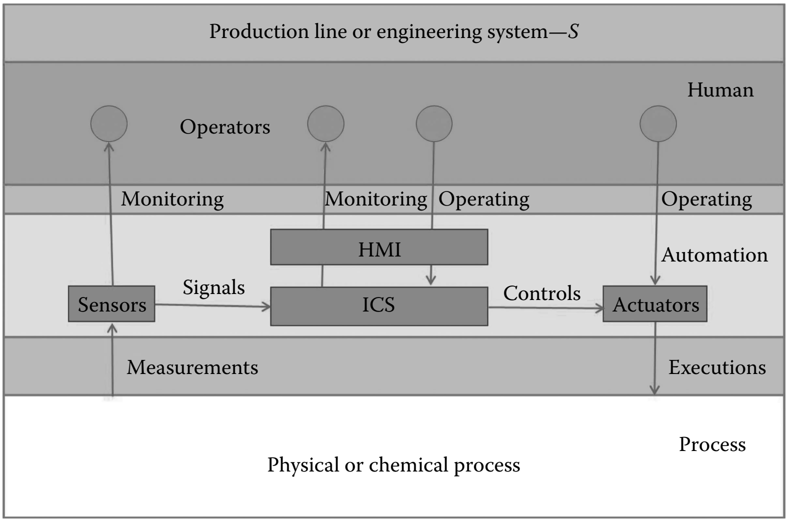

Figure 6.1: System model for a pipeline engineering system.

or systems. ICS includes supervisory control and data acquisition (SCADA) system, distributed control system (DCS), and programmable logic controllers (PLCs). A production line or engineering system S is shown in Figure 6.1: (1) the human layer sits at the top of the architecture, where operators monitor process data via sensors directly or via human machine interface (HMI) and control the process by operating actuators directly or by inputing command to HMI; (2) the physical process layer sits at the bottom of the architecture, where a physical or chemical process is monitored via sensors and controlled by actuators; and (3) the control and automation layer sits in the middle, where ICS is at the center to collect real-time data of the controlled process via sensors, provide status and diagnostic data to operators via HMI, receive commands and settings from operators via HMI, and control the controlled process via actuators. In a power grid, ICS includes the energy management system (EMS), remote terminal unit (RTU), and PLC. Meters are sensors, and circuit breakers, transformers, and tap changers are actuators; the controlled physical process is the electric power transmission.

In this section, we describe a layered architecture perspective toward resilient industrial control systems (RICSs), which helps us to identify research problems and challenges at each layer and build models for designing security measures for control systems in critical infrastructures. We also emphasize a cross-layer viewpoint toward the security issues in ICSs in that each layer can have security dependence on the other layers. We need to understand the tradeoff between the information assurance and the physical layer system performance before designing defense strategies against potential cyber threats and attacks.

We hierarchically separate ICSs into six layers, namely, physical layer, control layer, communication layer, network layer, supervisory layer, and management layer. The physical and control layers constitute the physical component of the system, while the communication and network layers constitute the cyber component of the system. The supervisory and management layers constitute the human component of an ICS. This hierarchical structure is depicted in Figure 6.2. The power plant is at the physical level, and the communication network and security devices are at the network and communication layers. The controller interacts with the communication layer and the physical layer. An administrator is at the supervisory layer to monitor and control the network and the system. Security management is at the highest layer, where security policies are made against potential threats from attackers. SCADA is the fundamental monitoring and control architecture at the control area level. The control centers of all major U.S. utilities have implemented a supporting SCADA for processing data and coordinating commands to manage power generation and delivery within the electric hybrid vehicle (EHV) and HV (bulk) portions of their own electric power system [32].

In subsequent subsections, we identify problems and challenges at each layer and propose problems whose resolution requires a cross-layer viewpoint.

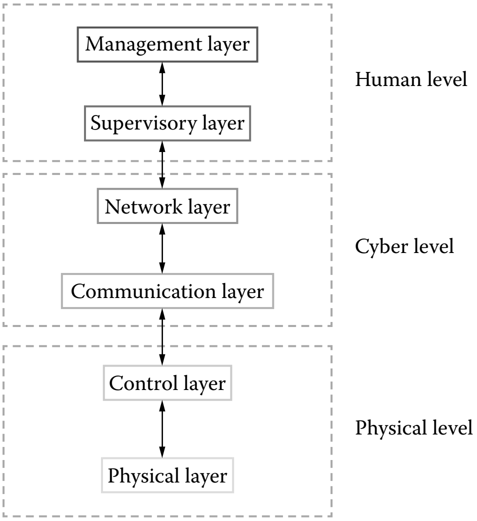

Figure 6.2: The hierarchical structure of ICSs composed of six layers. The physical layer resides at the bottom level and the management layer at the highest echelon.

6.3.1 Physical Layer

The physical layer comprises the physical plant to be controlled. It is often described by an ordinary differential equation (ODE) model from physical or chemical laws. It can also be described by difference equations, Markov models, or model-free statistics. We have the following challenges that pertain to the security and reliability of the physical infrastructure. First, it is important to find appropriate measures to protect the physical infrastructure against vandalism, environmental change, unexpected events, and so forth. Such measures often need a cost–benefit analysis involving the value assessment of a particular infrastructure. Second, it is also essential for engineers to build the physical systems with more dependable components and more reliable architecture. It brings up the concern of the physical maintenance of the control system infrastructures that demand cross-layer decision making between the management and physical levels.

6.3.2 Control Layer

The control layer consists of multiple control components, including observers and sensors, intrusion detection systems (IDSs), actuators, and other intelligent control components. An observer has the sensing capability that collects data from the physical layer and may estimate the physical state of the current system. Sensors may need to have redundancies to ensure correct reading of the states. The sensor data can be fused locally or sent to the supervisor level for global fusion. A reliable architecture of sensor data fusion will be a critical concern. An IDS protects the physical layer as well as the communication layer by performing anomaly-based or signature-based intrusion detection. An anomaly-based ID is more common for the physical layer, whereas a signature-based ID is more common for the packets or traffic at the communication layer. If an intrusion or an anomaly occurs, an IDS raises an alert to the supervisor or works hand in hand with built-in intrusion prevention systems (related to emergency responses, e.g., control reconfiguration) to take immediate action. There lies a fundamental trade-off between local decisions and a centralized decision when intrusions are detected. A local decision, for example, made by a prevention system, can react in time to unanticipated events; however, it may incur a high packet drop rate if the local decision suffers high false negative rates due to incomplete information. Hence, it is an important architectural concern on whether the diagnosis and control module needs to operate locally with IDS or globally with a supervisor.

