# 1

# Introduction

In this chapter, descriptions of traditional physical and cyber systems are provided to identify existing challenges. Current research trends of cyber-physical systems (CPSs) are then illustrated to address these challenges. The major applications of the proposed methods in CPSs are reviewed.

## 1.1 Challenges of Traditional Physical and Cyber Systems

Over the past three decades, studies have addressed numerous concerns regarding the capability of traditional static modeling methodologies, such as the fault tree method and the event tree method, to adequately and quantitatively analyze the impact of hardware and software interaction on the stochastic behavior of CPSs [1, 2]. During the past decade, the dynamical Markov reliability model was proposed to solve similar problems in CPSs [3]. Control block diagrams were presented for cooling loop systems. The reliability block diagram (RBD) was then established and used to describe the overall reliability status of individual components in a simplified form [4, 5]. However, RBDs are incapable of describing the dynamic maintenance and repairable activities; thus, various dynamic modeling methods have been reviewed in [6, 7]. The Markov methodology has the advantage of tracking the dynamic changes and time-dependent features of CPSs, and simply integrates all failure states that occur after each working state into one failure state. The Markov methodology eliminates most of the failure states into a system failure state (absorbing node) by conducting a necessary fault injection test and achieving a sparse transfer matrix but may still result in a very large model due to many existing surviving states. Its modeling precision largely depends on the number of fault injection tests, and more cycles yield higher accuracy. To avoid the disadvantages of these two methodologies, some studies have proposed hybrid reliability models combining RBDs and Markov models for CPSs [8].

The control block diagram introduces blocks to represent each part of the control system, including the controllers, actuators, and control objectives. Control block diagrams are widely used in modern control systems because they can visually describe the relations among the important components, data flow, and control sign flow. In addition, compared with other mathematical models, they have the advantage of simply reflecting the actual correlations in a CPS. It is reasonable to build a reliability model based on the control block diagram of a CPS. In the model, the controller has many input signals, including commands

*Cyber-Physical Distributed Systems: Modeling, Reliability Analysis and Applications,* First Edition.
Huadong Mo, Giovanni Sansavini and Min Xie.

and system state feedback. In general, commands are the system's expected outputs. Control signal flows are given in the control block diagram, and sensors play an important role in this feedback system. This control block diagram clearly indicates the internal dynamic relations of the system, covering most of the aspects that need to be studied.

For applications in CPSs, we are interested in real-time performance. Therefore, from a control perspective, the ability to adjust the transient and steady-state response of a feedback CPS is a beneficial outcome of the design of the CPS. One of the first steps in the design process is to specify the performance measures. In this chapter, we introduce common time-domain specifications, such as percent overshoot, settling time, time to peak, time to rise, and steady-state tracking error. We will use selected input signals, such as the step and ramp, to test the response of the CPS. The correlations between the system performance and the stability, reliability, and resilience strategies of CPSs are investigated. We will develop valuable relationships between the performance specifications and the component states for CPSs.

The ability of a feedback CPS to compensate for the consequences of the inherent faults redefines the concept of failures, i.e., the reliability of the CPS is dependent not only on the type of failure that may occur, but also on the evolving states of system output and control signals in each period [9, 10]. Classical reliability evaluation methods, such as fault tree analysis, event tree analysis, and failure mode and effect analysis, are not appropriate for application to these evolving states due to the level of complexity and dynamics of CPSs. In [11, 12], structured analyses and design techniques based on Monte Carlo simulation (MCS) for reliability evaluation are presented. This approach explicitly formalizes the functional interactions between subsystems, identifies the characteristic values affecting the reliability of complex CPSs, and quantifies the reliability, availability, maintainability, and safety (RAMS) parameters related to the operational architecture. As the remaining ability of the system to maintain the expected control goal after faults occur is crucial, ordered sequences of multi-failure methods have been applied to assess the reliability of all possible CPS architectures [10]. A new methodology called a multi-fault tree is proposed, and time-ordered sequences of failures are addressed.

