12

Cyber-Physical System Resilience

Frameworks, Metrics, Complexities, Challenges, and Future Directions

Md Ariful Haque[1], Sachin Shetty[1], and Bheshaj Krishnappa[2]

[1] *Computational Modeling and Simulation Engineering, Old Dominion University, Norfolk, VA, USA*
[2] *Risk Analysis and Mitigation, ReliabilityFirst Corporation, Cleveland, OH, USA*

12.1 Introduction

Cyber-physical systems (CPSs) are engineered systems built from the integration of computation, networking, and physical processes. Researchers often generalize "CPS" as an integrated system of cyber and physical systems, where embedded computers and networks are used to compute, communicate, and control the physical processes (Baheti and Gill, 2011; Wang, 2010). Advances in CPS make them crucial in most of the industries, e.g. energy delivery systems (EDS) (McMillin et al., 2007), healthcare systems (Cheng, 2008), transportation systems (Xiong et al., 2015), or smart systems (smart grid, smart homes, smart cities, etc.) (Amin, 2015; Yu and Xue, 2016). The advancements in engineering processes also bring the risk of cyberattacks because of the integration of the cyber and physical domains – in other terms information technology (IT) and operational technology (OT) domain. Therefore, the cyber resiliency of such systems considering the vulnerabilities of different components within the networked system is an integral part of CPS security analysis.

12.2 Cyber Resilience: A Glimpse on Related Works

The National Academy of Sciences (NAS) (Cutter et al., 2013) defined resilience as *the ability to prepare and plan for, absorb, recover from, or more successfully adapt to actual or potential adverse events*. The authors (Linkov, Eisenberg,

Complexity Challenges in Cyber Physical Systems: Using Modeling and Simulation (M&S) to Support Intelligence, Adaptation and Autonomy, First Edition. Edited by Saurabh Mittal and Andreas Tolk.

Plourde, et al., 2013) used the resilience definition provided by NAS to define a set of resilience metrics spread over four operational domains: physical, information, cognitive, and social. In another work (Linkov, Eisenberg, Bates, et al., 2013), the authors applied the previous resilience framework (Linkov, Eisenberg, Plourde, et al., 2013) to develop and organize useful resilience metrics for cyber systems. Bruneau et al. (2003) proposed a conceptual framework initially to define seismic resilience, and later the authors (Tierney and Bruneau, 2007) introduced the R4 framework for disaster resilience. The R4 framework comprises *robustness* (ability of systems to function under degraded performance), *redundancy* (identification of substitute elements that satisfy functional requirements in event of significant performance degradation), *resourcefulness* (initiate solutions by identifying resources based on prioritization of problems), and *rapidity* (ability to restore functionality in timely fashion).

MITRE presents a framework for cyber resiliency engineering (Bodeau and Graubart, 2011). The framework identifies the cyber resiliency goals, the threat model for cyber resiliency, and structural layers to which cyber resiliency could be applied. Most of these frameworks discuss standard practices and provide guidance from different angles of resilience study, but lack of clear explanation on the quantitative resilience metrics formulation. Another issue with these frameworks is that they are most suitable for information technology system (ITS) rather than the CPS. The CPSs have unique requirements that make them different from typical ITS: First, for CPS, real time, safety, and continuity of service are essential, while for ITS the confidentiality and integrity of data are important, and momentary downtime can be tolerated (Macaulay and Singer, 2016). Second, it is common to apply anti-malware software in ITS, and they often automatically download and apply security patches. The CPS uses control systems that are designed for functionality rather than security and with limited memory and processing capacity (Macaulay and Singer, 2016). The installations of anti-malware solutions that consume a lot of memory and processor capacity for the automatic updates are not applicable to the CPS.

Lots of research works are done on resilience study of industrial control system (ICS), which is mainly a type of CPS. The National Institute of Standards and Technology (NIST) provides a framework (Sedgewick, 2014) for improving the cybersecurity and resilience of critical infrastructures that are supported by both ITS and ICS. The NIST framework identifies five functions that organize cybersecurity at the highest levels: *identify* (develop understanding of and manage risk to systems, assets, data, and capabilities), *protect* (develop and implement appropriate safeguards to ensure delivery of critical infrastructure services), *detect* (identify the occurrence of a cybersecurity event), *respond* (take action regarding a detected cybersecurity event), and *recover* (maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event).

In another work (Stouffer, Falco, and Scarfone, 2011), NIST provides detailed guidelines for ICS security. Collier et al. (2016) outline the general theory of performance metrics and highlight examples from the cybersecurity domain and ICS. Bologna, Fasani, and Martellini (2013) define the necessary measures to be taken to make ICS and critical infrastructures resilient. The above works present different useful insights from the cybersecurity standpoint but analyze resilience considering a specific section of the CPS network rather than incorporating the complete CPS cyber threat scenario. We are concerned about the estimation of cyber resilience for the CPS considering the whole system domains of security concerns. Thus, a comprehensive resilience metrics formulation is necessary for the CPS.

Yong, Foo, and Frazzoli (2016) present a state estimation algorithm that is resilient to sparse data injection attacks on the CPS. On the survey side, Humayed, Lin, Li, and Luo (2017) present an excellent overall security survey on the CPS by considering security, cyber-physical components, and CPS-level perspectives. Koutsoukos et al. (2017) present a modeling and simulation integrated platform for the evaluation of CPS resilience with an application to the transportation systems. Although the resilience assessment irrespective of the types of the CPS is the goal of the chapter, we limit our focus on the CPSs involving ICSs, EDS, and oil and gas systems. The following subsections are going to discuss the CPS architecture in brief and relate the complexities to handle to make the system cyber-resilient.

12.3 Cyber-Physical System Resilience

There are different applications of CPS, and the network system architecture is varied based on the functional area. Here we present a generic CPS architecture by considering the applications related to the ICS to explain the cyber resilience concepts as illustrated by Haque, De Teyou, Shetty, and Krishnappa (2018). In Figure 12.1, we present an ICS architecture to discuss CPS in general. An ICS is a set of electronic devices to monitor, control, and operate the behavior of interconnected systems. ICSs receive data from remote sensors measuring process variables, compare those values with desired values, and take necessary actions to drive (through actuators) or control the system to function at the required level of services (Galloway and Hancke, 2013; Macaulay and Singer, 2016). Industrial networks are composed of specialized components and applications, such as programmable logic controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and distributed control systems (DCS) (Cardenas et al., 2009). There are other components of ICS such as remote terminal unit (RTU), intelligent electronic devices (IED), and phasor

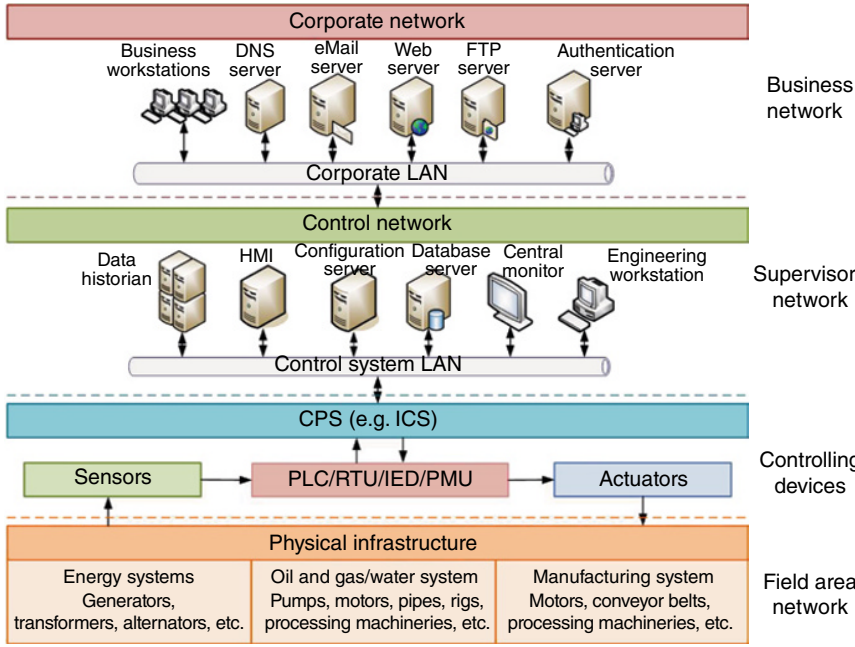

Figure 12.1 Generic CPS (ICS) architecture. *Source:* From Haque et al. (2018).

measurement units (PMU). Those devices communicate with the human–machine interface (HMI) located in the control network.

The risk of cyberattack comes into play when the corporate and control network have communications for regular business operations because part of the corporate network system is open to the Internet to communicate with stakeholders and business entities outside ICS network. Threat vectors also come from the heterogeneity (Humayed et al., 2017) of the different building blocks of the CPS and their control and monitoring hardware and software systems. Because of the complex interconnections and interactions among various components within the CPS, it is difficult to identify or trace any attack vector that may involve exploitation of multiple CPS components in sequence. Thus, to make the CPS cyber-resilient, it needs a wide range of efforts including the study of the system-level intrusion detection and prevention mechanisms as well as the system capabilities. Such capabilities can be the ability to divert the attack event, use redundant resources, respond and recover within the defined timeframe with minimal impact, keep learning the vulnerabilities and attack vectors, and evaluate and update security and privacy policies.

12.3.1 Resilient CPS Characteristics

Wei and Ji (2010) present the resilient industrial control system (RICS) model where the authors have identified the following three characteristics of the ICS to be resilient:

- Ability to minimize the undesirable consequence of an incidence.
- Ability to mitigate most of the undesirable incidents.
- Ability to restore to normal operation within a short time.

All the above characteristics are a repetition of robustness, resourcefulness, redundancy, and rapidity as illustrated in the R4 resilience framework (Tierney and Bruneau, 2007). As CPS or ICS works closely with the field devices with interfaces to the control centers and there need to be connections between control and the corporate network, a wide range of efforts spanning the system level and organizational level are necessary to make the CPS cyber-resilient. A detail resilience graph-based analysis is presented in Section 12.6 to illustrate the challenges in modeling and simulation of CPS resilience.

