IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received April 24, 2019, accepted May 12, 2019, date of publication May 31, 2019, date of current version June 13, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2920317

Soft Computing Techniques for Dependable Cyber-Physical Systems

MUHAMMAD ATIF[1], SIDDIQUE LATIF[1,2], RIZWAN AHMAD[1], ADNAN K. KIANI[1,3], JUNAID QADIR[4], ADEEL BAIG[1,5], (Senior Member, IEEE), HISAO ISHIBUCHI[6], (Fellow, IEEE), AND WASEEM ABBAS[4]

[1]School of Electrical Engineering and Computer Science (SEECS), National University of Sciences and Technology (NUST), Islamabad 44000, Pakistan
[2]Institute for Resilient Region, University of Southern Queensland (USQ), Springfield Central, QLD 4300, Australia
[3]London South Bank University, London SE1 6LN, U.K.
[4]Information Technology University (ITU), Lahore 54600, Pakistan
[5]College Engineering and Architecture, Al-Yamamah University, Riyadh 13541, Saudi Arabia
[6]Shenzhen Key Laboratory of Computational Intelligence, University Key Laboratory of Evolving Intelligent Systems of Guangdong Province, Department of Computer Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, China

Corresponding author: Hisao Ishibuchi (hisaoi@cs.osakafu-u.ac.jp)

This work was supported in part by the National Natural Science Foundation of China under Grant 61876075, in part by the Program for Guangdong Introducing Innovative and Enterpreneurial Teams under Grant 2017ZT07X386, in part by Shenzhen Peacock Plan under Grant KQTD2016112514355531, in part by the Science and Technology Innovation Committee Foundation of Shenzhen under Grant ZDSYS201703031748284, and in part by the Program for University Key Laboratory of Guangdong Province under Grant 2017KSYS008.

ABSTRACT Cyber-physical systems (CPSs) were envisaged as a way to manipulate the objects in the physical world through computer intelligence. This is usually done by providing a communication bridge between actuation and computing elements. This sought after control is hampered not only by the unavoidable certainty found in the physical world but also by the limitations of contemporary communication networks. These limitations hamper fine-grained control of elements that may be separated by large-scale distances. In this regard, soft computing is an emerging paradigm that can help to manage the unreliability of CPS by using techniques, including fuzzy systems, neural networks, evolutionary computation, probabilistic reasoning, and rough sets. We present a comprehensive contemporary review of soft computing techniques for CPS dependability modeling, analysis, and improvement. This paper provides an overview of CPS applications, explores the foundations of dependability engineering, and highlights the potential role of soft computing techniques for CPS dependability with various case studies while also identifying common pitfalls and future directions. In addition, this paper provides a comprehensive survey of the use of various soft computing techniques for making CPS dependable. This paper is timely due to the increasingly central role that CPSs are beginning to play in modern societies and the need to leverage all the relevant methodologies and tools (such as those provided by soft computing) for the development of highly dependable CPS.

INDEX TERMS Cyber-physical-systems, soft computing, machine learning, smart systems, communication networks, dependability, reliability analysis, reliability optimization.

I. INTRODUCTION

The internet has transformed human life in all sorts of beneficial ways. It has become an indispensable tool for all kinds of operations in the fields of business, manufacturing, trade, education, and services. Despite the ubiquity of high-speed data networks, the gap between the cyber world, in which information is exchanged or processed, and the physical world is not yet bridged [1]. This motivates a Cyber-Physical System (CPS) vision that will integrate computational resources into the physical world [2] to allow for better control over processes that generate and use information. A CPS can be envisioned as the orchestration of physical entities and computers in which embedded computing components control and monitor the physical processes, typically through feedback loops, and physical processes and computations interact with each other closely [3]. Examples include autonomous unmanned aerial vehicles (UAVs), self-driving cars, and home automation systems.

The associate editor coordinating the review of this manuscript and approving it for publication was Xiao-Sheng Si.

CPS began to emerge as an "engineering discipline" in 2006, although its intellectual roots date back considerably further [4]. The terms "cyberspace", "cyber-physical systems" share a common root with the term "cybernetics" that was coined by the influential American mathematician Norbert Weiner in the 1940s as the name of a new field that he founded which focused on the unification of physical processes along with the computation and communication using ideas from control systems theory. As discussed in [3], CPS is now an important independent field of engineering that demands its own techniques, theory, methods, and models. The ubiquitous presence of embedded systems and high-speed data networks and the potential benefits of CPS has led some leading thinkers to anticipate that the CPS revolution of the 21st century will likely overshadow the IT revolution of 20^{th} century [5].

The decreasing cost of complex embedded electronics, due to which embedded technology is finding its way into all kinds of everyday products, is heralding a vision of CPS with virtually endless benefits [6] [7]. CPS already exist in many forms including utility networks, transportation systems, and underlie many different industries such as entertainment, business, healthcare, manufacturing, and services [8]. More generally, one can envision CPS as a broad field that encompasses trends such as the Internet of Things (IoT), sensor networks, Machine-to-Machine (M2M), fog computing, and "Social Dispersed Computing" [9].

Some prominent CPS applications include the following (a more detailed description follows in the next section):

1) factories can be operated much more efficiently allowing us to cut down on greenhouse gas emissions;
2) autonomous vehicles, aware of other vehicles and obstacles in their vicinity, will allow us to manage urban problems like traffic congestion and to minimize pollution;
3) self-aware integrated healthcare systems will allow us to provide universal healthcare; and
4) the generation of electrical power can be managed better through "smart grids";
5) the security of individuals can be improved through intelligent surveillance and monitoring to reduce urban crime and reduce terrorism thread.