In contrast to the aforementioned studies, the reliability of a CPS as a function of the required performance from a control viewpoint is evaluated in [13]. The CPS is regarded as a failure if the dynamic performance does not satisfy all the requirements. Difference equations are introduced to describe the stochastic model of the CPS, explicitly illustrating the influence of the transmission delays and packet dropouts on changing the model parameters. A linear discrete-time dynamic approach for modeling the signal flow in, out, and among all subsystems promotes straightforward calculation of fundamental dynamic aspects, such as times and fault characteristics [14].

MCS has been shown to be a straightforward yet accurate approach for the study of such complex systems [11–13, 15]. The general approach in MCS for reliability assessment is to generate operational requirements that lead to the failure of the entire system. However, this approach requires knowledge of the system requirements-to-failure distribution in advance. In [16], an event-based MCS method was proposed for multi-component systems, in which the failure time for each component is generated and then used to verify the success or failure of the system subject to the required operational time. Because no attempt is made to generate the failure time for the entire system, which requires

knowledge of the time-to-failure distribution of the entire system as well as the distribution approximation at the component level, it is quite different from previous methods and can reduce the possible error and computational effort in estimating the system reliability.

In [13], this method was extended to estimate the reliability of CPSs and replaces the constraint on the number of replications used in [16] with two other constraints, namely, a precision interval and a percentage of simulations belonging to this interval. The networked degradations for each channel are generated and are then used to determine the success or failure of the CPS for a given combination of operational requirements. Therefore, the reliability of the CPS is estimated as a tabulated function of the operational requirements. Compared with the results in [16], the results obtained in [13] guarantee the estimated reliability to satisfy a given precision.

## 1.2 Research Trends of CPSs

### 1.2.1 Stability of CPSs

In power systems, communication delays always occur in the transmission of frequency measurements from sensors to the control center (S-C channel), and control signals from the control center to the plant side (C-A channel) [17, 18]. In local networks, time delays are usually ignored because the control is mainly applied locally, and communication delays are negligible compared with the subsystem time constants [19]. In recent years, with the rapid development of wide-area measurement systems (WAMSs), a large number of phasor measurement units (PMUs) have been deployed to facilitate the real-time control of wide-area power systems (WAPSs) to improve the load frequency control (LFC) performance [20–22]. However, when data packets are transmitted across a WAMS, communication delays may become significant and cannot be ignored [23–25].

The conventional control of WAPSs is centralized and employs dedicated communication channels over a closed communication network. However, new regulatory guidelines require coordination across multiple hierarchical levels of power systems for more effective market operations and, as a result, open communication infrastructures have been deployed to promote the control of these increasingly complex systems [26, 27]. While open networks have economic, maintenance, and reliability advantages, they are subject to time delays that are inherently stochastic (e.g., multiple delays [20] and probabilistic interval delays [24]), and thus cannot be calculated based on the procedures for dedicated networks. Numerical investigations show that time delays the open communication network have the potential to destabilize a WAPS [23, 28, 29]. For instance, the deregulation of the power industry has pushed many tie lines between control areas to operate close to their maximum capacity. This is especially true for tie lines serving heavy load centers, for example, in southern California [28]. Under these circumstances, operational stresses, such as large time delays, increase the possibility of inter-area oscillation, reducing the effectiveness of control system damping, and potentially leading to loss of system synchronism [30].

Recent studies on the LFC of WAPSs with communication delays have mainly focused on: 1) the influence of time delays on the WAPS and effective approaches for delay compensation [31, 32]; 2) control methods for providing robust performance against delays

(e.g., event-triggered control methods [33], wide-area phasor power oscillation damping controllers [34], and robust controllers [29, 35]); 3) exact methods for evaluating the delay margin for stability, that is, the maximal allowable delay (upper bound on the time delays), when WAPSs and open networks are integrated [17, 20, 36]. A WAPS is unstable if the real-time delays exceed the delay margin.