12.3.2 Need for Resilience Metrics

There are diverse applications of CPS, e.g. ICS, smart grid systems, medical devices, autonomous automobiles (intelligent cars), etc. Based on the field of application, there are variations in the cyber and physical components as well as in the cyber-physical interconnections and protocol communications within the cyber-physical devices. Within the scope of this chapter, we limit our focus on the ICS to explain the required aspects of resilience. As illustrated in the related works section, there are a lot of research works going on with the development of standard practices and guidelines to make the CPS cyber-resilient, which have lack of specific quantitative cyber resilience metrics. Therefore, we feel the need for the development of the quantitative cyber resilience metrics for the CPS.

The availability of quantitative cyber resilience metrics would assist the concerned industry operators to assess and evaluate the CPS and focus on the weak points to improve. Thus, one of the objectives of this work is to derive quantitative resilience metrics and development of a simulation platform that can handle the network architecture, scan the vulnerabilities, generate useful quantitative resilience metrics, and provide recommendations to improve the overall network resilience posture. There is no doubt that there is a high need for the resilience metrics automation across various industries. Thus, an approach to quantify the resilience metrics and development of a simulation platform to automate the metrics generation process is the need of the time. Also, the inclusion of the modeling and simulation paradigm in the CPS resilience study is a crucial research aspect to consider.

12.4 Resilience Metrics and Framework

Resilience metrics derivation is one of the goals of this chapter. In this section, we cover the CPS cyber threat landscape, CPS cyber resilience metrics and sub-metrics, and cyber resilience framework for the CPS. To have a smooth transition, we provide qualitative resilience metrics computation methodology in Section 12.5 and a detailed discussion on the quantitative modeling of resilience metrics in Section 12.6.

12.4.1 CPS Cyber Threat Landscape

The threat landscapes that CPSs are facing today are coming from different threat vectors. We use ICS to describe the threat landscape to CPS in general; in other terms we use ICS in some cases to represent the CPS. As the ICS industry grows larger and complex, the types and severity of targeted threats increased. Some of the threats that are identified to be a part of the CPS or ICS threat landscape are put together below. A mapping of the resilience metrics analysis domains with the threats is presented in Figure 12.2 where some of the attacks are collected from the discussion provided by Andrew Ginter (2017) and Cardenas et al. (2009):

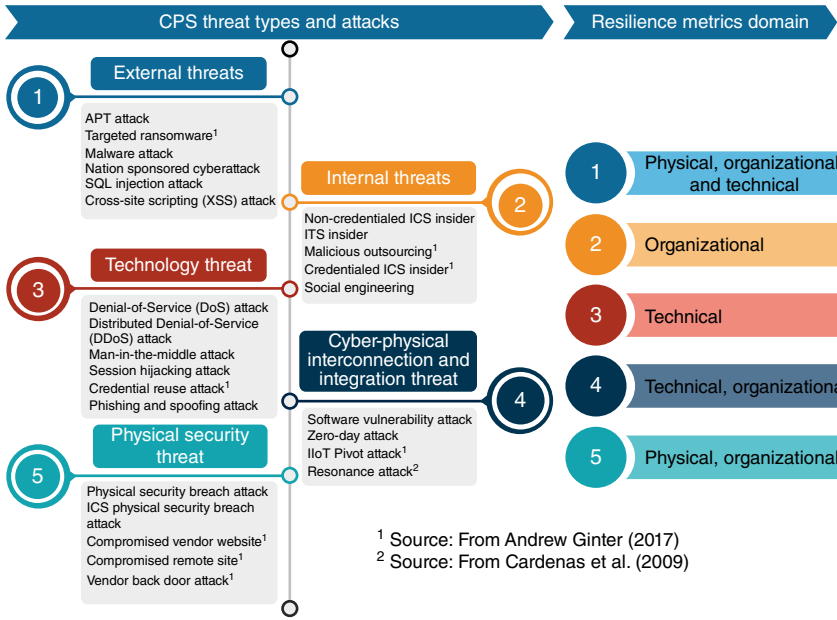

Figure 12.2 Categorization of CPS threat and attack types and mapping with resilience metrics domain.

- *External threats:* These threats arise from adversaries such as nation-sponsored hackers, terrorist groups, and industrial competitors through espionage activities. Cyber intruders may launch an advanced persistent attack (APT) attack, where the goal is to steal some valuable information on the network's assets without getting detected. One example of such an attack in recent times is the Stuxnet attack on the Iranian nuclear centrifuges. Some other threats such as targeted ransomware are discussed by Andrew Ginter (2017).
- *Internal threats:* Today, as the work processes in any industry are segmented and done by contractors or third-party vendors, ICS companies need to share system access information to outside business partners. That makes the ICS vulnerable to potential cyber threats. There also exists direct insider threat from the employees of the ICS company itself who are provided with legitimate access to the ICS network for regular operation and maintenance related tasks, which falls in the category of credentialed ICS insider attack.
- *Technology threats:* Many of the ICS networks run on legacy technology where the most concern part is the protocol-level communication among different ICS products within the network. Thus, many of them are lack of strong authentication or encryption mechanism (Laing, 2012). Even if they use authentication procedure, the weak security mechanisms (e.g. weak password, default user accounts) are not enough to protect the system from smart adversaries. Some of the attacks that can take place due to the CPS technology itself are presented in Figure 12.2.
- *ICS and ITS integration threats:* Due to the integration and interconnection of the ICS network with the control system network and corporate network for business operations, ICS devices become vulnerable to cyberattacks as part of the corporate network is open for communication over the Internet. Only putting the ICS devices behind the firewalls does not necessarily safeguard them, because today smart intruders are expert enough to launch a multi-host multi-stage cyberattack by exploiting several stepping stones on the way to the valued ICS assets.
- *Physical infrastructure security threats:* Sometimes lack of proper infrastructure security to the ICS devices poses severe threats to the ICS network. One such example of poor physical security is sharing of the floor space of ICS devices with the ITS devices (e.g. employees' computers, routers, switches, etc.) and thus providing easy access to the ICS devices (e.g. PLC, IED, RTU, PMU, etc.). Other sorts of threats may arise from compromised vendor website or compromised remote sites.

Each of the above categories of threats falls under any or a combination of the three major domains of resilience assessment: physical, organizational, or technical. To handle the external threats, it needs a comprehensive effort from all three

areas: physical, organizational, and technical. To control the cyber-physical interconnectivity threats although more emphasis should be given on the technical side, it also needs to consider the policies that mostly depend on the management decisions. Thus, it falls under technical and organizational domains. Similarly, physical security threats are part of physical security and organizational policy, and therefore, resilience metrics dealing with the physical security threats need to consider the physical and organizational security posture. We incorporate the categorization while defining the sub-metrics for the cyber resilience assessment of the CPS, which is discussed in the following subsections.

12.4.2 CPS Resilience Metrics

We decompose the four R4 metrics (*robustness*, *redundancy*, *resourcefulness*, and *rapidity*) proposed by Bruneau et al. (2003) into a hierarchy of several domains and sub-metrics, each of which can be analyzed independently. Each of the broad R4 metrics is subdivided into three domains – *physical*, *organizational*, and *technical* – to cover most of the threat vectors of the CPS. There are sub-metrics under each of the areas that are organized in a tree structure as given in Figure 12.3 and can effectively contribute to the cyber resilience assessment for ICS.

The metrics illustrated in Figure 12.3 are self-explanatory and easy to understand. Within the scope of this chapter, we analyze two different approaches to estimate cyber resilience metrics for CPS: qualitative approach and quantitative approach. We aim to assess the broad R4 metrics using both methods. The qualitative approach discussion is presented in Section 12.5, while the quantitative modeling and simulation approaches are discussed in Section 12.6. Within the scope of the chapter, the detail definition of each of the sub-metrics seems unnecessary. Here we explain some of the sub-metrics of the resourcefulness metrics.

Physical resourcefulness is having two sub-metrics: physical monitoring and protective technology. Physical monitoring includes all sorts of devices and systems that allow monitoring the physical ICS, which includes but not limited to the surveillance systems, alarm monitoring systems, etc. Protective technology refers to the efforts to protect information and asset security, physical solutions or policies to safeguard CPS assets, documentation, etc. This may also involve automatic action initiation based on the alarm or security breach, e.g. automatic door lock because of consecutive unauthorized access attempts to control centers.

Organizational monitoring and detection refer to monitoring of the employee actions and audit of the system command logs to identify the presence of potential insider threat. Organizational response and recovery refer to

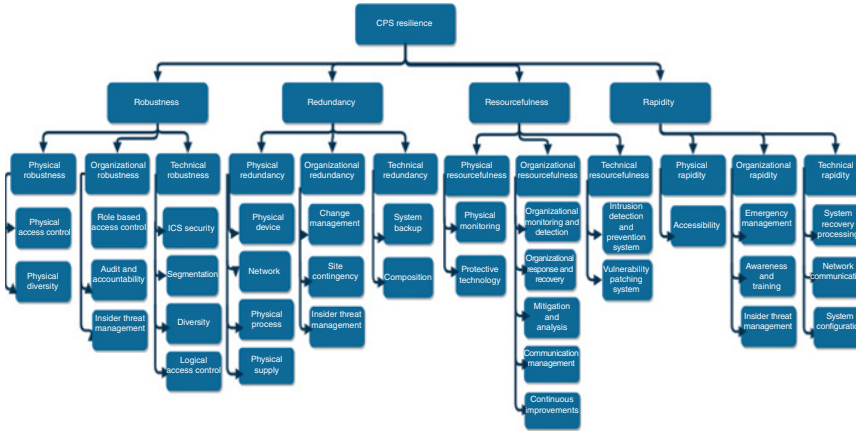

Figure 12.3 CPS cyber resilience metrics structural hierarchy.

the organizational policies to handle any cyberattack scenario, the performance of documented actionable policies, and evaluation of the actions performed. Mitigation and analysis refer to the organizational capabilities and efforts in mitigating any potential cyberattack, analyzing the attack types and originating points, and learning to prevent the similar attack in the future. This may also include training programs with a simulated attack in a controlled environment to train the operators better. Communication management refers to the organization hierarchy-wise communication that is necessary for detecting, protecting, and preventing any cyberattack. It may include the organizational communication policies in case of a cyberattack event. Continuous improvement is the resourcefulness area where CPS vendors and operators need to evaluate what measures should be in the cybersecurity detection and protection mechanism to cope up with the changing technological environment.