The socioeconomic benefits of CPS technology have been long recognized (decades before the coinage of term CPS) [10]. But the true benefits envisioned with CPS have yet to be unleashed [4]. Apprehension such as the lack of reliability, predictability, and lack of real-time control in today's computing and networking technologies impedes the broad adoption of CPS applications, especially for mission-critical applications (such as automotive safety, traffic control, and healthcare). For mission-critical applications, *dependability* and *reliability* assumes paramount importance since CPS must be robust enough to withstand unexpected conditions in communication networks and capable of adapting to subsystem failures [5]. In general, system dependability is often a non-compromisable fundamental requirement of most CPS applications due to the potential of great loss (financial loss or even loss of life).

In the world of today, the underlying components (embedded hardware and control sub-systems) of most CPS are quite dependable. However, attempts to unify them through network interconnection(s) introduce complexities and elements of uncertainty that can compromise their dependability. CPS is still vulnerable since it may suffer from deficiencies such as the lack of 'temporal semantics', and an inadequate concurrency model. In fact, a failure or an attack on a single component could initiate the cascading failure phenomenon with detrimental consequences for the overall system. CPS operations are marked by the faster operational time scales, dynamic environments, heterogeneous components, and a large number of mixed-initiative interactions [11]. All these factors introduce a certain degree of imprecision and uncertainty in the information required to undertake the necessary computations. Hence, a computational framework that can deal with all these factors is needed.

Soft computing techniques have emerged as an enabler to make CPS more robust and adaptable. Soft computing techniques were invented to overcome the limitations of traditional ('hard') computing techniques that rely on deterministic analytic techniques that aim to exactly solve problems while assuming full knowledge of the parameters involved [12]. Unfortunately, such assumptions are not met in practical real-life systems in which imprecision and unavailability of exact prior knowledge is the norm rather than an exception. Soft computing, in strict contrast to hard computing, can work with imprecision, uncertainty, and incomplete information to achieve approximate "good enough" solutions to computationally hard problems at lower costs [13], [14]. For example, soft computing can use computational intelligence techniques to heuristically solve intractable Non-deterministic Polynomial-time (NP-) complete problems [15] to produce approximate "good enough" solutions. A comparison of hard and soft computing is presented in Table 1.

TABLE 1. Hard vs Soft Computing (adapted from [13]).

Attribute	Hard Computing	Soft Computing
Accuracy vs. Robustness	Accuracy mandatory	Robustness has priority
Logic	Binary logic	Multi-valued logic
Input data	Exact data required	Can tolerate imprecise data
Computation mode	Mostly Sequential	Supports parallelism
Precision of results	Precise answers	Approximate answers
Determinism	Deterministic	Non-deterministic

Various studies, books, and review articles on the scope and applications of CPS are available in existing literature [5], [16]–[18], due to the enormous industrial and scientific research in CPS. Similarly, soft computing techniques for modeling, analysis, and optimization of specific CPS problems or aspects have been heavily researched in the literature [19]–[22]. *However, despite the vast literature, a comprehensive survey on the role of soft computing techniques*

TABLE 2. Comparison of our survey with existing surveys, review papers and books.

Authors	Year	Theoretical Foundations	Application Domains	Dependability Discussed	Soft Computing Discussed	Open Issues or Challenges
Wan et al. [22]	2011	✓	General CPS	✓	×	✓
Shi et al. [17]	2011	≈	General CPS	≈	×	✓
Gunes et al. [8]	2014	✓	General CPS	✓	×	✓
Khan et al. [19]	2014	✓	General CPS	✓	✓	×
Mitchell et al. [21]	2014	✓	General CPS	≈	✓	✓
Khaitan et al. [20]	2015	✓	General CPS	✓	×	✓
Lee et al. [3]	2015	✓	General CPS	≈	×	✓
Humayed et al. [23]	2017	✓	Multiple domains	×	×	✓
Ding et al. [24]	2018	×	Industrial CPS	✓	≈	✓
Our Survey	2019	✓	Multiple Domains	✓	✓	✓

✓ means covered; × means not covered; ≈ means partially covered

TABLE 3. List of abbreviations.

ACO	Ant Colony Optimization
ANN	Artificial Neural Network
BN	Bayesian Network
CPS	Cyber-physical system
CS	Cuckoo Search
EC	Evolutionary computation
FL	Fuzzy Logic
FS	Fuzzy Set
FT	Fault Tree
FTA	Fault Tree Analysis
GA	Genetic Algorithm
IDS	Intrusion Detection System
MC	Markov Chain
MLN	Markov Logic Network
MRF	Markov Random Field
NCS	Networked Control System
PN	Petri Net
PR	Probabilistic Reasoning
PSO	Particle Swarm Optimization
RAP	Resource Allocation Problem
RBD	Reliability Block Diagram
RL	Reinforcement Learning
RS	Rough Set
RST	Rough Set Theory
SA	Simulated Annealing
SPN	Stochastic Petri Net
SVM	Support Vector Machine
TS	Tabu Search

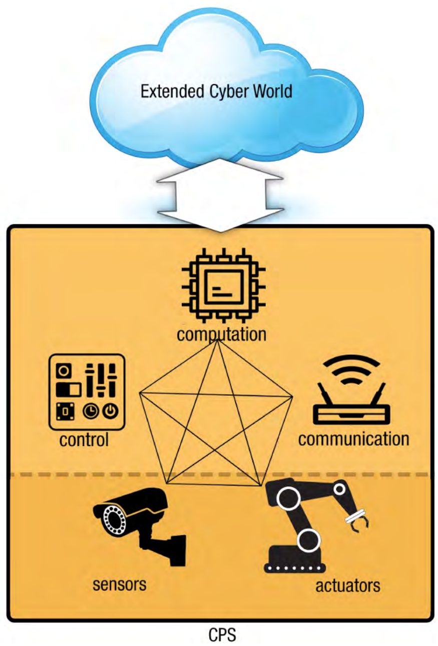

FIGURE 1. The building blocks of a cyber-physical system (CPS).

in dependable CPS is missing in the literature. This is highlighted in Table 2, where we compare our survey paper with existing resources in the same space.