Two classes of methods are available for computing the delay margin in a WAPS for constant and time-varying delays. Frequency-domain direct methods quantify the delay margin based on computing critical eigenvalues for constant delays with a known upper bound, for example, the Schur-Cohn-based method for commensurate delays [37], Rekasius substitution [38], and the elimination of exponential terms in the characteristic equation [36]. Indirect methods can deal with time-varying and constant delays; they are derived from Lyapunov stability theory [17, 23, 24], linear matrix inequality techniques [27, 28, 39], H-infinity robust synthesis [20], and the dual-locus diagram method [40].

These methods assume well-defined time delay models, that is, constant [20], uniformly distributed [25], multiple [17], and probabilistic interval time delays [24], and require prior knowledge of the lower bound, upper bound, and parameters of the delay distribution. However, delays in an open communication network vary with the number of active end-users [41] and media access control (MAC) protocols [42]; therefore, no prior knowledge of time delays is available, and they are intrinsically stochastic. These assumptions hinder the application to real systems and lead to excessively conservative results. To overcome these limitations, the LFC model of WAPSs should account for a real open communication network with various MAC-level protocols. The TrueTime simulator has been used to extract realistic scenarios of networked control systems (NCSs), in which the characteristics of the random delays are unknown and are statistically inferred after collecting sufficient delay observations [43–45]. As a specific application of NCSs, insights obtained from the integration of traditional control systems and open communication networks can foster the integration of open communication networks and WAPSs. However, to the best of the author's knowledge, few studies have analyzed the stabilization of WAPSs via real open communication networks.

During the computation of the control signals, the prediction of the C-A delay in the current period and the S-C time delay in the successive period can greatly improve the controller performance. However, this possibility has not been investigated in previous works on delay margins or robust LFC strategies. Several methods for delay estimation are available, such as the Markovian model approach [46], backpropagation neural network prediction [47], adaptive wide-area power oscillation damping [48], dynamic Markov jump filters [49], hidden Markov models (HMMs) [50, 51], and the exponentially weighted moving average (EWMA) method [52]. Time delays depend on the underlying network state, which is ever-changing and concealed [53, 54]. Indeed, network states cannot be observed directly, but random time delays can be measured using the time-stamp technique [55]. Therefore, the state variables of the open communication network can be estimated using the measured time delays; the transitions among these states can be modeled by a discrete HMM (DHMM). As a result, random delays are observations of the DHMM [56–58].

Traditionally, in HMM-based delay models, random delays are mapped to a discrete observation space through scalar quantization techniques, for example, uniform quantization and *k*-means clustering quantization [57–60]. Because the evolution of random

delays is described by a finite-state Markov chain, the communication network action can be learned via the DHMM [47, 57, 59]. In addition, DHMMs have been used for other applications in power systems, for example, the dynamic detection of transmission line outages [61], the generation of distributed photovoltaic systems [62], and residential energy use [63–65]. Chapter 3 introduces the missing data expectation maximization (MDEM)-based Baum-Welch algorithm [56, 59, 66] for the estimate of the parameters of the DHMM online, without previous knowledge of the state transition matrix. Following this step, the time delay can be predicted using the Viterbi algorithm [67]. The predictions are used as the inputs of the Smith predictor to compensate for time delays and improve the LFC strategy performance [68, 69]. Our work improves the conventional Smith predictor, which simply employs the summation of the latest measured C-A time delay and the S-C time delay to construct the prediction [41]. The conventional Smith predictor cannot capture the evolution of the network states, which is the root cause of stochastic time delays.