6.3.3 Communication Layer

The communication layer is where we have a communication channel between control layer components or network layer routers. The communication channel can take multiple forms: wireless, physical cable, Bluetooth, and so forth. The communication layer handles the data communication between devices or layers. It is an important vehicle that runs between different layers and devices. It can often be vulnerable to attacks such as jamming and eavesdropping. There are also privacy concerns of the data at this layer. Such problems have been studied within the context of wireless communication networks. However, the goal of a critical infrastructure may distinguish themselves from the conventional studies of these issues.

6.3.4 Network Layer

The network layer concerns the topology of the architecture. We can see it is comprised of two major components: network formation and routing. We can randomize our routes to disguise or confuse the attacks so as to achieve certain security or secrecy or minimum delay. Moreover, once a route is chosen, how much data should be sent on that route has been long a concern for researchers in communications. In control systems, many specifics of the data form and rates may allow us to reconsider this problem in a control domain.

6.3.5 Supervisory Layer

The supervisory layer coordinates all layers by designing and sending appropriate commands. It can be viewed as the brain of the system. Its main function is to perform critical data analysis or fusion to provide immediate and precise assessment of the situation. It is also a holistic policy maker that distributes resources in an efficient way. The resources include communication resources, maintenance budget, and control efforts. In centralized control, we have one supervisory module that collects and stores all historical data and serves as a powerful data fusion and signal processing center.

6.3.6 Management Layer

The management layer is a higher-level decision-making engine where the decision makers take an economic perspective toward the resource allocation problems in control systems. At this layer, we deal with problems such as (1) how to budget resources to different systems to accomplish a goal and (2) how to manage patches for control systems, for example, disclosure of vulnerabilities to vendors and development and release of patches.

6.4 Metrics for Resilient Control Systems

Although some literature discusses the definition of resilient control systems [13, 19, 23], each report covers only some parts of the resilience concept. There is no literature that defines a resilient control system quantitatively and its scope. In this chapter, we propose to define a resilient control system as follows: a *resilient control system* is designed and operated in a way that

- The incidence of undesirable incidents can be minimized.
- Most of the undesirable incidents can be mitigated or partially mitigated.
- The adverse impacts of undesirable incidents can be minimized, if these incidents cannot be mitigated completely.
- It can recover to normal operation in a short time.

Note that the undesirable incidents are not limited to those occurring on the control system itself. They can happen at the human layer, such as operators sending wrong commands or settings to ICS; they can happen at the physical process layer, such as broken cable in a power grid; they can also happen at the control layer, such as sensor damage and solenoid malfunction.

6.4.1 Properties of Resilient Industrial Control Systems

By definition, there are four desirable properties in a resilient industrial control system when it is designed and operated. Figure 6.3 illustrates those properties by using the example of cyber attacks on a power grid automation system.

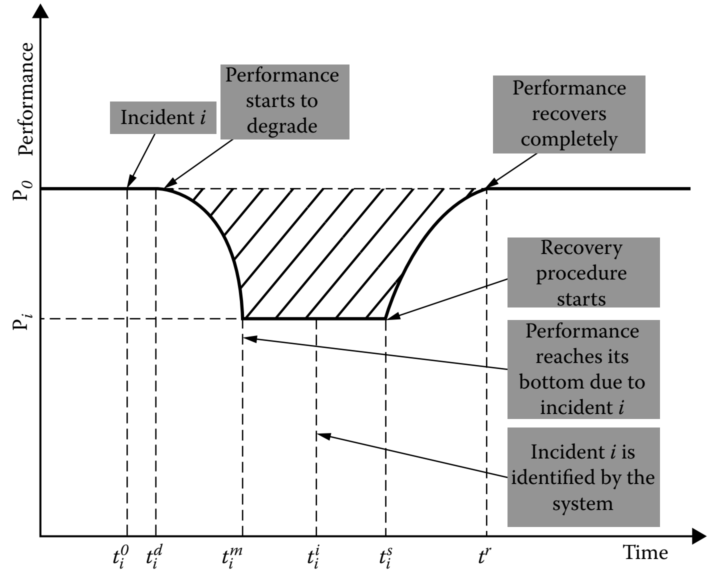

Figure 6.3: Resilience curve.

As shown in Figure 6.3, the performance axis shows the performance of the entire engineering system $\mathcal{S}$ (not the ICS), which can be defined as a function of production and quality, as in Equation 6.1. Let $\mathcal{P}$ denote the performance of the engineering system. p and q represent production and quality, respectively.

$$\mathcal{P}(t) = f(p(t), q(t)) \tag{6.1}$$

For instance, in a power grid, production can be measured by how much power is being delivered by the power grid, and quality is a function of voltage, frequency, harmonics, and so forth.

Property 6.1 A resilient control system is engineered and operated in a way that the incidence of undesirable incidents can be minimized.

For instance, to minimize the incidence of cyber attacks on a power grid automation, a control system can be designed and operated by using dedicated communication lines, isolating the automation network from the enterprise network, using cryptography, and hence reducing its exposure to potential hackers.

Property 6.2 A resilient control system is engineered and operated in a way that most of the undesirable incidents can be mitigated or partially mitigated.

For instance, assume that the only exposure point to the power grid automation network is the gateway to the enterprise network. In order to mitigate most cyber attacks, one firewall, which can detect intrusion and filter adverse data packets, can be implemented behind the gateway. And hence, with appropriate security policy, such as access control or an intrusion detection profile, it can mitigate most of the cyber attacks.

Property 6.3 A resilient control system is engineered and operated in a way that the adverse impacts of undesirable incidents can be minimized.

Assume incident i is a cyber attack on an automation system in one substation. In order to minimize the performance degradation, the power grid automation can be designed to be able to detect this attack and redirect some power flow to other substations before this substation automation system is compromised completely. Then the performance degradation is $P_0 - P_i$ (see notations in Table 6.1), provided that not all power flow can be shed to other substations.

Property 6.4 A resilient control system is engineered and operated in a way that it can recover from the adverse impacts of undesirable incidents to normal operation in a short time.

Assume, again, incident *i* is a cyber attack on an automation system in one substation, in Figure 6.3. In order to recover from the performance degradation, the power grid automation can be designed to be able to detect and locate this attack and isolate this attack or redirect the data path in a short time. Then the performance can come back to normal.

These properties of resilience can be regarded as four sequential steps to deal with undesirable incidents during both stages of engineering and operation, as shown in Figure 6.4.

A control system can be called *i* resilient if the engineering system is not adversely impacted by undesirable incident *i*. For instance, a power grid automation system can be called *cyber attack resilient* if (1) the control system has no exposure to hackers since the system is completely isolated; (2) if the system has exposure points to hackers, a firewall works efficiently to detect and block malicious data packets at the exposure points; or (3) the automation system possesses redundant devices and data paths and reroutes data packets to another path or uses other devices to avoid any adverse impact when it detects cyber attacks.

6.4.2 Distinguishing Terms

Terms such as *resilience*, *robustness*, *adaptiveness*, *survivability*, and *fault tolerance* are used interchangeably. However, they do not have the exact same meaning, although they may have some things in common. To focus on the resilience properties precisely, it is important to distinguish them.