To summarize, the main highlights of our paper are as follows: (1) this paper provides an overview of CPS and their applications in real life; (2) concepts related to the reliability of CPS are introduced in detail; (3) a detailed taxonomy of soft computing techniques is presented; (4) applications of soft computing techniques for modeling, analyzing, and improving the dependability of CPS are discussed; (5) insights are shared on the suitability of various soft computing techniques for various CPS dependability modeling, analysis, and optimization tasks, and finally (6) open issues and directions for future works are identified.

The rest of the paper is organized as follows. In section II, we present application domains of CPS and motivate dependability in CPS by highlighting various attacks in these domains. In section III, a detailed survey of existing soft computing techniques being used to improve or assess the dependability of CPS is presented. Section IV discusses the

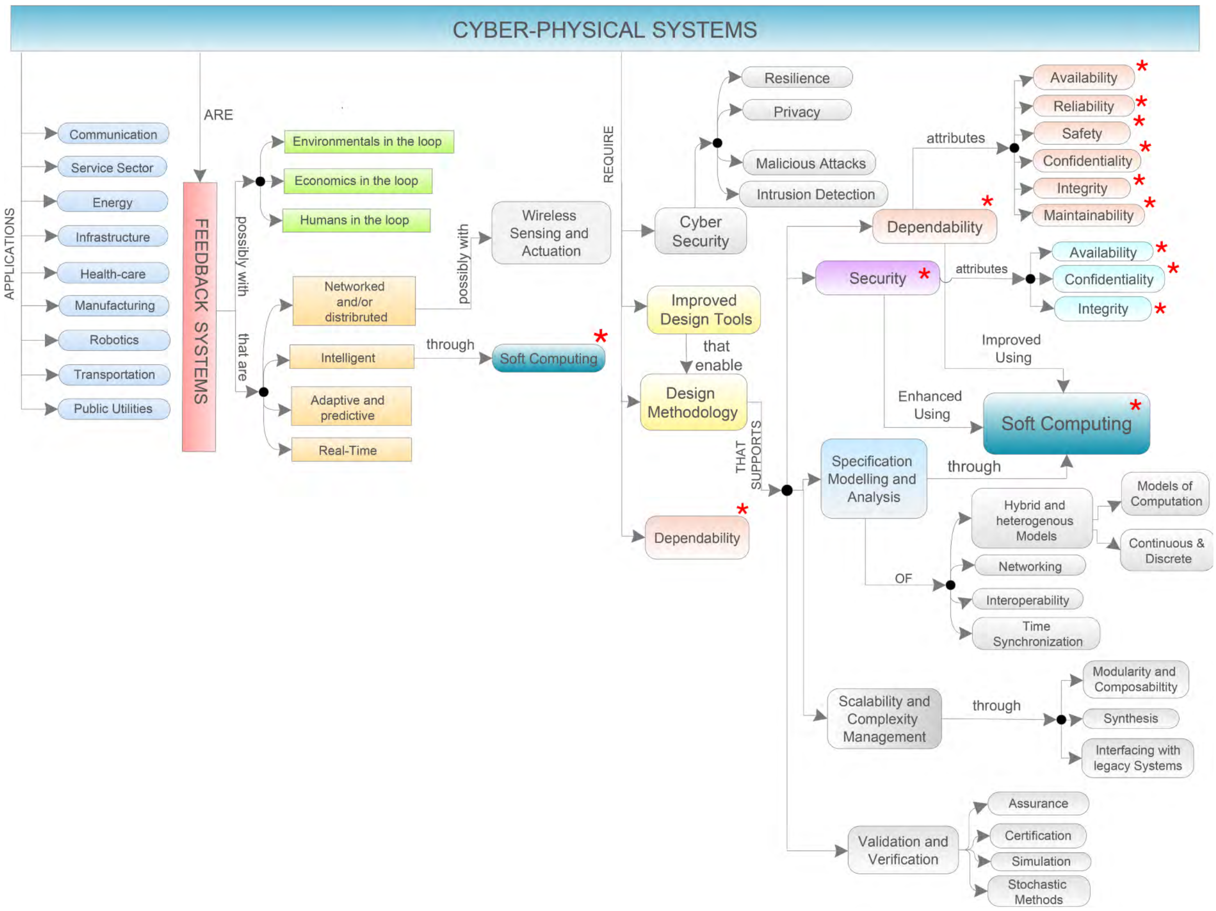

FIGURE 2. A concept map of cyber-physical systems (extended from [4], additions marked*).

limitations of current research, open issues and directions for future work. A list of abbreviations used frequently in the paper, as related to soft computing or dependability analysis, is also included (Table 3).