The relationship between the delay margin and the controller gains can only help achieve a compromise between the LFC performance and the maximum allowable delay. However, the delay margin-based method cannot compensate for random delays because it does not involve the real-time prediction of delays in each period. Therefore, in Chapter 3, the Smith predictor estimates the real-time delay, which is then integrated into the delay margin-based method to enhance the frequency stabilization performance. The Smith predictor can also enhance the LFC performance of robust proportional-integral-derivative (PID) controllers, whose gains are tuned via robust evolutionary algorithms [35]. Improvements to control strategies currently implemented in real systems, e.g., delay margin-based proportional-integral (PI) controllers [17, 24] and PID controllers [35], are presented to demonstrate the effectiveness of the proposed methodology for the control of WAPSs.

The power sector is experiencing a structural trend toward decentralization, stemming from the integration of large shares of renewable energy resources (RERs) [70]. This is fostered by distributed energy resources (DERs), which require the integration of power generation means located at or near the end-user side [71, 72]. However, the stochastic nature of RERs and the load demand induces system frequency fluctuations [73, 74]. An effective control strategy is needed to maintain the system frequency at its nominal value by balancing the power generation and demand in real time. To this end, automatic generation control (AGC) schemes have been developed for damping frequency oscillations in distributed generation systems (DGSs) [74–77]. AGC is performed by computing control signals based on the system frequency and delivering balancing inputs to various energy storage systems (ESSs) to absorb (release) the surplus (deficit) power from (to) the grid [77–79]. However, the ubiquity of DERs across wide areas and the complex structure of DGSs hinder the development of dedicated communication infrastructures for DGSs with massive DERs [80–83].

Recently, AGC has been integrated with open communication networks because of its low cost, high speed, simple structure, and flexible access. Data exchanges among PMUs, generators, and the control center are provided by the open communication network in the form of time-stamped data packets [42, 76, 82, 83]. Stable AGC depends heavily on the performance of the open communication network [42, 76–78, 84–88]. Cognitive

radio networks, cellular networks, local area networks (LANs), wide area networks (WANs), and wireless local area networks (WLANs) are employed as open communication infrastructures in these NCSs [79, 80, 83].

However, open communication networks are exposed to various types of degradation processes, such as network-induced time delays [77, 78, 86, 87], packet dropouts [88, 89], failures of the communication infrastructure [90], uncertain communication links [91], and cyberattacks [92]. As a result, the measurement signals (control signals) received by the control center (ESS or generators) degrade, effective AGC cannot be carried out, and the system frequency response worsens [78–82]. Studying the performance of open communication networks is critical for understanding the occurrence of time delays and packet dropouts. To this end, medium access and packet transmission must be analyzed. The MAC layer is the lower layer of the data link layer of the Open System Interconnection model, and it is responsible for moving data packets among network interface cards across communication channels. Several MAC protocols, for example, carrier-sense multiple access with collision detection (CSMA/CD, Ethernet), CSMA with arbitration on message priority (controller area network), and IEEE 802.11b/g (WLAN), prevent the collision of packets sent from different nodes across the same channel [83, 93–95].

Time delays are variable, challenging to predict, deteriorate AGC performance, and reduce the stability region [78, 79]. Packet dropouts refer to lost messages, which occupy network bandwidth but cannot reach the destination. They affect the operations of DERs and the reduction of frequency fluctuations, particularly in uncertain network environments. Optimal feedback AGC regulators for DERs have been investigated in numerous works for perfect communication networks, and the impact of transmission delays and packet dropouts on the controller cannot be captured [96]. Robust PID controllers against constant or uniformly distributed time delays [77–80] are designed to cope with perturbations of the control parameters. However, constant or uniformly distributed time delays cannot be generally assumed in realistic communication networks.