The robustness of industrial control systems aims to function properly as long as modeling errors, in terms of uncertain parameters and disturbances at the physical process layer, as in Figure 6.1, are bounded; the adaptiveness of industrial control systems aims to function properly by adjusting their control algorithms according to uncertain parameters at the physical layer. Note that the uncertain parameters and disturbances can be regarded as undesirable incidents at the process layer. Survivability is the quantified ability of an industrial control system to continue to function during and after a nature or man-made disturbance, which may be occur at any layer in Figure 6.1. Fault-tolerant industrial control systems are focused on overcoming failures that may happen at any layer in Figure 6.1.

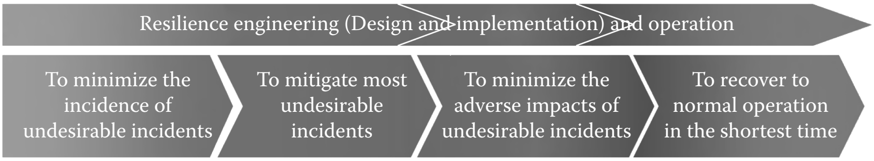
Resilience engineering (Design and implementation) and operation
To minimize the incidence of undesirable incidents
To mitigate most undesirable incidents
To minimize the adverse impacts of undesirable incidents
To recover to normal operation in the shortest time

Figure 6.4: Four-step process to improve system resilience.

They try to identify failure possibilities and take precautions in order to avoid them by any means without causing a significant damage in the system; however, they do not consider the presence of intelligent adversaries, such as cyber attacks. Unlike resilience, robustness, adaptiveness, survivability, and fault tolerance do not address how quickly the industrial control system recovers to normal operation after the undesirable incident. All those properties are part of the characteristics of resilience. Therefore, resilience is a superset of all the above properties in the proposed concept.

6.4.3 Quantifying Resilience of a Control System

There is no literature report so far to measure *how resilient a control system is*, although there are reports on how to measure system resilience. For instance, it is proposed to measure resilience performance [17] by buffering capacity, margin, tolerance, and so forth. However, these metrics do not show how fast the system can recover from the undesirable incidents. Since it is objective to “measure” an object, and resilience is hard to measure, the metrics in this chapter are proposed to *estimate* rather than measure resilience of an industrial control system. Notations used in this chapter are described in Tables 6.1 and 6.2.

For an undesirable incident i, the following metrics, as shown in Table 6.2, are proposed to estimate the resilience of the control system:

- **Protection time** T_i^p: The time that the system can withstand incident i without performance degradation:

$$T_i^p = t_i^d - t_i^0. \tag{6.2}$$

- **Degrading time** T_i^d: The time that the system reaches its performance bottom due to incident i:

$$T_i^d = t_i^m - t_i^0. \tag{6.3}$$

- **Identification time** T_i^i: The time that the system identifies incident i. Note that T_i^i is not necessarily greater than T_i^d—a well-designed and operated system is able to identify the incident before it reaches its performance bottom:

$$T_i^i = t_i^i - t_i^0. \tag{6.4}$$

- **Recovery time** T_i^r: The time that the system needs to recover to normal operation from incident i:

$$T_i^r = t_i^r - t_i^s. \tag{6.5}$$

- **Performance degradation** P_i^d: Maximal performance degradation due to incident i:

$$P_i^d = P_0 - P_i. \tag{6.6}$$

Table 6.1 Summary of Notations

Notation	Description
$\mathcal{S}$	3-layered engineering system with an ICS in the center
p	Production
q	Quality
P	Performance
t_i^0	Moment that incident i occurs
t_i^d	Moment that system performance starts to degrade
t_i^m	Moment that system performance reaches the bottom due to incident i
t_i^i	Moment that incident i is identified by the ICS or operators
t_i^s	Moment that the system starts to recover; either manually initiated by operators or automatically by the ICS
t_i^r	Moment that the system completely recovers from incident i occurring
P_0	Original system performance when incident i occurs
P_i	Minimum performance due to incident i
μ_i	Number of incidents i that may occur per year
I	Set of all possible undesirable incidents
I'	Set of all possible critical undesirable incidents, where $I' \subseteq I$
M, N	Subsets of possible undesirable incidents
$\mu_{M,N}$	Probability that incidents of M occur and incidents of N do not
$L_{M,N}$	Overall potential loss that incidents of M occur and incidents of N do not

- **Performance loss** P_i^l: Total loss of performance due to incident i:

$$P_i^l = P_0 \times (t_i^r - t_i^0) - \int_{t_i^0}^{t_i^r} P(t)dt. \tag{6.7}$$

- **Total loss** L_i: Total financial loss due to incident i, which includes performance loss, equipment damage, and recovery cost R_i^c:

$$L_i = f(P_i^l, R_i^c). \tag{6.8}$$

- **Overall potential critical loss** L': Overall loss due to all potential critical undesirable incidents I' per year:

$$L' = \sum_{\forall M,N \subseteq I'} L_{M,N} \times \mu_{M,N}, \tag{6.9}$$

where $M, N \subseteq I'$, $M \cap N = \phi$, and $M \cup N = I'$.

Table 6.2 Resiliency Metrics for ICS

Term	Notation	Description
Protection time	T_i^p	Time that system $\mathcal{S}$ can withstand incident i without performance degradation
Degrading time	T_i^d	Time that system $\mathcal{S}$ reaches its performance bottom due to incident i
Identification time	T_i^i	Time that system $\mathcal{S}$ identifies incident i
Recovery time	T_i^r	Time that system $\mathcal{S}$ needs to recover to normal operation from incident i
Performance degradation	P_i^d	Maximal performance degradation of system $\mathcal{S}$ due to incident i
Performance loss	P_i^l	Total loss of performance of system $\mathcal{S}$ due to incident i
Total loss	L_i	Total financial loss due to incident i, which includes performance loss, equipment damage, and recovery cost
Overall potential loss	L	Overall loss due to all potential undesirable incidents
Overall potential critical loss	L'	Overall loss due to all potential critical undesirable incidents I'

Since it is not possible to enumerate all potential incidents, it is hard to compute the total loss, L_i. Thus, the overall potential critical loss, L', is proposed to calculate the overall resilience of a control system. For engineering system $\mathcal{S}$, assume that there are two choices of control systems: System A and System B. System A is said to be more i-resilient than System B, or System A is more resilient than System B with regard to incident i if performance loss P_i^l and L_i of System A due to incident i are less than those of System B; System A is said to be more resilient than System B if the overall potential loss L of ICS A is less than that of ICS B.