II. BACKGROUND: SOFT COMPUTING FOR DEPENDABLE CPS

A. DEPENDABLE CPS BASED APPLICATION DOMAINS

CPS integrate physical processes with computation and networking. Figure 1 shows a typical CPS with the integration of Control, Communication, and Computation. They are sometimes referred to as a Networked Control System (NCS), Distributed Control System (DCS) and (variants of) Sensor Actuator Networks (SANs) [25]. It is possible to conceptually model a CPS as a temporally-integrated distributed control system [3]. CPS allows the integration of multiple technologies that have applications spread over several engineering disciplines as highlighted in Figure 2.

1) ELECTRICAL POWER GRID (SMART GRIDS)

The power grid is a complex and geographically distributed collection of entities that generate, regulate, and utilize power. A combined system of power generation, large-scale distribution, and automated power management in the consumer premises, form a CPS. Smart grids can perform real-time distributed sensing, measurement, and analysis of the production and distribution of electrical power [16]. This optimizes resource utilization while also reducing greenhouse gas emissions. Smart grids, however, are vulnerable to cyber and cyber-physical attacks [26] over and above traditional elements of failure in complex systems.

2) WATER NETWORKS

Water networks are critical infrastructures that have national importance. Water networks can be very complex consisting of various sensing devices and their complexity is rapidly increasing to meet the rising demands of big cities and industries. Like smart grids, they too are vulnerable to cyber and cyber-physical attacks. Such threats are a real concern in the modern age [27]. The integration of essential utility networks into a CPS mandates a secure and dependable framework for CPS operations.

3) INDUSTRIAL AUTOMATION

CPS can provide a broad control over complex and larger industrial facilities by using network architecture that embodies heterogeneous sensors, processors and actuators [28]. CPS in the industrial chain will result in unprecedented profits for industry and flexibility for consumers [29]. This convergence of automation in the industry with computing and real-time networking is being hailed as the next industrial revolution. This has the potential to optimize the entire cycle of production from the supply chain, manufacturing, inventory management, storage, and trade. The "industrie 4.0" initiative [30] was taken by the German government to bridge the gap between apparently disparate elements in the supply and production chain. Standards and protocols for communication between often heterogeneous elements in the industrial process are being developed. The introduction of intelligent systems in industrial automation will make the industry more adaptive to customer requirements. Industrial systems are relatively closed environments (compared to utility and transport networks) with well-defined objectives. As such earlier soft computing techniques like FL were traditionally applied in either design of reliable industrial systems [31]–[33] or for improving their productivity under given design constraints. The same objectives were later sought through the soft computing techniques discussed in section 3 (i.e. EC, GA, ANN, PR, and RST, etc.) These soft computing techniques are also used to improve system security.

4) INTELLIGENT TRANSPORTATION SYSTEMS (ITS)

Context-aware vehicular CPS with cloud support will provide more convenience and better safety for pedestrians, passengers, and drivers [34]. Such systems will minimize urban traffic and parking problems. Smart transportation will assist in times of disaster for emergency evacuation of urban population [18]. Whereas the infrastructure and vehicles required for truly smart transportation systems are in their infancy, the aviation industry is far more mature in terms of technology and communication networks. A failure in ITS can lead to environmental impacts, time wastage, and the compromising of public security. Such failures can come from a number of security flaws in the system by designers or due to individual components in ITS [35].

5) HEALTHCARE

In recent years, CPS are gaining considerable interest for their promising applications in healthcare. Such systems can integrate health monitoring devices such as sensors, actuators, and cameras with cyber components and intelligence. Recently various CPS architectures have been proposed to enhance the healthcare facilities [36] including those based on WSN-cloud frameworks and integration of cloud computing and big data analytics [37], [38]. Integration of the healthcare systems in a CPS can, however, make personal information of patients vulnerable to criminal attacks as reported in the 2017 ransomware attack [39].

B. DEPENDABILITY BACKGROUND

Most of the applications discussed in the previous section further emphasize the need to make CPS operations resilient and dependable. Because the applications and services provided by a CPS must be guaranteed and dependable in different contexts (i.e. local as well as global). In this section, first, we discuss the notion of dependability in a more general context and thereafter focus more specifically on the dependability issues for CPS.

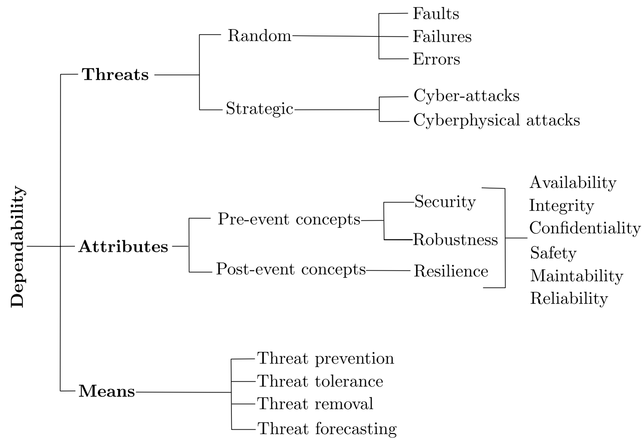

FIGURE 3. Dependability and security attributes.