In addition, recent studies focusing on primary and secondary control levels have been extended to the power management level by considering fuzzy controllers [97, 98], decentralized power management and sliding mode control strategies [99], static synchronous compensators [100], and two-degrees-of-freedom feedback-feedforward robust controllers [101, 102]. The reactive power reference can be determined and controlled by a novel application of radial basis function neural networks [103–105] to improve the power sharing and stability of microgrids with multi-DERs. To provide high reliability and robustness against network failure or time delays, droop-based control schemes are designed to specify the frequency of each DER unit by using complementary loops and fuzzy logic controllers [107], robust $H_\infty$ controllers [86], and PI controllers [107, 108]. On the other hand, novel approaches for mitigating the impact of random time delays quantify robust delay margins [109]. The delay margin-based sparsity-promoting wide-area control strategy, which requires few system observations, can reduce communication requirements and yield nearly optimal performance compared with centralized control [109]. Nevertheless, packet dropout still has the potential to affect the performance of this strategy.

### 1.2.2 Reliability of CPSs

Distributed renewable energy sources are increasingly connected to power distribution networks as a remedy for environmental and economic concerns [110–112]. However, their power outputs are dependent on the available intermittent natural resources, such as solar irradiation, wind velocity, and biofuel production [113–115]. The rapid deployment and commercialization of storage devices and electric vehicles (EVs) has become an attractive technological solution to facilitate the use of renewable energy sources, manage demand loads, and decarbonize the residential sector [115–117]. The above technological issues call for managing real-time energy imbalance in DGSs to meet electricity demand over a long-term horizon. In order to address the challenges of distributed control of energy sources, communication networks are being installed for accurate control of the different power sources and the timely operational scheduling of distributed generator (DG) units, with the objective of providing reliable and sustainable energy in a timely fashion [118–123]. However, most existing research works do not formally investigate the capability of communication networks in providing real-time power management and promoting the optimal power dispatch [124–127]. The effective integration of communication networks into DG systems is a key step in the realization of future smart grids [90, 128].

Most integrated system-of-systems models have been developed based on dedicated and closed communication networks, where the infrastructure is exclusively built for smart grid applications [90, 128, 129]. As the network is dedicated between the DG and the control center, the data exchange is assumed to be perfect and free of defects (e.g., induced time delays and packet dropouts [130–134]). However, experience has shown that dedicated communication networks are ill-suited to future DG systems, which require a different, more complex but much cheaper network, as its dimension would be much larger [135–137]. Because of the low installation cost, high transmission speed, and flexible access, the open communication network has the highest potential for integration with future DGSs [82, 84, 138]. As end-users have to share the limited bandwidth in the open communication networks, which could lead to local congestion, they can be unreliable and suffer from network-induced delays and packet dropouts [139–141].

Existing research works [42, 123, 139–146] do not model explicitly and adequately the behaviors of transmission delays and packet dropouts. Most of the aforementioned models are limited to constant or less stochastic transmission delays, which are not true in reality [147, 148]. The delays are described by discrete-time models or are neglected by assuming that they are much smaller than the communication interval [17, 123, 149, 150]. Packet dropouts are usually modeled by a two-state Markov chain and the associated quantitative loss rates; the detailed state evolution is masked and only input/output information is made available. The state transition matrix is known by assuming that the evolutions of packet dropouts can be fully observed [123, 140]. Additionally, the models of uncertain renewable power sources do not consider time-correlated properties [42, 123, 139, 142, 143, 151]. Consequently, the control schemes derived based on such assumptions can be very conservative and may not be readily applicable to real systems.

To bridge this gap, a generic and transparent mathematical model is necessary for the analysis of the impacts of integration of unreliable open communication networks (e.g., home area networks, neighborhood area networks, and WANs). The major challenges lie in the modeling and simulation of the interactions between degraded communication networks and DG systems, and the optimization of the real-time energy management problem on such system platforms. Note that the specific requirements (i.e., high-frequency data and data prediction) introduced by communication network integration need to be taken into account in this modeling, simulation, and optimization framework.