In the technological resourcefulness, the sub-metrics are intrusion detection and prevention system and vulnerability patching system. Intrusion detection and prevention system deals with the intrusion detection systems (IDS) and intrusion prevention systems (IPS). IDS detect and IPS prevent any potential information security breach in the ICS and ITS areas. The organization may have strict policies and regulations regarding the use and application of the IDS and IPS. The policy or the rule set in IDS and IPS need to keep updated constantly. Some vulnerabilities may not be detected by the IDS because there are zero-day vulnerabilities. In those cases, the system should have some sorts of abnormal behavior alarm generation in place. Vulnerability patching system makes sure if the computers and servers in the ITS domain are updated with the latest antivirus patches, automatic update of the system is enabled.

Unlike the ITS, ICS or CPS do not have traditional antivirus software. It is necessary to keep these systems updated by the vendor recommended system updates or patches. The resilience metrics and sub-metrics illustrated in Figure 12.3 are used to derive a cyber resilience framework for the CPS as presented in Section 12.4.3.

12.4.3 Cyber-resilient Framework for CPS

We provide a detailed CPS resilience framework in Table 12.1, as presented by Haque, De Teyou, Shetty, and Krishnappa (2018). The framework is designed to assess the cyber resilience of the CPS (i.e. ICS in this discussion) and is based on the CPS resilience metrics hierarchy presented in Figure 12.3. The framework can serve as a platform to create secure and resilient CPS/ICS across different industries (energy, oil and gas, manufacturing, etc.). Again, the resilience is assessed in terms of robustness, redundancy, resourcefulness, and rapidity in three domains: physical, organizational, and technical. The details provided in the framework make it self-explanatory.

Table 12.1 Cyber resilience framework for CPS.

	Robustness (R_1)	Redundancy (R_2)	Resourcefulness (R_3)	Rapidity (R_4)
Physical	*Access control* • Physical barrier policy (guards, walls, rooms, gates) • Identification and authentication (biometric, smart card, PIN code) • Physical ports protection and electronic device policy *Segmentation* • Physical isolation of ICS sites from corporate sites • Physical isolation of storage site from the processing site *Diversity* • Product and vendor diversity *Risk mitigation* • Threat identification, characterization, and mitigation	*Contingency* • Alternate storage/processing site, power supply, and communication network • Protection of alternate sites and power supply • PLC and RTU redundancy (shadow or separate mode) *Composition* • Capabilities to deploy new PLC/RTU interoperable with the ICS to ensure continuity of the process	*Monitoring and detection* • Capabilities to monitor the physical environment to detect cybersecurity events (video cameras, motion detectors, sensors, and various identification systems) *Response and recovery* • Capabilities to investigate and repair physical devices	*Communication latency* • The delay between adverse event and detection *Restoration delay* • The delay to access damaged devices (debugging ports, remote access) • The delay between detection and restoration (mean time to repair) • Switching delay for backup operations (hot, cold, warm) *Learning* • Update device configuration in response to recent events and performs better in the future

(*Continued*)

Table 12.1 (Continued)

	Robustness (R_1)	Redundancy (R_2)	Resourcefulness (R_3)	Rapidity (R_4)
Organizational	*Access control* • Visitor escort and access agreements policy • Restriction of physical access to ICS to authorized employee only • Personnel designation, screening, termination and transfer policy • Terms of employment policy *Segmentation* • Employee-specific roles and responsibility *Diversity* • Diverse group of employees to mitigate insider attacks *Risk mitigation* • Planning, implementation, and progress monitoring	*Contingency* • Business continuity planning and coordination *Composition* • Capabilities to deploy new manufacturing processes	*Monitoring and detection* • Capabilities to monitor personnel activity to detect cybersecurity events (account management, configuration change control) • Record and classification of incident *Response and recovery* • Collection of evidences for civil and criminal actions • Audit policy and change management policy	*Communication latency* • Cyber events are reported timely to appropriate personnel • Responsibilities and procedures are clearly defined for adequate personnel to ensure quick response *Restoration delay* • Timely availability of dedicated resources for service restoration (budget, manufacturer support, and tools) *Learning* • Registration to association and security conferences • Review security policy during and after adverse events • User awareness and training (penetration tests, role-based training)

Technical	*Access control* • Port, protocol, and traffic filtering in CS • Wireless and remote access policy (authentication and encryption policy) • Email and browser policy (URL filtering, attachment, supported email clients and browser, plugins) *Segmentation* • Firewalls/gateways between corporate and CS • Firewalls/gateways between ICS and third-party network • DMZ for control systems (CS) and corporate network *Diversity* • Disjoint technologies between CS and corporate network • Software, firmware, and hardware diversity *Risk mitigation* • Continuous vulnerability scanning and patching • Identification and mitigation of ICS weaknesses due to old technology design (clear communications, poor coding practices, low CPU/memory) • Identification and mitigation of ICS weaknesses due to implementation (weak logging/ authentication, weak scripting interface, malfunction devices) • Default configuration avoidance in CS and corporate network (default account/password, unused services/components)	*Contingency* • Backup secured on protected servers • Backup copies of information system and software • Adequate resource to ensure availability of data *Composition* • Capabilities to deploy new protocols and technologies interoperable with the ICS to ensure continuity of the process	*Monitoring and detection* • Capabilities to monitor network logs to detect cybersecurity events • ICS protocol attacks detection (Modbus, DNP3, ICCP, etc.) • Network-based IDS between CS and corporate • Host-based IDS in both CS and corporate *Response and recovery* • Anti-malware tools, IRS • Reduction of malware spread from corporate to control system network • Dynamic reconfiguration	*Communication latency* • Fault isolation latency • Measurement reading latency • Routine automation latency *Restoration delay* • Intrusion response frequency *Learning* • Logs correlation with vulnerability databases • Dynamic reconfiguration after cyberattacks • Online learning of attacker strategies

12.5 Qualitative CPS Resilience Metrics

One of the objectives in this work is to make the resilience metrics operational, i.e. the metrics should be analytically measurable and quantifiable with the available data and resources. One challenge of developing useful, generalizable resilience metrics for CPS/ICS is that the data regarding the cybersecurity of CPS/ICS is not available mostly due to regulation that requires reporting only a subset of cyberattacks as stated in McIntyre, Becker, and Halbgewachs (2007). Consequently, ICS companies with established cybersecurity policies prefer to keep their data confidential, mainly due to privacy and the proprietary nature of information. By taking into consideration the lack of system data availability, resilience metrics can be evaluated with a qualitative approach using cautiously chosen sets of questionnaires. The questionnaires should be designed in a way so that it can address each sub-metric and therefore capture qualitative information about the system resilience posture.

We derive the resilience metrics by aggregating the individual sub-metrics using a multi-criteria decision-making approach such as the analytical hierarchy process (AHP) (Saaty, 2008). N data sets are collected from N cybersecurity experts to compute the resilience metrics. Here data sets represent the response of questionnaires related to the ICS. For our example case as in Figure 12.4, we have used $N = 10$. This type of data collection from security experts is used to provide a scoring formula for cybersecurity metrics (Tran, Campos-Nanez, Fomin, and Wasek, 2016; Wilamowski, Dever, and Stuban, 2017), and we adopt the same methodology to collect the data.

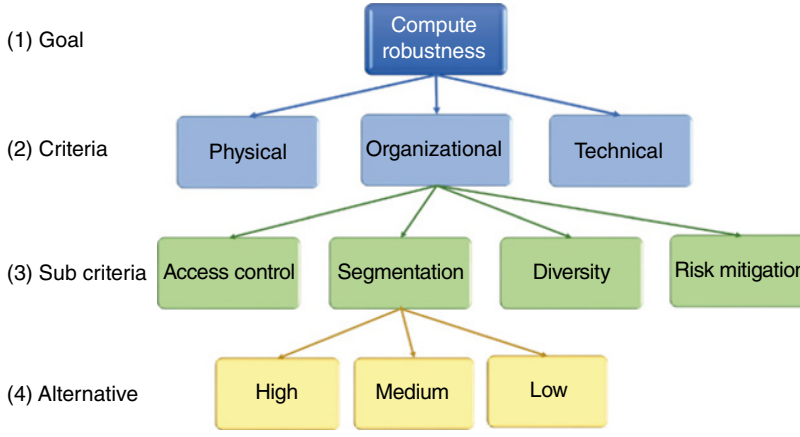

Figure 12.4 Decomposition of robustness using analytical hierarchy process.

The steps involved in implementing the AHP methodology are presented below:

Step 1: Each resilience metric is decomposed into a hierarchy of four levels: *goal* (maximize the corresponding resilience metric), *criteria*, *sub-criteria*, and *alternatives* (possible values that the sub-criteria can take). Figure 12.4 illustrates the hierarchy that we build for the robustness metric as an example. Each criterion at lower-level criteria affects the overall effort of maximizing the robustness. In the same way, each sub-criterion (respective to alternative options) affects its corresponding criterion.

Step 2: Data were collected from N cybersecurity experts (subject matter experts [SMEs]) corresponding to the hierarchy of Figure 12.4, $N = 10$ for our sample illustration. The data collection process was based on a pairwise comparison implementing the qualitative scale explained in Saaty (2008).

Step 3: The pairwise comparisons of all criteria and alternatives constructed in step 2 are organized into a square matrix. Mathematically, the pairwise comparison matrix A for m factors requires $m \times m$ elements. Each entry in A denoted by a_{ij} represents the comparison between factor i and factor j. The pairwise comparison matrix can be determined by using Eq. (12.1):

$$A = \begin{bmatrix} 1 & a_{12} & \cdots & a_{1m} \\ \dfrac{1}{a_{12}} & 1 & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ \dfrac{1}{a_{1m}} & \dfrac{1}{a_{2m}} & \cdots & 1 \end{bmatrix} \tag{12.1}$$

In addition, the individual responses of the N SMEs were aggregated by using the geometric mean, which yielded to one unique comparison matrix:

$$a_{ij} = \left[\prod_{k=1}^{N} \left(a_{ij} \right)_k \right]^{1/N} \tag{12.2}$$

where $(a_{ij})_k$ is the response obtained by the kth cybersecurity expert.

Step 4: When all judgments are made, the relative weight of each criterion with respect to the goal is calculated. These weights are obtained with the normalized right eigenvector of the pairwise comparison matrix A. The relative weights of all the sub-criteria and alternative options are generated using the same process.