Dependability is a system property that encompasses attributes like "reliability, availability, survivability, safety, maintainability and security" [40]. It essentially borrows important concepts from various technologies and merges them into one term [41]. International Standards Organization (ISO) defines dependability as *"the collective term used to describe the availability performance and its influencing factors: reliability, performance, maintainability performance and maintenance support performance"* [42]. The International Electrotechnical Commission (IEC) defines dependability in terms of the percentage of availability [42]. In computing, dependability is a property of a computing entity or system that enables the user to place reliance on the service it delivers [43]. An alternate definition for dependability as laid out by the leading researchers in the field is *"the ability to avoid service failures that are more frequent and more severe than is acceptable"* [42]. The term dependability carries different meanings in different scenarios. The complementary attributes of dependability, highlighted in Figure 3, include:

- *availability*: readiness for correct service;
- *reliability*: continuity of correct service;
- *safety*: absence of catastrophic consequences on the environment or users;
- *confidentiality*: absence of unauthorized disclosure of information;
- *integrity*: absence of improper system state alterations;
- *maintainability*: ability to undergo repairs and modifications.

These attributes are difficult to quantify in the absolute sense [40]. Real systems can never be totally available, reliable or safe: treats are inevitable in real systems. In CPS paradigm, typically we consider two different types of threats, including *random* faults and failures, and *strategic* threats consisting of attacks by an adversary with an objective to maximally disrupt the CPS operations. A dependable computing system may require a combination of multiple techniques that can provide threat prevention, threat tolerance, threat removal, and threat forecasting. The concept of dependability must be explored in terms of threats to dependability and means to attain it.

In order for a system to be dependable, it must support the following:

- *Threat prevention*: prevention of the occurrence or introduction of threats;
- *Threat tolerance*: delivery of correct service in the presence of threats;
- *Threat removal*: reduction in the number or severity of threats;
- *Threat forecasting*: estimation of the present count, future incidence and possible consequences of threats

Embedded systems electronics, in general, are far more predictable and reliable than general-purpose computing [5]. CPS should increase the reliability of embedded systems. Reliability and predictability of CPS are mandatory for their deployment in critical applications like healthcare, air traffic control, and automotive safety [3]. Other attributes like security must also be dealt with. The ever-increasing integration of new information technologies means that modern CPS face uncertainties both from the physical world and from the system's cyber components [44]. These vulnerabilities in the CPS can disclose the system to various potential risks and threats from attackers which can lead to intensive damages. Hence, it is crucial to consider both physical and cyber uncertainties while designing a reliable and robust CPS.

The robustness of CPS is its strength to resist a known range of uncertain disturbances, while its security represents the ability to withstand unanticipated and malicious events, and be protected against them. These two properties are pre-event: the CPS is designed to be robust and secure. The designing of robust and secure CPS is very costly and it is impossible to have complete security and robustness [44]. Consequently, it becomes necessary to analyze the resilience of the system (post-event), which is the system's ability to achieve recovery from disruptive events.

The concept of *security* comes in handy while describing the dependability of communication or computing systems. Security has been recognized as the composite of integrity, confidentiality, and availability [42]. Figure 3 depicts the relation between security and dependability in terms of the principal attributes of dependability. The development of a resilient CPS requires a deep understanding of disruptions caused by cyber attacks. This requires an evaluation of CPS dependability on its cyber component and its ability to withstand the failures events [45].

CPSes represent complex systems and have many loops of operation working at different scales of time and space [46]. The reliability of a complete system can (often) be estimated from the reliability of its components. The probability of failure for a system with no redundant components is more than the probability of failure of any of its individual components. The properties of a CPS depend on both the component properties as well as the system architecture [46]. The subject of reliability and dependability analysis generalizes these truths and encapsulates them into applicable frameworks. Reliability and dependability analysis of CPS is usually based on traditional techniques for systems reliability analysis [47]. Some contributions in reliability analysis of CPS include [48]–[50] and [51]. Comprehensive research on the dependability of CPS is still needed to predict their reliability and formulate methods to improve dependability. This is where concepts from traditional reliability analysis and reliability modeling must be used or extended.

Reliability analysis allows us to identify problems in telecommunication networks as well as to determine the particular redundancy requirement of a particular network [52]. *Reliability modeling* comes before analysis in the design phase. This is followed by reliability analysis in later design stages when we have more precise details about the implementation [53]. Reliability modeling is the development of a model to predict the reliability or vulnerability of a system from information available. Reliability modeling allows us to calculate dependability metrics for a system. It can be achieved by combinatorial models: Reliability Block Diagram (RBD), Fault Tree (FT), etc or through state-based stochastic models such as Markov Chains (MC) and Stochastic PetriNets (SPN) [54]. Combinatorial models allow us to represent system reliability in terms of the reliability of components and provide closed-form equations. Their complexities increases with addition of components (e.g., state-space explosion [55]). Therefore other models are needed for more complex systems. More recently Graphical Stochastic models like Bayesian Networks (BNs) have been employed for reliability modeling, either directly or by mapping fault trees into them [55], [56].

Once a model is developed, it can be examined using traditional analytical modeling techniques or through simulation tools. Formal methods are now gaining attention as a useful tool for modeling reliability and validating models [52]. Analytical models rely on the abstraction, simplification and unrealistic assumptions of the complex system. This can make them error-prone, particularly in the case of large complex systems. Formal methods are a rigorous method for analysis compared to traditional analytic and simulation techniques. Reliability assessment, analysis, and modeling of networks are beyond the scope of this paper. The reader can find a comprehensive study on reliability analysis in a paper by Ahmed *et al.* [52].