## 1.3 Opportunities for CPS Applications

### 1.3.1 Managing Reliability and Feasibility of CPSs

CPSs perform critical tasks in many industrial applications, for example, manufacturing systems [152], transportation systems [153, 154], and power systems [18, 155]. The components of control systems, that is, actuators and sensors, are subject to degradation when operating under severe working conditions [155–159].

Sudden load variations in electric power systems are often balanced by promptly changing the output of natural gas power plants following the LFC strategy [160]. However, the degradation of gas turbine compressors, that is, the deviation of compressor flow capacity and isentropic efficiency [161], and the degradation of PMUs, that is, measurement drifts and errors [162, 163], reduce the LFC performance by decreasing the available balancing power, and by producing inaccurate frequency readings. Deteriorated LFC performance may result in power system failures because the system frequency exceeds its maximum allowable drop or fails to attain the steady-state frequency tolerance band in the required time in compliance with ISO 8528-5 [164]. As a result, power system failures are determined by the LFC performance, stemming from the partial information on the power system conditions, that is, the health indexes of gas turbines (flow capacity and isentropic efficiency), and measurement drift. Therefore, it is necessary to study these degradation processes to predict the real-time LFC performance loss and ensure adequate LFC through proper maintenance activities.

Lifetime prognostic studies of gas turbines [165] have shown that the failure time of these systems varies between 24 000 h and 35 000 h. Such variability stems from different working conditions [166] and different starting points of the degradation paths [167]. Therefore, the degradation model should reflect the unit-to-unit variability in the degradation process of gas turbines [168]. Moreover, many condition-based maintenance (CBM) models determine maintenance activities based on the estimated remaining useful lifetime (RUL) of gas turbines using health indexes (reduction in flow capacity and isentropic efficiency [161]) derived from on-line measurements, for example, rotor speed, inlet temperature, and pressure [169, 170]. Maintenance activities are scheduled based on the two health indexes. However, in control systems, failures are determined by the system performance [171] and not by the health indexes of individual components, that is, they are system-level failures rather than component-level failures [172–174]. Control systems may still operate normally even if the component health indexes exceed failure thresholds [157, 175].

In addition, the feedback control mechanisms hide the explicit mapping from the individual component degradation state to the control performance loss [175]. It is easy to estimate the RUL of an individual component, but difficult for degraded control systems, because their failure time cannot be described by any particular distribution [171, 176]. Therefore, when applied to degraded control systems, general CBM models should connect the component degradation and the control performance loss, so that maintenance activities depend on the reduction of control performance [176].

The Wiener process is often employed in degradation models because of its favorable mathematical properties; in particular, it can capture non-monotonic degradation signals frequently encountered in practical applications, because consecutive independent increments are normally distributed [172]. Therefore, this stochastic process has been widely applied to characterize the path of degradation in realistic scenarios, where fluctuations are observed in the degradation process, for example, brake-pad wear for automobiles [177], bearing degradation [174, 178], gyroscopes in inertial navigation systems [172, 179, 180], contact image sensors in copy machines [181], the resistance of carbon-film resistors [159], and the pitting corrosion process [167]. To overcome the aforementioned limitations, the Wiener degradation model with unit-to-unit variability is introduced to describe gas turbines exhibiting different lifetimes. The Wiener model considers the random starting time of the degradation process, which follows a non-homogeneous Poisson process [167, 182]. Furthermore, the drift parameter, which denotes the aging rate, is also variable and follows a normal distribution, where the mean denotes the average aging rate and the variance represents the variability in the aging rate [170, 183–186]. These parameters can be estimated from the lifetime dataset via an expectation-maximization (EM) algorithm [172, 180, 183–186].

Thus, the data-driven degradation model with unit-to-unit variability is integrated into the control system model described by control block diagram, resulting in a real-time simulation model. In such control models, the interplay among the reduction in the control signal due to component degradation, the transfer functions of the subsystems, and the feedback control loop, provides the mapping between the component degradation states and the system performance loss. This interaction is modeled via control-block diagrams, which implement the feedback control mechanism and quantify the control signal by comparing the control performance to the setpoint. Therefore, such an integrated model does not require explicit mapping from the component degradation states to the system performance loss and is well-suited to represent a degraded control system. As such, this simulation model realistically predicts the performance of the control system at different operating times and degradation stages.