Step 5: A consistency ratio (CR) is calculated to measure how accurate or consistent are the judgments of the N expert responses. For the kth cybersecurity

Table 12.2 Values of the random index for small problems ($m < 10$).

m factors	2	3	4	5	6	7	8
RI	0.00	0.58	0.9	1.12	1.24	1.32	1.41

expert response, if $CR_k < 0.1$, then the judgment of this expert can be accepted; otherwise it should be excluded from the analysis for inconsistency. The consistency ratio can be evaluated by comparing the consistency index (CI) with the random index (RI) (Saaty, 2008):

$$CR = \frac{CI}{RI} \tag{12.3}$$

The values of the random index are shown in Table 12.2 for small problems ($m < 10$), and the consistency index *CI* is given by

$$CI = \frac{\lambda_{max} - m}{m - 1} \tag{12.4}$$

In Eq. (12.4), λ_{max} is the maximum eigenvalue of the expert judgment.

Step 6: The resilience metric is calculated by combining the total of the weights of the elements of each level multiplied by the weights of the corresponding lower-level elements.

12.6 Quantitative Modeling of CPS Resilience

CPSs are highly interconnected systems with heterogeneity in different system levels. Thus, any attempt to quantitative resilience modeling and estimation needs to consider the network topology, system vulnerabilities, asset criticality, interconnectivity, and underlying physical processes. It is hard to model and estimate the cyber resilience considering all the areas of security concerns in CPS without impacting system performance and stability. In this section, we discuss in high level the step-by-step modeling and simulation approaches that need to be carried out for the quantitative modeling and estimation of CPS cyber resilience.

12.6.1 Critical Cyber Asset Modeling

Determining asset criticality is one of the fundamental security analysis techniques used by researchers (Haque, Shetty, and Kamdem, 2018; Kellett, 2016).

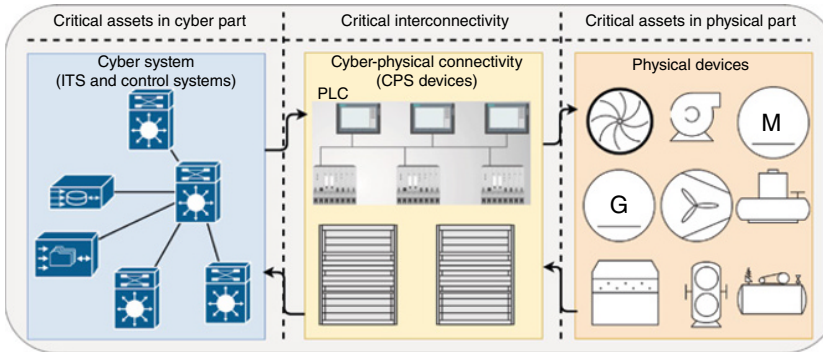

Figure 12.5 Critical assets in different system levels.

Identifying the critical assets provides network administrator a direction to focus on the most critical network components and thus facilitates the best use of resources concerning cost and time. In the CPS, asset criticality comes into play in three different layers: critical assets in the cyber and control part, essential interconnectivity between the cyber and the physical part, and the critical assets in the physical part as shown in Figure 12.5. Critical assets in the cyber domain are those assets that upon exploitation can lead to the exploitation of control devices or cause significant damage to the physical processes. Critical interconnections are those cyber-physical interconnections whose disturbances can result in the unavailability of the services and may cause physical processes to shut down.

While determining the critical asset in the cyber part is not difficult, consideration of all the three parts of criticality and combining them within a single platform undoubtedly need a lot of efforts. As we are concerned about the CPS resilience, we focus mostly on the first two parts, which include the cyber part and the interconnectivity part. We plan to use the graph-theoretical approach considering the network topology and vulnerabilities of the network nodes to assess the asset criticality in a CPS environment. Graph-theoretical approach facilitates to analyze the shortest paths, in other terms most probable attack paths by modeling the cost of the attacker along the paths by using established shortest path algorithms. Also, different multi-criteria decision analysis (MCDA) methods assist in taking the optimum decision in identifying the asset criticality in a complex CPS.

12.6.2 Stepping Stone Attack Modeling

Different CPS components within the IT and OT systems have specific functionalities. Thus, because of the distinct nature and behavior of the systems at different parts such as in the cyber part, interconnectivity part, and physical part as in Figure 12.5, it makes hard for an intruder to exploit a vital asset in the CPS in one

single step. However, today smart intruders are expert enough to launch a multi-host multi-stage cyberattack by utilizing several intermediate stepping stones on the way to the valued ICS or CPS assets. NIST has provided several guidelines (Stouffer et al., 2011) considering the vulnerabilities that arise because of ITS and ICS integration. Modeling the stepping stone attacks is a difficult problem to address because on the one hand the intruder gets more knowledge and expertise by exploiting different hosts in sequence and on the other hand the defender may apply dynamic network configuration based on the detected exploitation scenario. Thus, modeling the stepping stone attack paths is an important aspect in CPS resilience assessment to consider the dynamic nature of the attacker and defender actions. There are several attempts to detect and model the stepping stone attacks in ICS or CPS (Gamarra et al., 2018; Nicol and Mallapura, 2014; Zhang and Paxson, 2000).

Figure 12.6 illustrates an approach to model the stepping stone attack paths using the vulnerability graph where the different network layers are based on the NIST recommended defense-in-depth architecture (Stouffer et al., 2011). The graph model (Haque, 2018) uses different layers to represent different IT and OT layers, where it considers the physical devices such as the power generation systems and the field devices as the potential targets for cyberattacks. The layers corporate demilitarized zone (DMZ) and corporate local area network (LAN) belong to the pure cyber domain or the IT domain. Control system DMZ and control system LAN belong to the interconnectivity layer between the cyber (IT) and physical device layer (ICS/CPS). The network is drawn for application to the EDS where the physical device layer consists of power station networks and other field communication devices. The edge weights in the vulnerability graph model are coming from the exploitability and impact metrics of the Common Vulnerability Scoring System (CVSS) by Mell, Scarfone, and Romanosky (2007). In the probabilistic modeling of such stepping stone attacks in the CPS, game theory and Markov decision process (MDP) are useful to model the attacker and defender actions and to determine the most suitable actions for the defender in different states of the network.

12.6.3 Risk and Resilience Modeling and Estimation

One of the main objectives of CPS resilience assessment is to estimate the risk and resilience of the CPS. In the resilience estimation of CPS and other systems, the resilience graph (Bruneau et al., 2003; Wei and Ji, 2010) is utilized. Figure 12.7 presents a generic resilience graph for the CPS resilience modeling and estimation in the event of a cyberattack incident. The parameter notations are given in Table 12.3. We aim to model the CPS resilience using a combination of the vulnerability graph analysis and the resilience curve estimations and derive the broad R4 resilience

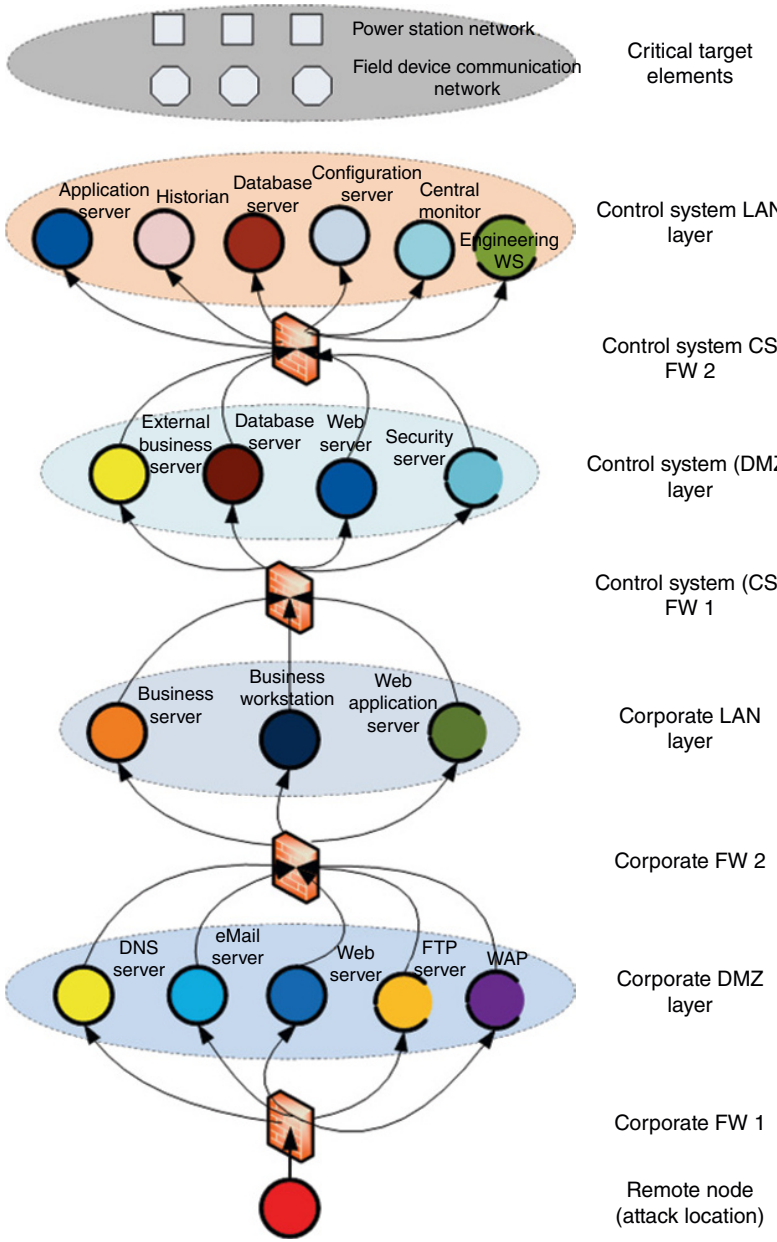

Figure 12.6 Attack graph-based stepping stone modeling. *Source:* From Haque (2018).