Classical modeling and reasoning techniques are based on Boolean logic, crisp classification, determinism, and analytical models. In the realm of modeling the system (or CPS) is supposed to have complete and precise details to solve the particular problem. In the real world, relevant information is often available in the form of empirically acquired prior knowledge and system behavior determined from past

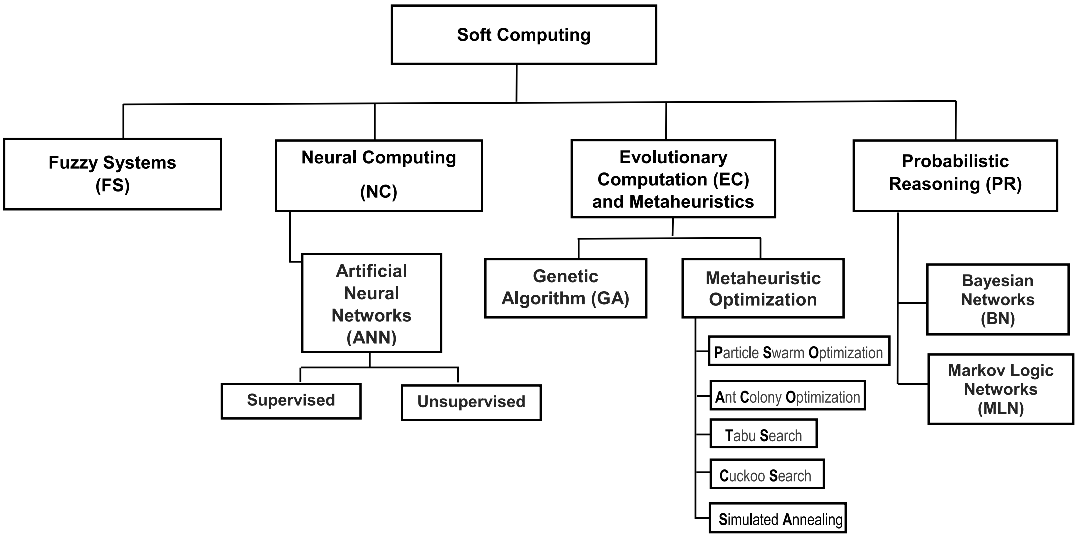

FIGURE 4. **Taxonomy of soft computing (adapted from [12], [57]).**

input-output data. In many instances, multiple solutions may exist within a large scale solution space that can fit our problem. Soft computing techniques encompass a set of flexible computing tools that can deal with imprecise information and search for approximate answers [60]. Multiple soft computing techniques can be used in cyber-physical and other complex systems to improve system dependability or to model dependability. Unlike sensor networks, CPS perform physical actions that are characterized by distributed control loops which receive essential feedback from the environment. In addition, the number of nodes and communication capabilities in CPS vary significantly. Such an ecosystem of complex smart systems leads to a hybrid system that makes use of fuzzy sets, neural networks, and evolutionary computation in different processes or stages [61].

C. SOFT COMPUTING FOR DEPENDABLE CPS

Soft computing is a collection of computing methodologies that include Fuzzy Logic (FL), (Artificial) Neural Networks (ANN), Evolutionary Computation (EC) as their principal members [14]. The taxonomy of primary soft computing techniques is shown in Figure 4. These methodologies are complementary and symbiotic for the most part as evident from the use of a combination of these methodologies in intelligent systems [14]. Later Probabilistic Reasoning (PR), Machine Learning (ML), Belief Networks (i.e. Bayesian Networks (BNs)), Chaos Theory, parts of Learning Theory and Wisdom-based Expert Systems were subsumed under the same umbrella [12]. Rough Set Theory (RST) is also considered by some researchers as a soft computing technique [57], [62] since it extends concepts from fuzzy logic.

These soft computing techniques have been used for the improvement in the dependability aspects like reliability or security of complex systems. They have also been used in modeling the reliability of complex systems and computer networks. They are required in instances when it is hard to obtain an analytical model to evaluate system reliability [63] and also prove useful when Monte Carlo simulations are not feasible to evaluate reliability. Soft computing techniques can be a substitute for simulation models (as meta-models) [63]. They are also useful in solving complex optimization problems, particularly when information is vague or incomplete. The strengths and weaknesses of different soft computing techniques are listed in Table 4. We will briefly introduce these soft computing techniques in this section and will describe their applications in the context of developing dependable CPS in the next section.

1) FUZZY SET THEORY AND FUZZY LOGIC

Fuzzy set theory has been incorporated into reliability theory by altering the conventional assumptions about the reliability of a component or system, i.e. binary state (success or failure) and probability measure of its reliability [64]. Fuzzy Logic (FL) was designed to handle imprecision using approximate reasoning [14]. It is a pioneering technology in granular computing. It has been described as a form of computing with words [65] since it mimics the human method of reasoning with words by using linguistic variables and values. FL is a generalization of Boolean logic [12] centered on fuzzy sets. Any object belonging to a fuzzy set can have a degree of membership (quantified as a real number between 0 and 1) for that particular set. Fuzzy inference maps inputs to outputs using FL. This mapping can then be used to infer patterns or make decisions. This inference involves four steps, namely *fuzzification* (real value to fuzzy membership values), *rule evaluation*, *aggregation* (of rules) and finally *defuzzification* [66]. A system's states (i.e. success and failure) can be represented by fuzzy states, and systems can be in one of these two states to some extent. Further, the failure state of the systems can be fully described by *possibility measures*

TABLE 4. Strengths and weaknesses of various of soft computing techniques (derived from [12], [57]–[59]).