6.5 Building, Operating, and Improving a RICS

In practice, it is not easy, if not impossible, to enumerate all potential undesirable incidents. Therefore, a reduced incident set I' is proposed to be used to analyze probability and adverse impacts of critical incidents, where $I', \bar{I}' \subseteq I$, $I' \cup \bar{I}' = I$, $I' \cap \bar{I}' = \phi$, and $\bar{I}'$ represent the set of undesirable incidents that can be ignored due to their insignificance of probability or adverse impacts.

Since it is also not easy to obtain precise information of all possible incidents i and their incidences μ_i, a cyclic process is proposed here, as shown in Figure 6.5, to improve the resilience of an ICS:

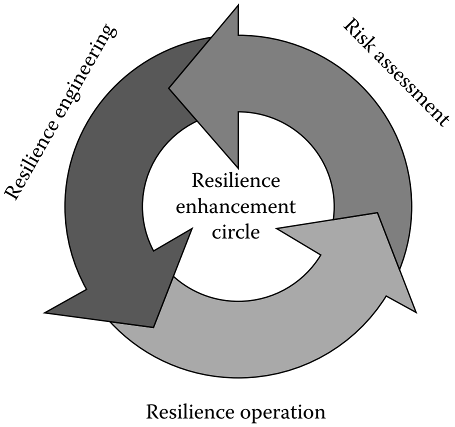

Figure 6.5: Process of improving resilience of an ICS.

1. **Risk assessment:** Enumerate all possible undesirable incidents i, their incidences μ_i, and losses L_i.

2. **Resilience engineering:** Design and implement the ICS to minimize the overall possible loss L' with cost constraints.

3. **Resilience operation:** Operate system $\mathcal{S}$ in a way that the overall possible loss L' is minimized.

4. **Resilience enhancement:** Update information of I' and L'; repeat Steps 2 and 3.

6.5.1 Risk Assessment

The resilience properties discussed in Section 6.2 indicate that adding resilience elements to an industrial control system is focused on dealing with undesirable incidents. This requirement necessitates a control design strategy shift from reactive methods to proactive methods with consideration of assessing potential threats and taking necessary protection measures against them. In order to minimize the incidence and adverse impacts of all possible undesirable incidents, it is very important to understand them first:

- Enumerate all possible undesirable incidents that can be imagined, I'.
- Analyze how frequently they occur or the probability they happen, $\mu_{M,N}$.
- Analyze the adverse impacts they can have on engineering system $\mathcal{S}$, L'.

Undesirable incidents should be considered at all three levels:

- Improper commands and invalid settings from operators at the human level; wrong messages from ICS to operators could lead to wrong operation by the operators.
- Malfunctions and failures, at the control layer, of sensors and actuators; communication failure between controllers, HMIs, sensors, and actuators.
- Nonprecise and even wrong process model at the physical level.

Since it is difficult to enumerate all undesirable incidents and estimate the probabilities they happen, risk assessment cannot be performed once. After a period of operation time, this information should be updated iteratively, and risk assessment should be performed again based on the updated information.

6.5.2 Resilience Engineering

Based on the risk assessment presented in Section 6.5.1, resilience engineering is focused on dealing with some undesirable incidents, and it is a two-stage process: design and implementation. The design of a resilient industrial control system necessitates novel interactions between two engineering disciplines: computer and control engineering. From the control engineering point of view, the control of a complex dynamic industrial system is a well-studied area, such as advanced control technologies including robust control, adaptive control, and so forth, but much less is known about how to improve control system tolerance to cyber attack. As mentioned in Section 6.2, resilience is a superset of all the other properties; resilient decision and control laws should be synthesized as augmentation of existing control decisions such as robustness or adaptiveness, with the additional objective of reliable and fast recovery from undesirable incidents. The proactive control design strategy should be considered all the way from design through the implementation stages.

The following areas should be studied to improve system resilience during the stage of resilience engineering:

- To minimize the probability of undesirable incidents $\mu_{M,N}$ (1) a well-designed ICS can validate the inputs from HMI by operator authentication and authorization and input limits of data, thus identifying invalid commands from the operator; (2) it can also validate input data from sensors and pass correct data to operators; and (3) a well-designed system monitoring and prognosis tool monitors and predicts failures of some key components and enables operators to prevent them from happening.
- To mitigate undesirable incidents or minimize the adverse impacts of them $L_{M,N}$, (1) as a general paradigm, the most accepted and used

implementation principle for resilience is redundancy; systems make use of redundant components along with primary components and switch to them in a failure condition; (2) deploy distributed control system, which can still work if one single controller fails; and (3) enable the control system to be aware of its states and keep distance from its operation boundaries.

- To recover in a short time $T^r_{M,N}$, (1) enable the control system to identify the undesirable incidents accurately, and pass the corresponding information to operators, if they are in the control loop; (2) provide a functionality that can generate backup recovery plans online and automatically for some critical undesirable incidents; and (3) enable the system to start the corresponding recovery plan when the undesirable incident is identified.

6.5.3 Resilience Operation

Based on the risk assessment and resilience engineering, resilience operation should be of state awareness, cyber-attack awareness, and risk awareness. With all real-time information, a resilient industrial control system should be operated to minimize the potential loss of System $\mathcal{S}$:

- To minimize the probability of undesirable incidents $\mu_{M,N}$, (1) a well-designed and well-operated ICS can monitor System $\mathcal{S}$ and intelligently analyze real-time data, and identify boundary conditions and operation margins, (2) it can also pass the analysis results to operators and provide operation suggestions to operators.

- To mitigate undesirable incidents or minimize the adverse impacts of them $L_{M,N}$, (1) a well-designed and well-operated ICS can generate and adjust control strategies online according to detected undesirable incidents or potential incidents; (2) it can be aware of its state, cyber attacks, and risks, and keep distance from boundaries; and (3) it can interpret, reduce, and prioritize undesirable incidents based on the information from the state awareness, thus providing adaptive capacity to perform corresponding responses, such as prioritized response to focus on mitigating the most critical incidents if parallel responses are limited.

- To recover in a short time $T^r_{M,N}$, (1) a well-operated ICS can identify the undesirable incidents online accurately and pass the corresponding information to operators; (2) it can also generate backup recovery plans online and automatically for detected undesirable incidents; and (3) it can start the corresponding recovery plan once the undesirable incident is identified.

6.5.4 Resilience Enhancement

Due to the uncertainty and complexity in control system applications, control system redesign becomes inevitable to meet challenges in real applications that might have been ignored at the beginning. This is also true for resilience. Since it is hard to list all critical undesirable incidents and estimate their corresponding losses, it is important to update this information with more complete and accurate data after engineering and operation. On the other hand, with this updated information, new control strategies can be developed during engineering and executed during operation accordingly, hence further enhancing system performance in terms of resilience.