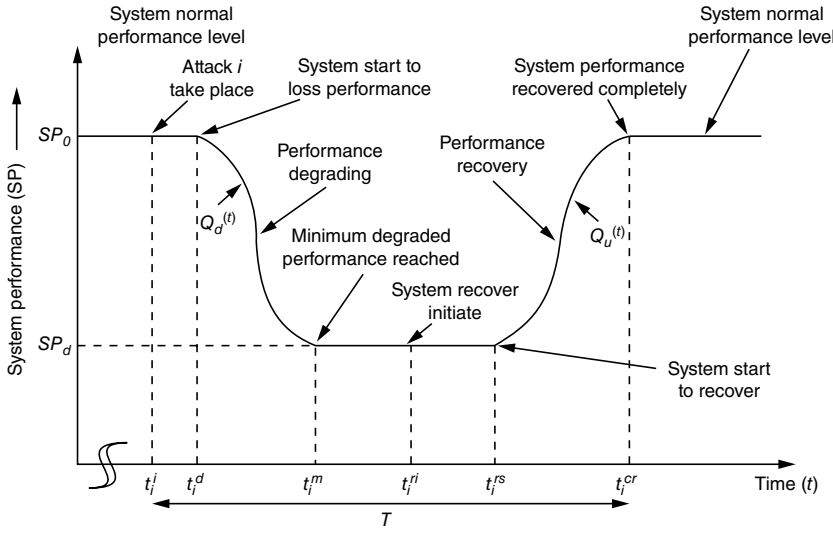

Figure 12.7 System performance graph in the event of cyber incident.

Table 12.3 Notations and parameter description for resilience graph.

Notation	Parameter description
SP_0	System normal performance level before any cyberattack incidence
SP_d	System minimum degraded performance level after a cyberattack incidence
t_i^i	Time when attack incidence i starts taking place
t_i^d	Time when system overall performance starts degrading due to attack incidence i
t_i^m	Time when system reaches to minimum performance level due to attack incidence i
t_i^{ri}	Time when operators identify the attack event and start initiating system recovery
t_i^{rs}	Time when system starts to recover performance after recovery attempt initiation
t_i^{cr}	Time when system completely recover performance and reach to pre-incident performance level
T	Time period of attack initiation to system complete recovery
$Q_d(t)$	Time-dependent system performance degradation behavior
$Q_u(t)$	Time-dependent system performance recovery behavior

metrics as illustrated in Figure 12.3. Here we present a brief discussion on the modeling of resilience and risk using the system performance graph of Figure 12.7.

The system performs at the performance level SP_0 before a cyber incident takes place. This performance is the overall system performance considering the normal stable operation and required services availability. At time t_i^i, a cyberattack event i takes place on the CPS, and the system starts showing degraded performance at time t_i^d. We assume the attack incidence causes damage to part of the systems and the complete system is not taken out of service. Thus, the system continues to perform in reduced performance and reach to the minimum degraded performance SP_d at time t_i^m. Because there are IDS and intrusion prevention mechanisms present in the CPS network, the system administrators and operators can identify the attack incident, analyze it, and initiate recovery at time t_i^{ri}. Because of the recovery initiation, the system performance starts recovering at time t_i^{ts} and performance reach to normal operation level as like pre-attack incidence at time t_i^{cr}. The time between t_i^i and t_i^{cr} is the total period T of resilience due to an attack event i as given in Eq. (12.5):

$$T = t_i^{cr} - t_i^i \tag{12.5}$$

To estimate the resilience, the only challenge is to estimate the nature of time-dependent performance degradation $Q_d(t)$ and time-dependent performance recovery $Q_u(t)$, which are functions of attack severity, the fraction of the system under adverse event, nature and severity of service losses, attack recover capability, etc. In general, the two time-dependent performance parameters are expressed in Eq. (12.6) as follows:

$$\left.\begin{aligned} Q_d(t) &= f\left(attack\ severity, system\ fraction\ under\ attack, service\ loss\right) \\ Q_u(t) &= f\left(attack\ diagnostic, system\ fraction\ out\ of\ service, recover\ ability\right) \end{aligned}\right\} \tag{12.6}$$

Using Figure 12.7, the resilience $\mathfrak{R}$ for the CPS is estimated as follows:

$$\mathfrak{R} = \frac{1}{T * SP_0}\left[SP_0\left(t_i^d - t_i^i\right) + \int_{t_i^d}^{t_i^m}\left\{SP_0 - SP_d - Q_d(t)\right\}dt + \int_{t_i^{rs}}^{t_i^{cr}}\left\{SP_0 - SP_d - Q_u(t)\right\}dt + \int_{t_i^d}^{t_i^{cr}}\left(SP_0 - SP_d\right)dt \right] \tag{12.7}$$

Resilience $\mathfrak{R}$ is normalized by the system normal performance level SP_0. As risk and resilience are treated as having opposite nature in evaluating a system performance during a cyber incident, risk $\mathcal{R}$ is defined as follows:

$$Risk, \mathcal{R} = 1 - \mathfrak{R} \tag{12.8}$$

We consider risk and resilience analysis as complementary to each other. While the computation of resilience is the goal, determining risk cannot be ignored. Both risk and resilience would give a complete posture of the security analysis for the CPS.

12.6.4 Modeling and Design of Attack Scenarios

Most of the cyberattacks that take place in the ITS domain are also applicable in the CPS domain. Figure 12.2 illustrates some of the attacks and threats that are directly applicable to the CPS domain. Often the cyberattack in the CPS is composed of multiple combinations of attack types. One of the challenges in CPS resilience modeling and estimation is to model different attack scenarios and their possible impacts on the CPS to get an estimate of the CPS security and resilience posture.

We present an illustration of the CPS attack scenario in Figure 12.8 using the NIST recommended defense-in-depth architecture by Stouffer et al. (2011) where

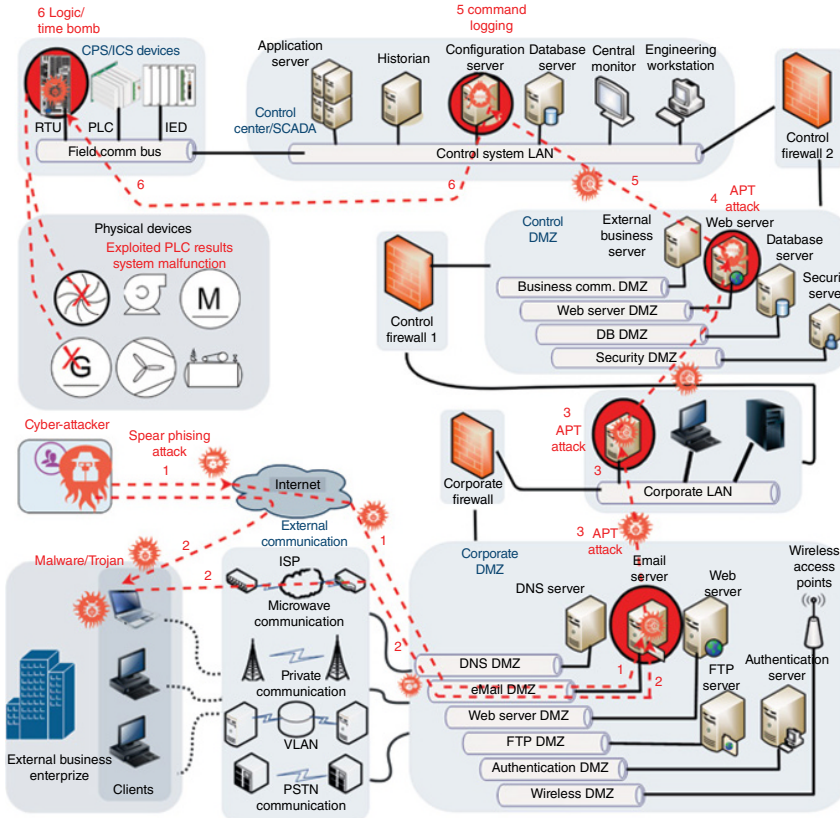

Figure 12.8 CPS attack scenario illustration using NIST defense-in-depth architecture.

we consider the ICS or SCADA systems as the target CPS. In this example, an attacker, having no information whatsoever about the network architecture and intellectual intelligence, uses two different attack mechanisms to penetrate the corporate DMZ network. On the one hand, the attacker installs malware or Trojan in one of the client computers through Internet malicious website browsing (marked as 2 in Figure 12.8), and on the other hand, he tries continuously spear phishing attacks through the Internet communication by sending malicious email attachments to the DMZ users' email accounts (marked as 1).

Using the above mechanisms, the attacker is successful in getting access to one of the email servers in the corporate DMZ, launches APT (marked as 3), and steals system access information and gets important idea about the systems communications. From there he gets successful in penetrating one of the desktop computers attached to the corporate LAN and installs backdoors to bypass the firewalls. Following a similar way, the attacker gets successful in accessing one of the web servers in the control DMZ and start logging the commands and communications (marked as 4).

Using the knowledge gathered from control DMZ, he becomes successful in getting access to the file systems in the configuration servers of the control LAN bypassing the firewalls (marked as 5). Then it is all about a suitable time to set and launch the logic time bomb attack (marked as 6), which may initiate at low traffic hours (generally at late nights when limited operators are available in the control centers to monitor the abnormality). Depending on the nature of the attack, the logic bomb may initiate destructive commands, delete important configuration file, delete backup files so that restoration of the system becomes difficult, and execute other actions depending on the information the attacker is able to gather about the CPS network. The regular lines on the diagram show the network internal connectivity, and the dashed lines on the diagram show the attack propagation.

The above example points to the necessity of modeling and design of the attack scenarios in a simulated environment to be able to make the system resilient from different types of cyberattacks. Again, to model the attacks, the network topology and the vulnerability information are necessary. We plan to use the directed multigraph as illustrated in Figure 12.6 to model and design the attack scenarios. One of the essential requirements to address the designing of attack scenarios is to map the vulnerabilities with the attack types. It is one of the areas we are currently working on.

12.6.5 Modeling Underlying Physical Processes and Design Constraints

CPS is the crucial part of the ICS, SCADA, smart grids, medical devices, and intelligent autonomous vehicles. Because of the diverse applications of the CPS, it is difficult to create a single cyber-resilient model considering the underlying physical processes and design constraints. The goal of this work is not to model the

physical processes or bring any change to the current established physical systems, but to consider up to certain levels the physical processes in the cyber-resilient architecture modeling. The objective is not to contradict the modeling processes with each other, but to make them complement each other. Thus, there is a need for research works in the cyber-resilient modeling of the physical processes. Examples of such can be to incorporate the PLC ladder logic of the ICS or IEEE bus system analysis of the EDS into the cyber-resilient modeling architecture development. Often machine learning (ML) techniques are useful in designing the intrusion detection and prevention systems. ML can also be used in the complex decision-making processes where there does not exist enough data to support the underlying processes due to system confidentiality and regulatory requirements. Qualitative data with decision tree analysis generate convincing results in such cases.