Feature	Fuzzy Logic (FL)	Artificial Neural Nets (ANN)	Evolutionary Computation (EC)	Probabilistic Reasoning (PR)	Rough Sets (RS)
Training through data	No	Yes	Yes	No	Yes
Parallel Processing Ability	No	Yes	Yes	No	No
Symbolic input required	Yes	Yes	Yes	Yes	Yes
Unlabeled data support	NA	Yes	Yes	No	Yes
Computational complexity	Low	High	High	Medium	Low
Incomplete information support	Yes	No	No	No	Yes
Linguistic information support	Yes	No	No	No	No

instead of probabilities. Fuzzy logic and possibility theory are an alternative to probabilistic modeling [67]. Probability is the degree of likelihood assumed from the frequency of occurrence of an event [68]. Whereas the possibility is defined as the degree of feasibility or ease of attainment [67]. In practice, it makes more sense to use possibility, particularly in the design phase when actual frequency tables of a component's reliability are not available [68]. For small sample sizes, the probability assumption is also not valid [69].

2) EVOLUTIONARY COMPUTATION (EC) AND META-HEURISTICS

EC is a mechanism for systematic random search aimed at finding an optimal solution to a given problem [65]. Genetic Algorithm (GA) and other methods of genetic computing are special cases of EC. GAs generate a population in terms of candidate solutions to a particular problem by evaluating them on a fitness function from which good solutions are then selected. Similar to the natural evolution, surviving solutions retain the fittest parts from previous generations [70]. The best solution in each population usually survives as an elite individual and passes its characteristics to its offspring. Genetic programming (GP) is an extension of genetic algorithms. It is a technique to encode computer programs as a set of genes that may evolve using an evolutionary algorithm. EC techniques also include metaheuristic population-based optimization algorithms with names inspired by nature. Particle Swarm Optimization (PSO), Cuckoo Search (CS), and Ant Colony Optimization (ACO) [71] are some prominent EC algorithms. Metaheuristic optimization algorithms like Simulated Annealing (SA) (a stochastic optimization metaheuristic) [72], and Tabu Search (TS) [73] may also be categorized in the same group as EC. Reinforcement Learning (RL) is an adaptive (learning) search mechanism that finds the best actions based on present and past information. RL can solve the same problems solved by GA and other metaheuristics. EC and metaheuristic optimization algorithms are well suited for modeling or estimating the dependability of systems.

3) ARTIFICIAL NEURAL NETWORKS

Based on their biological counterparts, Artificial Neural Networks (ANN) are massively parallel distributed systems for information processing. ANNs are comprised of a large number of simple interconnected units that work in a parallel manner to perform a global task. The units of an ANN can learn and update the parameters as a response to an evolving input [12]. ANNs learn from training examples. They update previous estimates in light of newly available evidence [60]. ANNs are often used for supervised learning when training data is available. In some systems where this is not the case, RL can be used for training an ANN. The recent developments in deep learning have sparked a new interest in this field and motivated its use as an alternative or extension to other soft computing or machine learning methods. Deep learning can be used offline for reliability analysis in the design phase and also deployed in industrial systems for real-time robustness.

4) PROBABILISTIC REASONING

Probabilistic Reasoning (PR), also referred to as probabilistic inference and probabilistic logic in literature — deals with uncertainty and belief propagation [14]. PR is a formal mechanism based on probability theory and its subsidiary techniques with the aim of making decisions under uncertainty. It allows us to analyze stochastic systems and helps in BN cluster analysis [65]. The term probabilistic in PR hints at the reasoning mechanisms and probabilistic representations grounded in probability theory [74] and Dempster-Shafer's theory of evidence [75]. PR subsumes Chaos Theory, Belief Networks, and parts of machine learning theory [76]. Graphical methods like Markov Logic Networks (MLN) (also known as Markov Random Fields, MRF) also fall under this category [77], [78].

5) ROUGH SET THEORY

Introduced in 1982, Rough Set Theory (RST) is a relatively new method for data analysis and inference in the presence of vagueness and uncertainty [86]. They are a form of

TABLE 5. Applications of fuzzy logic in improving system performance and system dependability modeling of CPS.

Paper Reference	Soft Computing Technique	Description	Dependability Attribute
Huiling et al. 2008 [80]	FL	Software dependability evaluation. Fuzzy inference of attributes of dependability	Reliability, Availability Confidentiality, safety Integrity and Maintainability
Toosi et al. 2007 [81]	FL, ANN, GAs	Neuro Fuzzy classifiers was used as a intrusion detection system for computer networks (and GA helps to optimize structure of fuzzy decision engine). FL and ANN used to identify intrusion.	Security, Confidentiality
Knezevic et al. 2001 [82]	FL	Reliability modeling using SPNs and calculation of reliability indices using FL and lambda-tau technique	Reliability, Availability, Maintainability
Garg et al. 2014 [31]	FL	Estimation of reliability indices for industrial systems using Lambda–Tau method supported by FL (and ABC algorithm for finding fuzzy membership)	Reliability, Availability
Rotshtein et al. 2012 [32]	FL	Modeling and optimization of reliability using FL and chaos theory	Reliability
Mahapatra et al. 2006 [83]	FL	'Multi-objective optimization' based on FL for reliability optimization of series and complex systems	Reliability, Availability
Cho et al. 2002 [84]	FL, ANN	Intrusion and anomaly detection in computing systems using HMM and ANN	Security, Confidentiality
Pandey et al. 2009 [85]	FL	Early Software Fault Prediction (based on reliability metrics and expert knowledge)	Reliability, Availability, Maintainability
Mahapatra et al. 2014 [33]	FL	Complex system reliability optimization using intuitionistic fuzzy sets	Reliability
Ebrahimipour et al. 2013 [63]	FL	Fuzzy inference system based on emotional learning to improve performance of reliability evaluation systems. ANN and GA etc. used as system reliability meta-models that are hybridized using meta-heuristics.	Reliability
Tyagi et al. 2014 [86]	FL, ANN	Estimating reliability of component-based software systems	Reliability, Availability