### 1.3.2 Ensuring Cybersecurity of CPSs

Attacks on complex systems, for example, CPSs, are fundamentally different from traditional internal failures (e.g., degradation and design) and external failures (e.g., natural disasters) [187–190]. Many attack models for complex systems embrace a partial perspective, which only focuses on component vulnerability, and neglects the dependence of system performance on it [191–193]. As a result, the insights provided by these models are not adequate for providing general recommendations in realistic applications. To address this

limitation, recent studies investigate the influence of component vulnerability (attacks at the component level) on system performance [194–197].

Pioneering works [192, 198–202] develop optimal defense strategies to minimize the attachment vulnerability of parallel systems, assuming that attackers maximize either the damage probability or the expected damage over a time horizon. They also consider general features, that is, imperfect false target techniques and genuine targets [201, 203]. These defense strategies reach a trade-off between increasing the protection of existing components and providing redundancy by allocating additional components [192, 203–205].

System performance is an essential feature in CPSs that can still operate if some components are unavailable and, therefore, are characterized by multiple performance levels [206–211]. System performance degrades with increasing component destruction or unavailability; if the system performance level decreases, the required demand may be partially unsatisfied. Two risk measures can be used for multi-state complex systems [203–205]: 1) the probability that the demand is not satisfied is considered for complex systems that fail if performance cannot meet demand, for example, automatic train protection and block systems [212, 213], and power system dynamic security systems [190]; 2) the expected damage proportional to the unsupplied demand is considered for complex systems that can operate even if the demand is partially supplied, for example, mobile ad hoc networks [191], NCSs [214, 215], supervisory control and data acquisition (SCADA) systems [216, 217], water distribution networks [218], and electric power grids [219–221].

Several works consider both the vulnerability and performance of complex systems subject to attacks [201–207, 222, 223]. These works generally describe a case as a dynamic contest between an attacker and a defender to develop a component vulnerability model and a multi-state system performance model. The number of destroyed components quantifies the demand loss and expected damage costs [200, 205]. To make the above contest more realistic, attack time uncertainties and the attacker's preference on the attack time should be considered.

In the literature, two different approaches exist for determining the attack time, that is, the strategic selection and the selection based on probability distributions. In the former, the attacker strategically selects whether to attack at some point in time or at a later point in time, based on the outcome of the game, given that the attack occurs at a specific time [224]. Thus, complex attack and defense strategies can be derived from a two-stage min-max multi-period game. Extensive attack or defense in one period limits the attack or defense that can be exerted in the next period, and vice versa. Thus, players strategically choose whether to exert effort now or in the future [224–226]. The defender may determine optimal resource allocation strategies for redundancy [192] and protection, that is, individual or overarching protection [205, 227–229]. On the other hand, the attacker may distribute the constrained resources optimally across sequential attacks [230–233].

In the second approach, the attacker prefers to conduct the attack at the time of the critical event [206]. Indeed, attacks in Nice, Berlin, Manchester, and London occurred several days before and after Bastille Day, Christmas, a concert, and the Champions League 2017 Final, respectively. In these cases, the defenders have increased the protection level in the immediate aftermath; therefore, it is not worthwhile and cost-effective for the attacker to deploy another attack in a short period. Because attacks occurred at critical times, they can greatly influence public opinion. As a result, the attacker aims to maximize the system loss

by strategically selecting a set of elements to attack based on the two-stage min-max game [234]. Because we can predict the distribution of the time at which the critical event occurs, the attack time can be inferred from a data-driven probability distribution [192]. The two approaches aim to maximize the outcomes of the game given that the attack occurs at a specific time under a similar system structure and variable resources.