12.7 Simulation Platform for CPS Resilience Metrics

The CPSs are complex. As there is lack of visibility of the underlying interconnections and message communications due to heterogeneous nature of the system, a simulation tool can assist to assess the CPS security and resilience posture to some extent without making any change to the existing system and physical processes. A simulation platform is proposed in this chapter to handle the complex CPS resilience assessment. The simulation tool has two broad approaches: qualitative approach and quantitative approach. Both approaches generate from the resilience framework discussed in Section 12.4, follow some form of mathematical analysis, and produce resilience metrics and analysis from two different angles as presented in Figure 12.9. The details of both simulation tools and their integration process are discussed in the following subsections.

12.7.1 Qualitative Simulation Platform

Figure 12.10 presents a high-level architecture of the simulation engine for the CPS qualitative simulation platform as illustrated by Haque, Shetty, and

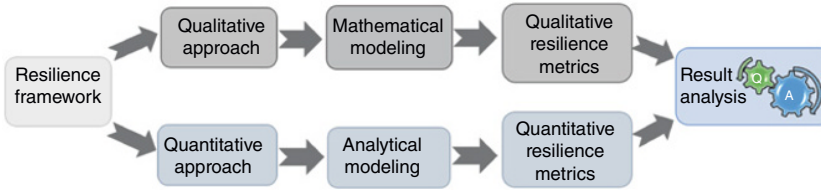

Figure 12.9 Process flowchart of cyber resilience tool for CPS.

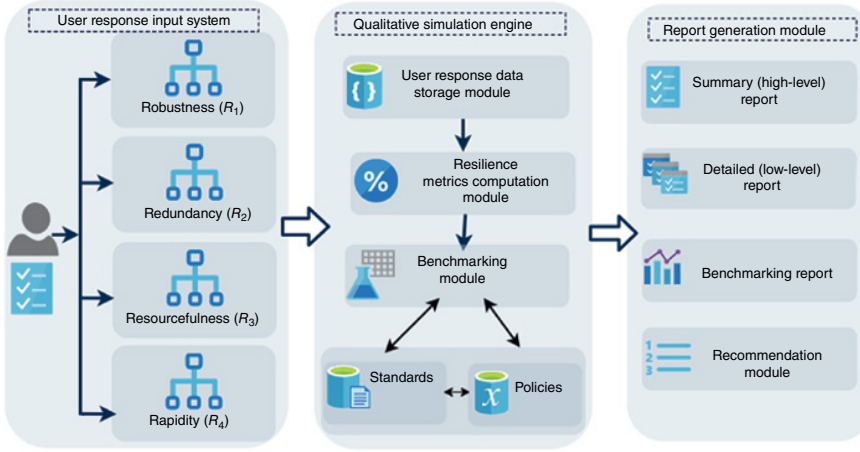

Figure 12.10 Qualitative cyber resilience simulation engine for CPS.

Krishnappa (2019). The user response system is the input systems where the users (CPS operators, engineers, cybersecurity experts, SMEs, etc.) are asked to respond to the questionnaires regarding the systems security posture. As illustrated in the framework in Table 12.1, the questionnaires are spanned across physical, organizational, and technical domain under each of the broad R4 resilience metrics: robustness, redundancy, resourcefulness, and rapidity. There are significant challenges in designing the questionnaires as some of the technical survey questions are application specific.

The responses provided by the users are sent to the qualitative simulation engine. The simulation engine is responsible for analyzing the qualitative responses, generating qualitative resilience metrics, and performing benchmarking with the industry standards and recommended best practices by different regulatory bodies (NIST, ICS-CERT, NERC-CIP, ISA, etc.). Lastly, the report generation module presents the analysis results in the form of a high-level summary report, a detailed low-level report, benchmarking report, etc. The report generation module also provides necessary recommendations to improve the overall resilience posture by comparing the assessment with the industry standards.

12.7.2 Quantitative Simulation Platform

Figure 12.11 presents a generic architecture of the quantitative simulation platform for CPS resilience assessment. The quantitative simulation platform is analogous to the testbed. The quantitative simulation platform is entirely different from the quantitative simulation platform and works independently. There are several management systems and modules to capture the resilience assessment perfectly. A brief description is provided here:

- *Interface management system (IMS):* IMS of the quantitative simulation platform is divided into admin and user interfaces. The admin interface can make changes in the simulation platform (e.g. the creation of new user accounts, modification in the input systems, etc.). The user interface is not allowed to create new users, but it can make changes in the network topology as required. Network topology input is the first step in simulation of the CPS resilience because the simulation engine will produce a graph-theoretic network based on the user inputs of the network components, software, and other applications.
- *Database management system (DMS):* DMS is the local repository of the commonly known vulnerabilities. It downloads the vulnerability information provided by the National Vulnerability Database (NVD) (NIST). The data are stored in a local database designed for the tool where it contains necessary vulnerability information and their CVSS exploitability and impact metrics (Mell et al., 2007). These metrics are used as the weights in the graph-theoretical models in the vulnerability graph module of the quantitative simulation engine.

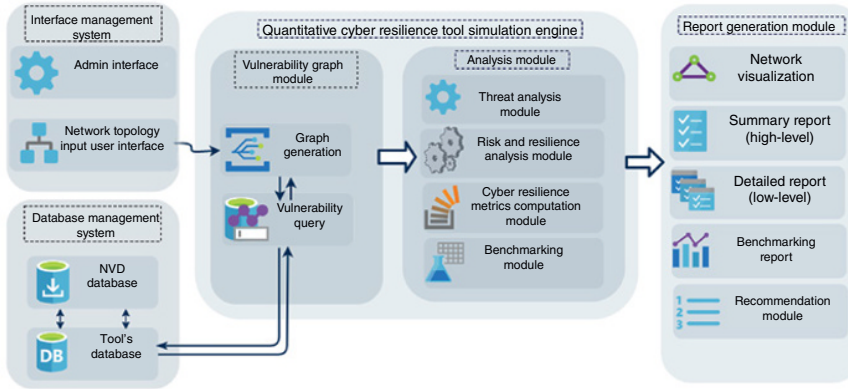

Figure 12.11 Quantitative cyber resilience simulation engine for CPS.

- *Quantitative simulation engine:* There are two major parts in the quantitative simulation engine. One is the vulnerability graph generation module, and the other is the analytical module. The vulnerability graph module takes the network topology input from the user, extracts the corresponding vulnerabilities for the network nodes by communicating with the vulnerability repository in DMS, and generates the graph model for the simulated network like what we present in Figure 12.6. The graph consists of edges where the edges represent the detected vulnerabilities, and the weights are quantitative exploitability and impact scores found from the exploitability and impact scores of confidentiality, integrity, and availability provided by the CVSS. As such, the simulation engine can only handle the known vulnerabilities, and it cannot handle the zero-day vulnerabilities. The analysis module analyzes the threats, computes the risk and resilience metrics, and performs the benchmarking for the resilience assessment of the CPS.
- *Report generation module:* The report generation module provides the network visualization, high-level summary report, a detailed low-level report, benchmarking report, and important recommendations for resilience improvement.

12.7.3 Verification and Validation Plan

The analytical models that are under development will be verified by the simulation platforms. Because of the lack of CPS security and resilience data, it is hard to validate the analytical results. We plan to use different statistical tools to validate our models. One such method is the multivariate analysis technique, which can be used to illustrate the relationships among the broad R4 metrics of resilience.

12.7.4 A Use Case of the Simulation Platform

A use case of the proposed simulation platform for the CPS of the oil and gas sector is presented using Figure 12.12. In this illustration, the physical layer is the bottommost layer where the physical processes occur. There are different sensors to monitor the system and the environment, such as temperature sensor, smoke detectors, fire alarm systems, security surveillance camera, ventilation system, lighting system, etc. The physical layer is transferring sensor data to the control center through the PLC, IED, or RTU in the cyber-physical layer. We consider the I/O processing devices (such as PLC, RTU, IED, etc.) and actuators to be the cyber-physical layer devices because these devices receive physical sensor data from field devices and controls the physical systems through the actuators using the commands initiated from the HMI in the control station. The control layer contains the control servers, master terminal units (MTU), HMI, application servers, data historian, etc. Control layer is responsible for monitoring and controlling

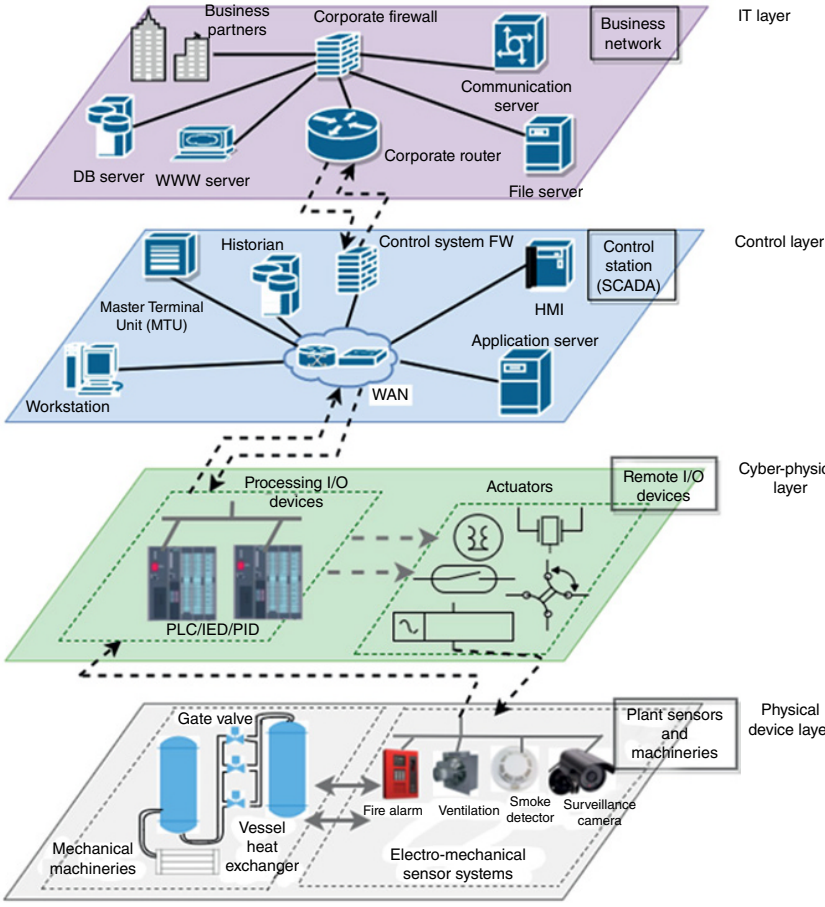

Figure 12.12 A use case example using CPS application in oil and gas industry.

the system performances. The IT layer communicates with the control layer to receive system data to evaluate the performance of the physical devices. We illustrate here the use case using both qualitative and quantitative approaches of the simulation platform.