6.6 Cyber-Attack-Resilient Power Grid Automation System: An Example of Resilient ICS

This section further discusses resilience by using an example—cyber-attack-resilient power grid automation system. The approaches to improve power grid automation system resilience with respect to cyber attacks are presented. A cyber risk assessment model and a framework to protect the power grid from cyber attacks are disclosed. Some ideas in this section are part of the author's previous works in [20] and [29], and some parts are their extension.

The emerging smart grid requires the conventional power grid to operate in a way that it was not originally designed to. Bringing more participants to the smart grid will open the originally isolated automation networks to more people, if not to the public. This brings big concerns of cyber-security issues of automation systems. To improve cyber-attack resilience of the power grid automation system, a security solution framework with three major elements is proposed:

1. **Dynamic and evolutionary risk assessment model:** The model assesses the critical assets of the power grid. It uses dynamic quasi-real-time simulations to reveal potential vulnerabilities. It detects security events and activities both previously known and currently unidentified. Using the existing topology of the power grid, a risk assessment graph is created. And this graph dynamically evolves through design and real-world operation. The graph is translated into a Bayesian network where edges are weighted according to predefined economical measures and business priorities. The model provides a list of assets with utility functions that reflect the associated risks and economic loss.

2. **Integrated and distributed security system:** It overlays across the intelligent power grid network in a hierarchical and distributed manner. The system includes (a) security agents, which reside next to or are integrated to field devices and controllers, providing end-to-end security; (b) managed switches in control networks, providing quality of service (QoS)

in terms of delay and bandwidth; and (c) security managers, which are distributed across control centers and substations, managing cyber-security-related engineering, monitoring, analysis, and operation. The proposed security system enables power grid operators to monitor, analyze, and manage cyber security of the power grid.

3. **Security network topology optimization model:** It optimizes the topology on the security system without compromising the performance of control functionalities.

6.6.1 Risk Assessment Model

To construct a general model for risk assessment, an integration of physical features of power grids and substations with cyber-related and security characteristics of such systems is needed. To make the model practical as well, a level of aggregation in cyber-security analysis should be considered to avoid complexity and dimensionality that cannot be implemented with existing calculation capacities. Therefore, the proposed framework is decomposed as follows:

1. First-pass model runs at the grid level to identify the most critical substations to the power grid operation
2. Second-pass model runs at the substation level to identify the most critical components to the substation operation

This risk assessment model can be run both offline and online. When running offline (risk assessment stage), it receives inputs including power grid topology, substation primary circuit diagrams, statistical power flows, and automation system topology. It calculates and outputs all potential loss due to cyber attacks to critical components in substations. The result can help power grid operators to find critical cyber-security assets and understand the potential loss, L', related to cyber attacks on these assets. When running online (resilience operation stage), the inputs of this model replace statistical power flow data with real-time power flow data. The outputs L' are the same as those of the offline model. The results can help the operator identify critical security assets and understand the potential loss due to cyber attacks according to real-time information, and further improve its resilience during both resilience operation enhancement stages.

6.6.2 Integrated Security System

To address the security issues in power grid automation systems, a paradigm to build a distributed and scalable security framework is proposed, as shown in Figure 6.6. Note that DMS is distribution management system, IED is intelligent

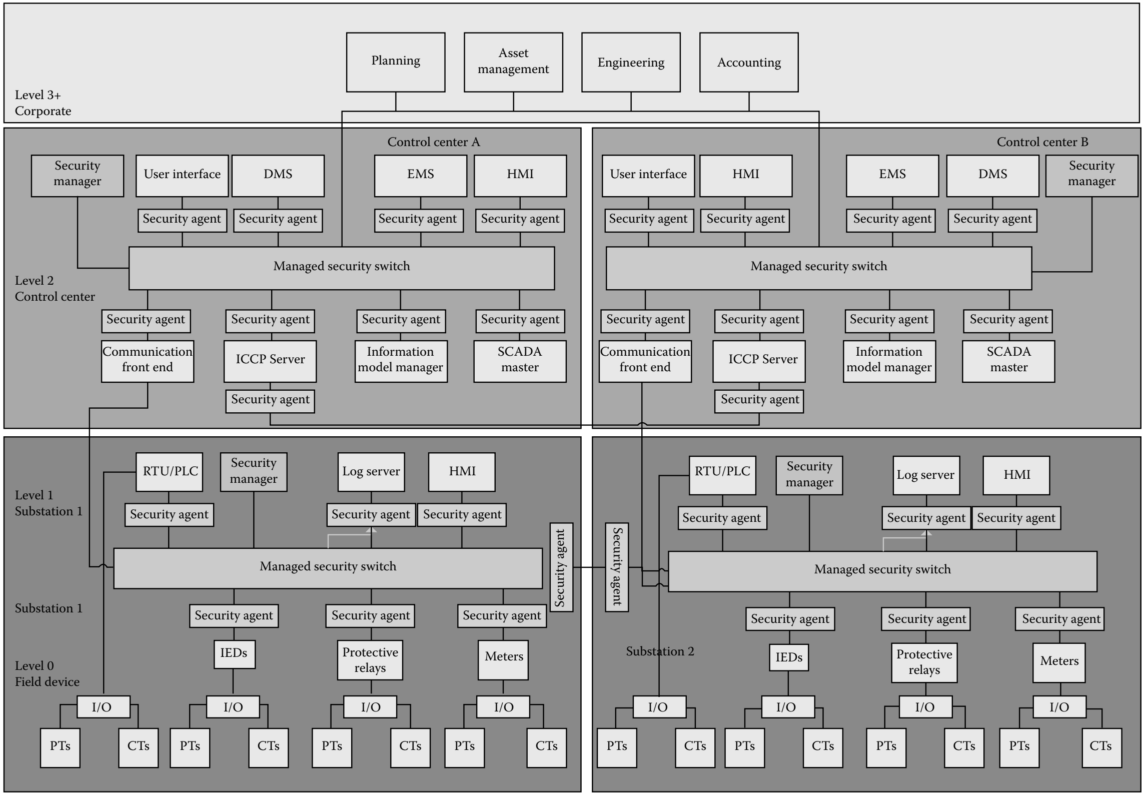

Figure 6.6: The integrated security system for power grid automation systems.

electronic device, and PT and CT are potential transmitter and current transmitter, respectively. There are three major conceptual components in the proposed integrated security framework, as follows:

- **Security agent:** It brings security to the edges of the system by providing protection at the networked device level. These agents are firmware or software agents, depending on the layer of the control hierarchy. At the field device layer (e.g., IEDs), these agents are less intelligent—containing simple rules and decision-making capabilities—and do more of event logging and reporting. At higher control layers (e.g., RTUs), these software agents are more intelligent with more complex rules for identification and detection of intrusive events and activities within the controllers. In particular, a security agent is commissioned to accomplish the following functionalities:
    - Acquire and run the latest vulnerability patches from its security manager
    - Collect data traffic patterns and system log data and report to the security manager
    - Analyze traffic and access patterns with varying complexity, depending on the hierarchical layer
    - Run host-based intrusion detection
    - Detect and send alarm messages to the security manager and designated devices, such as HMI
    - Acquire access control policies from the security manager and enforce them
    - Encrypt and decrypt exchanged data
- **Managed security switch:** To protect bandwidth and prioritize data, the managed switches are used across the automation network. These switches, working as network devices, connect controllers, RTUs, HMIs, and servers in the substation and control center. They possess the following functionalities:
    - Separate external and internal networks, hide the internal networks, and run network address translation (NAT) and network port address translation (NPAT)
    - Acquire bandwidth allocation pattern and data prioritization pattern from the security manager
    - Separate data according to prioritization pattern, such as operation data, log data, trace data, and engineering data
    - Provide QoS for important data flow, such as operation data, guaranteeing its bandwidth and delay

  - Manage multiple virtual local area networks (VLANs)
  - Run simple network-based intrusion detection

- **Security manager:** Security managers reside in the automation network and directly or indirectly connect to the managed switches across the automation networks. They can be protected by existing IT security solutions and are able to connect to a vendor's server, managed switches, and security agents via a virtual private network (VPN). Security managers possess the following functionalities:
  - Collect security agent information
  - Acquire vulnerability patches from a vendor's server and download them to the corresponding agents
  - Manage cryptographic keys
  - Work as an authentication, authorization, and accounting (AAA) server, which validates user identifications, authorizes user access right, and records what a user has done to controllers
  - Collect data traffic patterns and performance matrices from agents and switches
  - Collect and manage alarms and events from agents and switches
  - Generate access control policies based on collected data and download to agents
  - Run complex intrusion detection algorithms at automation network levels
  - Generate bandwidth allocation patterns and data prioritization patterns and download them to managed switches

The integrated security system monitors communication traffic, detects possible cyber attacks, and minimizes the adverse impacts of those cyber attacks.

6.6.3 Security Optimization Model

Based on the result of the risk assessment model (most vulnerable components such as RTUs and communication links), the security optimization model can help power grid operators place security agents and switches with constraints of cost, bandwidth, and data delay requirements, hence improving system cyber-attack resilience during the engineering stage; this model can also help operators adjust security policies to improve cyber-attack resilience during resilience operation and enhancement stages, according to online risk assessment results and detected cyber intrusions.

6.6.4 Cross-Layer Co-Design

Security solutions at the physical and cyber layers of an integrated control system need to take into account the interaction between these two layers. Figure 6.7 illustrates the concept of security interdependence between the cyber system and the physical plant. We need to adopt a holistic cross-layer viewpoint toward a hierarchical structure of industrial control systems. The physical layer is comprised of devices, controllers, and the plant, whereas the cyber layer consists of routers, protocols, and security agents and manager. The physical layer controllers are often designed to be robust, adaptive, and reliable for physical disturbances or faults. With the possibility of malicious behavior from the network, it is also essential to design controllers that take into account the disturbances and delay resulting from routing and network traffic, as well as the unexpected failure of network devices due to cyber attacks. On the other hand, the cyber-security policies are often designed without consideration of control performances. To ensure the continuous operability of the control system, it is equally important to design security policies that provide a maximum level of security enhancement but minimum level of system overhead on the networked system. The physical and cyber aspects of control systems should be viewed holistically for analysis and design.

The cyber infrastructure serves as an interface between the controller and the physical plant. The control signals are sent through a security-enhanced IT infrastructure, such as wireless networks, the Internet, and local area networks (LANs). The security architecture of the IT infrastructure is designed to enable the security practice of defense in depth for control systems. The cascading countermeasures using a multitude of security devices and agents, ranging from physical protections to firewalls and access control, can offer the administrators more opportunities for information and resource control with the advent of potential threats. However, it also creates possible issues on the latency and

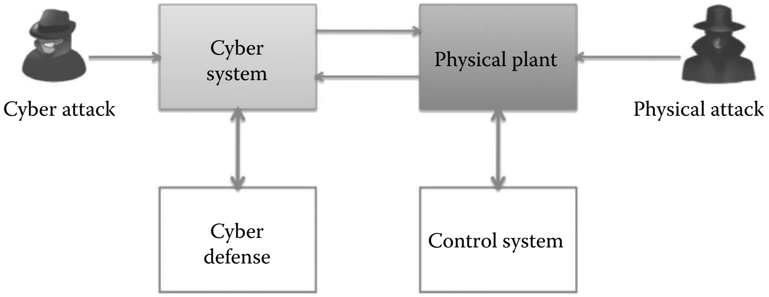

Figure 6.7: Security of cyber-physical systems: the physical and cyber layers of the control system interact with each other.

packet drop rate of communications between the controller and the plant. We propose a unifying security model for this cyber-physical scenario and investigate the mitigating strategies from the perspectives of control systems, as well as of cyber defenses. At the physical layer, we often aim to design robust or adaptive controllers that take into account the uncertainties and disturbances in the system to enhance robustness and reliability of the system. At the cyber level, we often employ IT security solutions by deploying security devices and agents in the network. The security designs at the physical and cyber layers usually follow different goals without a unifying framework. Hence, the design of optimal security policies at the cyber level requires a cross-layer approach between the interacting layers of the entire system. Hence, it is important to jointly consider the controller design of the physical layer dynamical processes together with security policy designs. The control performance of the physical process relies on the cyber-security policies that have been enforced at the communication and network layers. The time delay of data delivery, packet drop rates, and quality of service need to be taken into account when designing high-performance controllers for the underlying processes. In addition, the design of cyber policies has to consider their potential impact on the physical layer of the system.

6.6.5 Multiagent System Design

For large-scale complex ICSs, it is difficult to coordinate all components of the system using a centralized supervisory system. Hence, a multiagent system (MAS) architecture with communications between different components of the system is desirable. While communication and negotiation are common to all multiagent systems, data analysis and control are more specific and necessary within a control system design. The negotiation and communications aspects themselves must be tailored to the control system objectives, which are based on the desired operation of a physical process operation. Control, communications, data analysis, and negotiation comprise four technologies that characterize the functionality of an agent within a multiagent hierarchy.

6.6.5.1 Data Analysis

By its nature, a MAS implies a philosophy of achieving a level of global optimization based on decisions made from multiple sensors. To ensure that the degradation of sensors and resulting data does not lead to a failure in the design, mechanisms to interpret the data and ascertain status are required. Graceful degradation of sensor systems becomes a critical aspect of these designs to maintain the highest level of the MAS autonomous relationships through recognition and replacement of sensory inputs. These additional inputs can come from multiple replicant sensors, diverse technology sensors, and models coupled with sensors to provide the same sensory aspect. Salient features of this aspect of MAS should include:

- Diagnostic detection of failure for all sensors and synthetic sources of sensory data that are used as a basis for confirming performance of the system.
- Prognostic prediction of future degradation, specifically failures with equipment that is necessary for operation. This is especially critical for equipment with a long lead time for replacement.
- Data fusion of inputs for data reduction, prioritization, and targeting of mixed initiative response. Characterization and measurement of blended performance, specifically where more than one measure of normal operation comes to bear. For example, the characterization of cyber health can be enhanced with the temporal data on physical security and plant stability.