The truncated normal distribution is used to describe the uncertainty of the most probable attack time, that is, the time of the critical events, and the accuracy of the defender's estimate of it [206, 235, 236]. The truncated normal distribution has been adopted to represent uncertainties in many realistic applications, for example, traffic peaks of online video websites [193], the peak season of power supplies [237–239], the peak demand of water distribution systems [240], and the rush hour of public transportation [241]. Accounting for the influence of this uncertainty increases the relevance of the insights gained for the optimal resource allocation strategy against attacks.

CPSs are a new class of engineered complex systems that provide tight interactions between cyber and physical components. The corruption of a small subset of their components has the potential to trigger system-level failures leading to entire system performance disruptions [191, 215, 221, 242]. Previous studies on attack vulnerability and performance of complex systems can be extended to identify resource allocation strategies for cyber components and promote system performance during cyber-attacks in CPSs [243, 244]. Cyber vulnerabilities are exploited by attackers to launch insidious attacks on the integrity, confidentiality, and availability of cyber data by injecting false data into measurement devices, eavesdropping estimation of system states, and deploying denial of service (DoS) attacks on communication networks [216, 217, 220, 245]. More sophisticated attack models specifically target weaknesses to cause maximal damage [191]. In this respect, it is key to capture the uncertainties intrinsic to the behavior of the attacker and the defender.

With respect to applications in smart grids, upgrading traditional grids to smart grids has brought many benefits to the overall management of power and energy systems, including higher reliability, better efficiency, improved integration of RERs, more flexible choice for stakeholders, and lower operation costs [246–248]. However, the core technologies, for example, communication techniques and SCADA systems [249–252], which deliver the advantages of smart grids, also open the grids to vulnerabilities that already exist in the information and communications technology (ICT) world. These vulnerabilities pose threats to smart grids, such as DoS attacks, false data injection, replay attacks, privacy data theft, and sabotage of critical infrastructure [253–255]. In addition, the failures in a smart grid caused by cyberattacks can easily cascade to other highly dependent critical infrastructure sectors, such as transportation systems, wastewater systems, health care systems, and banking systems, resulting in extensive physical damage and social and economic disruption [249, 256].

While government, the private sector, and academia are recognizing the cyber vulnerability of smart grids, the likelihood and impact of a cyberattack are difficult to quantify. Furthermore, for a smart grid, there may be mandatory standards and operational requirements from grid stakeholders. Current risk management strategies are generally qualitative or heuristic [257]. In these strategies, some assumptions, for example, constant reward with respect to successful anti-cyberattack [258, 259], may be unrealistic for most smart grids.

Chapter 7 presents a probabilistic risk analysis framework to enhance smart grid cyber security. In particular, the dynamic and stochastic characteristics of smart grids, such as uncertain demands, are taken into account to investigate the effect of defending strategies on the real operation cost. The optimal power flow (OPF) model [260] is applied to an 11-node radial smart grid originating from the Elia grid in Belgium. Compared with the existing studies that focus on the inherent risk [254, 260], such as the natural degradation and uncertain RERs for better maintenance actions and power dispatch, Chapter 7 addresses the impact of the external threat (cyberattacks) on the operation cost for effective deployment of cyber defense teams. In previous works, the cost of each attack on a node was assumed to be a constant [259]. Nevertheless, by investigating some practical scenarios, it has been found that the costs are more likely to be determined by some adversarial factors. Therefore, an adversarial cost sequence associated with each node is assumed, and a widely used variation constraint is introduced for each cost sequence. To cope with the objective of sequential decision strategies, the problem is formulated using the reinforcement learning framework [261–263]. In particular, the Bayesian prior method [259] is employed for the model parameters, and the problem is formulated as a Bayesian adversarial multi-node bandit model. In addition, a Bayesian minimax type regret function is constructed, which is subject to the learning context.