Use Case of Qualitative Simulation Platform: The qualitative simulation platform is designed with a set of system-specific questionnaires to serve the security and resilience assessment for the use case. In the qualitative tool, the users are expected to provide the answers to the systems security-related questions.

The tool then aggregates the results and provides quantitative metrics that would not only help the executives but also help the system operators to analyze

the security and resilience of the system using their assessment. Here we provide some of the usages of the proposed qualitative tool:

- *In-depth insights from resilience sub-metrics:* Figure 12.13 shows a sample simulation output generated from the proposed qualitative tool for the sub-metrics of robustness and resourcefulness. The tool produces the metrics directly from

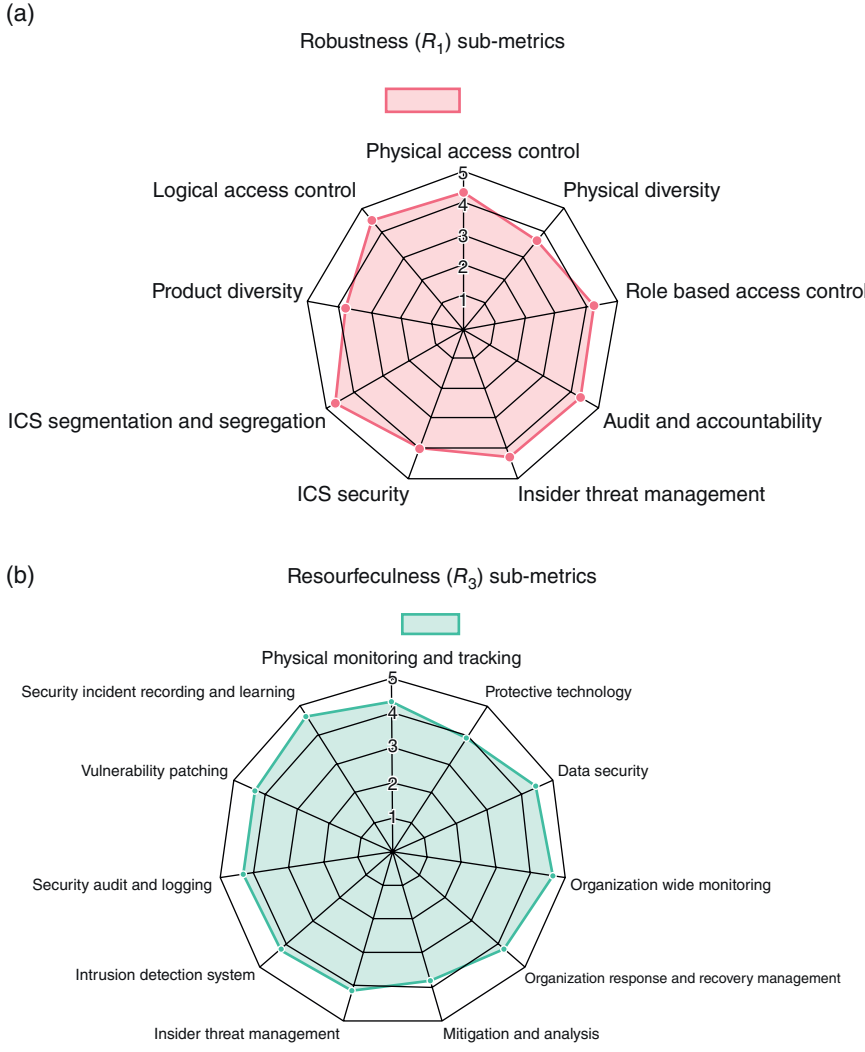

Figure 12.13 Sample qualitative metrics of (a) robustness and (b) resourcefulness generated from the qualitative tool.

the users' qualitative responses. In both the robustness and resourcefulness metrics, we see that most of the resilience areas are working fine with values ≥4.0 on a scale of 1.0–5.0, which means ≥75% of resilient performances in those areas.

- *Overall insights on cyber resilience:* The qualitative tool computes the cyber resilience metrics R and its major components R_1, R_2, R_3, R_4. It also provides physical, technical, and organizational metrics under each of the R4 resilience metrics. Thus, it could give a satisfactory overall insight on the cyber resilience of the CPS based on the users' assessment.

Use Case of Quantitative Simulation Platform: In the quantitative simulation platform, the users need to set up the network topology up to the cyber-physical layer starting with the IT layer. In each of the layers, the user needs to provide the host, software, or applications running on the host, patch information, and the physical or logical connectivity. The tool then generates the vulnerability multigraph using the information provided by the user where the vulnerability information is extracted using the DMS of the tool as illustrated in Figure 12.11. The tool performs the analysis in the simulation engine and is expected to provide (but not limited to) the following information:

- *Network vulnerability visualization:* The tool provides a complete visualization of the system with the connectivity and vulnerability information, which would assist the operators to analyze the security of the system.
- *Cyber critical paths:* The tool would identify the critical assets in the network and provide the cyber critical paths with scores or probability of the attack using the underlying modeling and simulation techniques.
- *Risk and resilience metrics:* The tool would provide the cyber risk and resilience metrics in both high level and low level to facilitate further analysis by the network operators and security experts.
- *Benchmarking and recommendations:* The quantitative tool is designed to perform benchmarking with the industry and regulatory standards provided by the authorized bodies and provide meaningful recommendations for improving overall CPS network security and resilience posture.

12.8 Complexities, Challenges, and Future Directions

CPS is an active research field with numerous complexities and challenges from the cybersecurity perspective. The complications come from the complex nature of the system design, components heterogeneity, complex interconnections, lack of overall visibility, the trade-off between security and reliability of physical

processes, etc. This section discusses some of the selected complexities and challenges of CPS security and future directions:

- *Security by design:* CPSs (e.g. ICS) are legacy systems where security is not considered as a design consideration because of the isolated command and control mechanisms and isolation from direct Internet communication. Physical security is thought to be enough for safeguarding the physical devices and underlying connections. Considering the widespread use of CPS and the growing need for different layers of interconnectivity, it is now the high time to include the security of the devices as an essential concern in the design processes.
- *Real-timeliness nature:* CPSs are real-time systems. The operational requirement of real-time availability makes CPS hard to assess a security threat and implement a preventive mechanism in real time within the tolerable delay limit. As pointed out by Humayed et al. (2017), cryptographic mechanisms could cause delays in the operations of real-time devices. Thus, the design of the CPS should consider inclusion of security mechanisms that recognize the real-timeliness nature and security processes without significant delay.
- *Heterogeneity and interconnectivity:* CPSs are heterogeneous in nature having complex interconnections of the cyber and physical layer devices. The proprietary protocols (e.g. Modbus and DNP3 in ICS or smart grids) are not free of vulnerabilities due to the isolation consideration during the design of the protocols. Thus, the communication due to the interconnections of the devices and protocol-level security need to be taken into account in the design process. The authors (Fovino, Carcano, Masera, and Trombetta, 2009; Majdalawieh, Parisi-Presicce, and Wijesekera, 2007) focus on this in details.
- *Underlying physical processes:* CPSs are designed to operate closely with the embedded physical processes. The complex underlying processes reduce the visibility of the overall security of the CPS, and thus, the underlying processes and dependencies should be considered in the resilient network topology design process.
- *IDS and IPS:* There are some fundamental differences of the IDS and IPS design between the ITS and the CPS. In ITS, the security is ensured by software patching and frequent updating, which is not suitable for the CPS because of limited memory resources. Another concern in the IDS and IPS design for the CPS is that CPSs are real time, and thus, patching of those devices that needs to take them offline by suspending operations is difficult to justify economically and operationally. Therefore, design of IDS and IPS solutions specific to the CPS and design of novel attack-detection algorithms are the need of the time. The article by Mitchell and Chen (2014) focuses on the development of the IDS solutions applicable to the CPS.

- *Secure integration:* The integration of new components with the existing CPS should perform security testing before putting online. There is a need for vulnerability assessment of the components to be added to the existing systems.
- *Understanding the consequences of an attack:* Often it is difficult to visualize the consequences of an attack in the ICS or CPS. It is essential to perform penetration tests and assess the impacts of a cyberattack on the CPS. Also, the prediction of the attacker strategy is crucial in defending the CPS network. The organizational and technical security policy should consider performing penetration tests up to certain security levels.
- *Malicious insider:* It is one of the most difficult challenges in securing the CPS against cyberattacks. Often disgruntled employees can be an attack vector for the targeted attacks on the CPS, which are hard to identify. There is also social engineering, which may have temptation effect on an employee with ICS credentialed access. Often unintentional attacks are also possible such as the use of USB sticks. Thus, organizations should have clearly defined policies and conduct security training for the employees to be aware of the situation and responsibilities.
- *Resilience, robustness, security, and reliability:* Resilience, robustness, and security are critical challenges from the cybersecurity perspective for the CPS devices. Often CPSs are designed to be reliable as the stability of operation is considered most important during the design process. Although the reliability is utmost necessary for the physical devices, security and resilience cannot be ignored. The uncertainty in the environment, cyberattacks, and errors in physical devices threaten the overall CPS security and reliability. Therefore, the resilience and security of the devices need to be considered equally important as reliability during the design phase.