6.6.5.2 Control

The type of control engineering adaptable to the multiagent design will be dependent on the application and layer of hierarchy. The type of control at the lower layers of the autonomy may often be more diverse and application dependent. At the higher layers, where more cognitive aspects and decisions are expected, a greater use of computational intelligence is expected. The following considerations should be included in the development of the control design:

- Final implementation of the MAS design includes practitioners, and therefore the interactions should be targeted to just those aspects that require input to align operations to the particular environment.
- The application of control to the device layer of the MAS should be based on need as determined by the designer and implementing practitioners, where advanced control is applied as needed to achieve better performance. However, while advanced control is not necessarily encouraged, the ability to implement conventional proportional-integral-derivative control with supervisory inputs is required.
- The application of control to the coordination layer of the hierarchy is for the negotiation of resources to the MAS, as well as an interpreter of philosophy from the hierarchy superior to the subordinates. This role implies, at least in part, a hybrid control system design. That is, superior information will often come in the form of state-based direction, which must often be applied to a continuous plant. If the mechanism to dictate the philosophy to the subordinate can occur through state-based mechanisms, such as set-point adjustment, this is not an issue. However, in the

case where trajectories are necessary to gracefully shift plan states, this is more difficult. Given that these trajectories can be identified as part of the device layer design, the method of dictating philosophy can still be through the variation of set points or discrete settings.

- At the management layer of a MAS hierarchy, the decomposition of operating philosophy occurs. By operating philosophy, the intent is to define what the desired operation of the control system should be. The overall participation in the directly or indirectly human-related aspect comes from several sources. Bayesian inference, fuzzy logic, and other intelligent systems technology can provide a means of characterizing and normalizing these potentially disparate sources of philosophy. The resulting output of this layer, however, is to associate performance desires within the limitations of the system and regulations.

6.6.5.3 Communications

As the interactive framework is established, the mechanism for interacting between layers and peers is required. The types of interaction change depending on the layer and path, peer to peer or peer to superior or subordinate. The communications design will need to accommodate these interactions, which might at first glance appear to be fulfilled by current 802-based protocols. However, there are some specific MAS considerations that require accommodation:

- Determinism and latency are important considerations and the constraints will vary, depending on the MAS layer in which the communications are occurring. Response time is slower at the higher layers of the hierarchy, and the forms of the interaction changes can be relatively simple (e.g., set points and ranges) or complex (e.g., intelligent interpreters of system and performance indices for optimal tracking).
- Assurance of authenticity is required in the exchange of data, specifically to defend against the injection of a malicious agent. As part of the data analysis, cyber security is considered one of the performance parameters for evaluation. However, the key aspect for the communications design is to consider the unique identification of agents and mechanisms to confound a malicious attacker from determining this identification.
- Standards such as Foundation for Intelligent Physical Agents (FIPA) and the IEEE 802 series exist to govern the fundamental aspects of communication. However, such standards are expected to evolve as techniques are codified in cyber defense, such as randomization of communications, including control system–specific defenses. These defenses will occur while still ensuring that the determinism and maximum latency are maintained for the control system application.

6.6.5.4 Negotiation

Consensus of agents within a resilient control system framework requires consideration of the dynamical attributes of the design. A MAS in the context of this chapter is intended to afford reconfiguration of agents, and ultimately control of resources to achieve an optimum performance of the overall system. The stability aspect of performance must therefore be considered during the negotiation of resources. In this regard, negotiation of a MAS system should consider the following:

- The dynamics of the system require tracking of the optimum path or trajectory to achieve optimum stability, in addition to achieving stability. Stated another way, the performance of the system remains within its constraints for operation. This implies a performance index that considers path and endpoints.
- The ability to share and ultimately negotiate resources is limited by the uniformity of the system. For example, an unmanned air vehicle squadron provides a highly uniform implementation of a MAS, and therefore a higher level of resource sharing is theoretically possible within the constraints of the design. The level of uniformity is defined, in this case, as the ability of an agent to provide a necessary functionality in the fulfillment of a need.
- Decisions for shifting of resources can occur at different layers of the MAS hierarchy, with control action taken at both the middle and lower layers. However, the goal of negotiation is the same regardless of the level, which is to adjust resources to reach optimum performance. The difference lies in the sphere of influence. That is, the coordination layer has the responsibility for multiple lower-level agents and, as such, will better orchestrate shifts in operation to accommodate the philosophy of the management layer.

6.6.6 Discussion

The proposed cyber-attack-resilient power grid automation system is engineered and operated in a way that (1) the system can be aware of power grid operation states, cyber attacks, and their potential adverse impacts on power grid operation by online risk assessment and intrusion detection; (2) the system can analyze what cyber attacks are and where they occur, and pass this information to operators; (3) the system can mitigate detected cyber attacks by adjusting corresponding security policies, such as access control in security agents; (4) the system can minimize the adverse impacts by rerouting data path from the attacked communication link or redirecting power flow from the attacked substations if these cyber attacks cannot be mitigated; and (5) the system can help operators reroute the data path from the attacked communication link or redirect power flow from the compromised substations, and hence recover to normal operation quickly.

6.7 Conclusion

This chapter aimed to shed some light on resilient industrial control systems by proposing a six-layer system model and resilience curve; conceptualizing resilient industrial control systems; distinguishing the concept of resilience from other terms, such as robustness, adaptiveness, survivability, and fault tolerance; presenting desirable properties of resilient industrial control systems; and offering metrics to estimate system resiliency quantitatively. The general approaches to improve industrial control system performance in terms of resilience were discussed as well. A cyber-attack-resilient power grid automation system was presented as an example to illustrate the proposed approaches.

Acknowledgment

This material is based on work supported by the National Science Foundation under grant no. EFMA-1441140, SES 1541164, and CNS-1544782.

References

1. I. Aad, J. Hubaux, and E. Knightly. Denial of service resilience in ad hoc networks. In *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, New York, ACM, pp. 202–215, 2004.
2. D. Andersen, H. Balakrishnan, F. Kaashoek, and R. Morris. Resilient overlay networks. *ACM SIGOPS Operating Systems Review*, 35:131–145, 2001.
3. D. van Opstal. Transform—The resilient economy: Integrating competitiveness and security. Technical report, Compete, Council on Competitiveness, Washington, DC, July 2007.
4. da Fontoura Costa, L. Reinforcing the resilience of complex networks. *Physical Review E*, 69(6):066127, 2004.
5. Department of Homeland Security. National infrastructure protection plan—Critical manufacturing sector. Department of Homeland Security, Washington, DC, April 2008.
6. Department of Homeland Security. Critical infrastructure resilience final report and recommendations. Department of Homeland Security, Washington, DC, September 2009.

7. Department of Homeland Security. Information technology sector baseline risk assessment. Department of Homeland Security, Washington, DC, August 2009.

8. Department of Homeland Security. National infrastructure protection plan—Partnering to enhance protection and resiliency. Department of Homeland Security, Washington, DC, 2009.

9. C. S. Holling. Resilience and stability of ecological systems. *Annual Review of Ecology and Systematics*, 4:1–23, 1973.

10. M. Huynh, S. Goose, and P. Mohapatra. Resilience technologies in ethernet. *Computer Networks*, 54(1):57–78, 2010.

11. S. E. Flynn. Building a resilient nation: Enhancing security, ensuring a strong economy. Technical report; keynote address, Reform Institute, New York, October 2008.

12. S. Jaggi, M. Langberg, S. Katti, T. Ho, D. Katabi, M. Medard, and M. Effros. Resilient network coding in the presence of Byzantine adversaries. *IEEE Transactions on Information Theory*, 54(6):2596–2603, 2008.

13. A. Krings. Design for survivability: A tradeoff space. In *Proceedings of the 4th Annual Workshop on Cyber Security and Information Intelligence Research: Developing Strategies to Meet the Cyber Security and Information Intelligence Challenges Ahead* (CSIIRW '08), F. Sheldon, A. Krings, R. Abercrombie, and A. Mili (eds). ACM, New York, Article 12, 2008.

14. D. Liu. Resilient cluster formation for sensor networks. In *Distributed Computing Systems, 2007. ICDCS '07. 27th International Conference on*, pp. 40–40, Toronto, Canada, June 25–29, 2007.

15. M. H. Manshaei, Q. Zhu, T. Alpcan, T. Başar, and J. P. Hubaux. Game theory meets network security and privacy. *ACM Computing Surveys (CSUR), 45(3):25*, 2013.

16. N. McDonald. *Organizational Resilience and Industrial Risk*, pp. 155–180. Ashgate, Surrey, 2006.

17. D. Mendonca. *Measures of Resilient Performance*, vol. 1, pp. 29–47. Ashgate, Surrey, 2008.

18. M. Menth, M. Duelli, R. Martin, and J. Milbrandt. Resilience analysis of packet-switched communication networks. In *IEEE/ACM Transactions on Networking (TON),* 17(6):1950–1963, 2009.

19. S. M. Mitchell and M. S. Mannan. Designing resilient engineered systems. Technical Report 4, Chemical Engineering Progress, New York, April 2006.

20. Z. Mohajerani, F. Farzan, M. Jafari, Y. Lu, D. Wei, N. Kalenchits, B. Boyer, M. Muller, and P. Skare. Cyber-related risk assessment and critical asset

identification within the power grid. In *Proceedings of IEEE PES Transmission and Distribution Conference and Exposition*, New Orleans, LA, April 2010.

21. D. Nathanael and N. Marmaras. *Work Practices and Prescription: A Key Issue for Organizational Resilience*, vol. 1, pp. 101–118. Ashgate, Surrey, 2008.

22. C. G. Rieger. Notional examples and benchmark aspects of a resilient control system. In *Proceedings of International Symposium on Resilient Control Systems*, Idaho Falls, ID, pp. 64–71, 2010.

23. C. G. Rieger, D. Gertman, and M. A. McQueen. Resilient control systems: Next generation design research. In *Proceedings of IEEE Conference on Human System Interactions*, Catania, pp. 632–636, May 2009.

24. S. Roy, S. Setia, and S. Jajodia. Attack-resilient hierarchical data aggregation in sensor networks. In *Proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks*, Alexandria, VA, pp. 71–82, 2006.

25. Y. Sheffi. *The Resilient Enterprise: Overcoming Vulnerability for Competitive Enterprise*. MIT Press, Cambridge, MA, 2005.

26. P. Sousa, A. Bessani, M. Correia, N. Neves, and P. Verissimo. Resilient intrusion tolerance through proactive and reactive recovery. In *Proceedings of Pacific Rim International Symposium on Dependable Computing*, Melbourne, 17–19 December, pp. 373–380, 2007.

27. P. Sousa, N. F. Neves, and P. Verissimo. How resilient are distributed f fault/intrusion-tolerant systems? In *Proceedings of International Conference on Dependable Systems and Networks*, Yokohama, Japan, June 28–July 1, pp. 98–107, 2005.

28. D. Wei and K. Ji. Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights. In *Proceedings of International Symposium on Resilient Control Systems*, Idaho Falls, ID, pp. 15–22, 2010.

29. D. Wei, Y. Lu, M. Jafari, P. Skare, and K. Rohde. An integrated security system of protecting smart grid against cyber attacks. In *Innovative Smart Grid Technologies (ISGT)*, Gothenburg, Sweden, pp. 1–7. IEEE, 2010.

30. E. E. Werner. *The Children of Kauai: A Longitudinal Study from the Prenatal Period to Age Ten*. University of Hawaii Press, Honolulu, HI, 1971.

31. J. Wreathall. *Properties of Resilient Organizations: An Initial View*, pp. 275–285. Ashgate, Surrey, 2006.

32. F. F. Wu, K. Moslehi, and A. Bose. Power system control centers: Past, present, and future. *Proceedings of the IEEE*, 93(11):1890–1908, 2005.

33. Q. Zhu and T. Başar. Indices of power in optimal IDS default configuration: Theory and examples. In *Proceedings of International Conference on Decision and Game Theory for Security*, College Park, MD, pp. 7–21, 2011.

34. Q. Zhu and T. Başar. A dynamic game-theoretic approach to resilient control system design for cascading failures. In *Proceedings of International Conference on High Confidence Networked Systems*, Beijing, pp. 41–46, 2012.

35. Q. Zhu and T. Basar. Dynamic policy-based IDS configuration. In *Proceedings of IEEE Conference on Decision and Control*, Shanghai, pp. 8600–8605, 2009.

36. Q. Zhu and T. Basar. Robust and resilient control design for cyber-physical systems with an application to power systems. In *Proceedings of IEEE Conference on Decision and Control and European Control Conference*, Orlando, FL, pp. 4066–4071, 2011.

37. Q. Zhu, C. Rieger, and T. Basar. A hierarchical security architecture for cyber-physical systems. In *Proceedings of International Symposium on Resilient Control Systems*, Boise, ID, pp. 15–20, 2011.

38. Q. Zhu, H. Tembine, and T. Basar. Network security configurations: A nonzero-sum stochastic game approach. In *Proceedings of American Control Conference*, Baltimore, MD, pp. 1059–1064, 2010.