The big question that comes naturally is how the proposed simulation platform to assess the resilience metrics for the CPS would handle the above challenges. As we have explained in Section 12.3, the availability of the resilience metrics would provide guidelines and directions in the different stages of CPS operations (e.g. design process, monitoring, recovery, etc.) and ensures the overall security by pointing to the improvement areas with essential recommendations. The qualitative and quantitative methods of resilience assessment are complementary to each other, and they are designed to handle the security challenges in the CPS by providing quantitative operational metrics of cyber resilience for the CPS. Including the physical processes and cyber-physical interconnectivity in the simulation platform would be a big challenge because of system connectivity changes based on the application area. Thus, the authors would like to include partial if not complete physical and cyber-physical components into the simulation platform. It is also possible to add multiple simulation modules where each module would serve specific CPS

application area (such as one module for the smart grid, another module for oil and gas, etc.). Modeling and simulation of the complete CPS regardless of the application area would be a mammoth task and could be saved for future works.

12.9 Conclusion

CPSs play a vital role in critical infrastructures, ICSs, and many other applications. The growing interdependencies and interconnections among different parts of CPS make it vulnerable to cyber threats than any time before. The complex nature of CPS in conjunction with the lack of clear visibility due to the integration of different cyber, cyber-physical, and physical components make it difficult to handle the security concerns and resilience challenges. The chapter aims to present essential cyber resilience metrics for the CPS and proposes a simulation platform to help in the automation of the resilience computation process. Among the other discussions, the authors try to explain the need for the resilience metrics in the CPS and the way the proposed resilience metrics can help in identifying technical areas for improvement and generate recommendations. The authors discuss the complexities and challenges to secure the CPS from cyberattacks and answer the big question of how the resilience metrics can assist in handling those challenges. Overall, the authors believe that the chapter provides the necessary guidance in the ongoing CPS resilience and security analysis and would also provide directions for future research.

Acknowledgment

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780.

Disclaimer

This report was prepared as an account of work sponsored by an agency of the U.S. government. Neither the U.S. government nor any agency thereof nor any of their employees makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation,

or favoring by the U.S. government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S. government or any agency thereof.

References

Amin, M. (2015). Smart grid. *Public Utilities Fortnightly*, March 2015.

Baheti, R., & Gill, H. (2011). Cyber-physical systems. *The Impact of Control Technology*, *12*(1), 161–166.

Bodeau, D., & Graubart, R. (2011). Cyber resiliency engineering framework. *MTR110237, MITRE Corporation*.

Bologna, S., Fasani, A., & Martellini, M. (2013). Cyber security and resilience of industrial control systems and critical infrastructures. In *Cyber Security* (pp. 57–72). Springer.

Bruneau, M., Chang, S. E., Eguchi, R. T., Lee, G. C., O'Rourke, T. D., Reinhorn, A. M., ... Von Winterfeldt, D. (2003). A framework to quantitatively assess and enhance the seismic resilience of communities. *Earthquake Spectra*, *19*(4), 733–752.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009). *Challenges for securing cyber physical systems*. Paper presented at the Workshop on Future Directions in Cyber-Physical Systems Security.

Cheng, A. M. (2008). *Cyber-physical medical and medication systems*. Paper presented at the 28th International Conference on Distributed Computing Systems Workshops (ICDCS).

Collier, Z. A., Panwar, M., Ganin, A. A., Kott, A., & Linkov, I. (2016). Security metrics in industrial control systems. In *Cyber-Security of SCADA and Other Industrial Control Systems* (pp. 167–185). Cham: Springer.

Cutter, S. L., Ahearn, J. A., Amadei, B., Crawford, P., Eide, E. A., Galloway, G. E., et al. (2013). Disaster resilience: A national imperative. *Environment: Science and Policy for Sustainable Development*, *55*(2), 25–29.

Fovino, I. N., Carcano, A., Masera, M., & Trombetta, A. (2009). Design and implementation of a secure modbus protocol. In *International Conference on Critical Infrastructure Protection* (pp. 83–96). Berlin, Heidelberg: Springer.

Galloway, B., & Hancke, G. P. (2013). Introduction to industrial control networks. *IEEE Communications Surveys and Tutorials*, *15*(2), 860–880.

Gamarra, M., Shetty, S., Nicol, D. M., Gonazlez, O., Kamhoua, C. A., & Njilla, L. (2018). *Analysis of stepping stone attacks in dynamic vulnerability graphs*. Paper presented at the 2018 IEEE International Conference on Communications (ICC).

Ginter, A. (2017). The top 20 cyber attacks on industrial control systems. *Waterfall Security Solutions*.

Haque, M. A. (2018). *Analysis of bulk power system resilience using vulnerability graph* (Master of Science (MS) thesis). Modeling Simulation and Visualization Engineering, Old Dominion University. doi:https://doi.org/10.25777/fqw2-xv37.

Haque, M. A., De Teyou, G. K., Shetty, S., & Krishnappa, B. (2018). *Cyber resilience framework for industrial control systems: Concepts, metrics, and insights*. Paper presented at the 2018 IEEE International Conference on Intelligence and Security Informatics (ISI).

Haque, M. A., Shetty, S., & Kamdem, G. (2018). Improving bulk power system resilience by ranking critical nodes in the vulnerability graph. In *Proceedings of the Annual Simulation Symposium* (pp. 8). Society for Computer Simulation International.

Haque, M. A., Shetty, S., & Krishnappa, B. (2019). *ICS-CRAT: A cyber resilience assessment tool for industrial control systems*. Paper presented at the 4th IEEE International Conference on Intelligent Data and Security (IDS).

Humayed, A., Lin, J., Li, F., & Luo, B. (2017). Cyber-physical systems security: A survey. *IEEE Internet of Things Journal*, *4*(6), 1802–1831.

Kellett, M. (2016). Ranking assets based on criticality and adversarial interest. *Defence Research and Development Canada*.

Koutsoukos, X., Karsai, G., Laszka, A., Neema, H., Potteiger, B., Volgyesi, P., ... Sztipanovits, J. (2017). SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber-physical systems. *Proceedings of the IEEE*, *106*(1), 93–112.

Laing, C. (Ed.) (2012). *Securing Critical Infrastructures and Critical Control Systems: Approaches for Threat Protection*. USA: IGI Global.

Linkov, I., Eisenberg, D. A., Bates, M. E., Chang, D., Convertino, M., Allen, J. H., ... Seager, T. P. (2013). *Measurable Resilience for Actionable Policy* (pp. 10108–10110). USA: ACS Publications.

Linkov, I., Eisenberg, D. A., Plourde, K., Seager, T. P., Allen, J., & Kott, A. (2013). Resilience metrics for cyber systems. *Environment Systems and Decisions*, *33*(4), 471–476.

Macaulay, T., & Singer, B. L. (2016). *Cybersecurity for Industrial Control Systems: SCADA, DCS, PLC, HMI, and SIS*. UK: Auerbach Publications.

Majdalawieh, M., Parisi-Presicce, F., & Wijesekera, D. (2007). DNPSec: Distributed network protocol version 3 (DNP3) security framework. In *Advances in Computer, Information, and Systems Sciences, and Engineering* (pp. 227–234). Springer.

McIntyre, A., Becker, B., & Halbgewachs, R. (2007). Security metrics for process control systems. *Sandia National Laboratories* (Sandia Report SAND2007-2070P).

McMillin, B., Gill, C., Crow, M., Liu, F., Niehaus, D., Potthast, A., & Tauritz, D. (2007). Cyber-physical systems distributed control: The advanced electric power grid. *Proceedings of Electrical Energy Storage Applications and Technologies*.

Mell, P., Scarfone, K., & Romanosky, S. (2007). *A complete guide to the common vulnerability scoring system version 2.0*. Paper presented at the Published by FIRST-Forum of Incident Response and Security Teams.

Mitchell, R., & Chen, I. R. (2014). A survey of intrusion detection techniques for cyber-physical systems. *ACM Computing Surveys (CSUR)*, *46*(4), 55.

Nicol, D. M., & Mallapura, V. (2014). *Modeling and analysis of stepping stone attacks*. Paper presented at the Proceedings of the 2014 Winter Simulation Conference.

Saaty, T. L. (2008). Relative measurement and its generalization in decision making why pairwise comparisons are central in mathematics for the measurement of intangible factors the analytic hierarchy/network process. *RACSAM-Revista de la Real Academia de Ciencias Exactas. Fisicas y Naturales. Serie A. Matematicas*, *102*(2), 251–318.

Sedgewick, A. (2014). *Framework for improving critical infrastructure cybersecurity, version 1.0*. NIST-Cybersecurity Framework.

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to industrial control systems (ICS) security. *NIST Special Publication*, *800*(82), 16–16.

Tierney, K., & Bruneau, M. (2007). Conceptualizing and measuring resilience: A key to disaster loss reduction. *TR News* (250).

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. (2016). Cyber resilience recovery model to combat zero-day malware attacks. *Computers and Security*, *61*, 19–31.

Wang, F. Y. (2010). The emergence of intelligent enterprises: From CPS to CPSS. *IEEE Intelligent Systems*, *25*(4), 85–88.

Wei, D., & Ji, K. (2010). *Resilient industrial control system (RICS): Concepts, formulation, metrics, and insights*. Paper presented at the 3rd International Symposium on Resilient Control Systems (ISRCS), 2010.

Wilamowski, G. C., Dever, J. R., & Stuban, S. M. (2017). Using analytical hierarchy and analytical network processes to create Cyber Security Metrics. *Defense Acquisition Research Journal: A Publication of the Defense Acquisition University*, *24*(2), 186–221.

Xiong, G., Zhu, F., Liu, X., Dong, X., Huang, W., Chen, S., & Zhao, K. (2015). Cyber-physical-social system in intelligent transportation. *IEEE/CAA Journal of Automatica Sinica*, *2*(3), 320–333.

Yong, S. Z., Foo, M. Q., & Frazzoli, E. (2016). *Robust and resilient estimation for cyber-physical systems under adversarial attacks*. Paper presented at the American Control Conference (ACC), 2016.

Yu, X., & Xue, Y. (2016). Smart grids: A cyber-physical systems perspective. *Proceedings of the IEEE*, *104*(5), 1058–1070.

Zhang, Y., & Paxson, V. (2000). *Detecting stepping stones*. Paper presented at the USENIX Security Symposium.