unsupervised learning that can learn structure in data. RS theory is a method for analyzing uncertain systems and is gaining interest as a technique for knowledge discovery [59], data mining, classification and image processing. It provides a systematic framework for dealing with vagueness caused by indiscernibility when complete information about a system is not available [87]. RS need minimal model assumptions and can usually determine all parameters from within the observed data [88]. This alleviates the need for other information like the membership grade or the *possibility* values required by the fuzzy set theory [89]. RS theory can help in the construction of models that represent the underlying domain theory from a set of data alone [76]. Rough and Fuzzy set theories are different approaches to handle vagueness that attempt to remedy the difficulties with classical set theory [90]. They were an attempt at the generalization of classical set theory so that vagueness and uncertainty could be modeled [87]. RS based analysis provides a self-contained framework that can potentially obviate the need for external information such as a priori distributions in statistical analysis, model assumptions, or membership grade in fuzzy set theory. The core of RST is to weigh attributes by importance and reduce their total number [91].

III. APPLICATION OF SOFT COMPUTING TECHNIQUES FOR DEVELOPING DEPENDABLE CPS

In this section, a summary of applications of soft computing techniques for CPS dependability is provided. This work is broadly focused on CPS, and for completeness, we have included works on all components of CPS including works that have addressed the dependability of software systems, complex systems, computer networks, or any other CPS component.

A. FUZZY SET THEORY AND FUZZY LOGIC

Fuzzy inference is relatively simple to implement and has found extensive use in contemporary control systems and even in consumer appliances since the 1980s. FL has been used in the analysis of structural reliability, fault detection, probist systems (characterized by a binary state and probability of failure [92]), software reliability, safety, security and risk engineering [93]. Application of Fuzzy Set Theory and FL in CPS reliability analysis and improvement is presented in Table 5. It can be seen from the Table 5 that FL has mainly been used in fault diagnosis, Resource Allocation Problems (RAP), software reliability evaluation, safety & security assessment and intrusion detection [93].

The popularity and practicality of fuzzy logic in control applications motivated researchers to investigate and even apply it for large scale industrial or control systems in the 1990s. Traditional reliability modeling techniques are based on statistics of the past performance of a system or components. Sometimes it is not feasible to obtain such long-term data for statistical analysis. Classical reliability treatment also involves human judgment to some extent [94]. Fuzzy probabilities or possibilities [95] provide a flexible and efficient means for modeling such systems [81]. FL was traditionally focused on reliability analysis of components or systems—but there are also cases where fuzzy set theory has been used for global optimization of reliability [64]. Mahapatra *et al.* have discussed the optimization of reliability for series and complex systems with (conflicting) reliability and cost objectives. They have used a multi-objective optimization method and fuzzy parameters [33]. In another paper, the same authors have used intuitionistic fuzzy optimization for the reliability of complex systems [96].

FL is also used in conjunction with or to aid other techniques for reliability modeling improvement or optimization. Huang *et al.* [97] have used GAs to estimate boundary values of the fuzzy membership functions, and ANNs to estimate fuzzy parameters for their Bayesian model for reliability analysis. Toosi and Kahani [80] have devised an Intrusion Detection System (IDS) built upon an FL aided by ANNs. They have used GAs to optimize parameters for their fuzzy classifier. Knezevic and Knezevic [81] have used Lambda-Tau method with the aid of fuzzy logic to calculate reliability indices like availability, Mean Time To Failure (MTTF), Mean Time To Recovery (MTTR), etc. They have used fuzzy arithmetic with SPNs to model reliability with the benefit of increased flexibility and requirement of a smaller data set of prior reliability. Garg *et al.* [31] have presented a similar method to calculate reliability indices for industrial systems using Lambda-Tau technique with FL and artificial bee colony algorithm to calculate fuzzy membership degrees. Tyagi and Sharma [85] used an adaptive neuro-fuzzy inference system (ANFIS) to calculate the reliability of component-based software systems. For reliable communication network design, Lin and Gen [98] used FL with GA. They have used FL for tuning the probabilities of genetic operators. FL is used as a classifier in the IDS by Cho [83] for computer networks.

B. EVOLUTIONARY COMPUTATION AND META-HEURISTICS

EC has seen rapid growth in terms of applications for CPS reliability. GAs are a family of heuristic optimization techniques and used to find optimal solutions to diverse problems. However, optimality is not guaranteed. Because GA's ability to dig up good solutions mostly depends upon proper customization of the fitness functions, encoding, and breeding operators for the specific problem [100]. Optimization approaches like integer programming, Dynamic Programming (DP), Mixed Integer Non-Linear Programming (MINLP), and other heuristics are used to determine optimal solutions. GAs have been used to solve various complex problems from the engineering domain. They are suited to solve combinatorial optimization problems within complex search spaces. However, there are relatively few examples of their use in the field of reliability analysis. Over the past two decades, GAs have been used in diverse ways in CPS or CPS like systems. These applications include optimization of maintenance scheduling [101], [141]–[144], general redundancy allocation problem [145], [146], automated system design of fault-tolerant structures [99], smart grids [102], detection of sensor faults [107], software reliability analysis [106].

Meta-heuristic optimization techniques that fall under EC, have been used for reliability optimization and reliability analysis of various systems. ACO is a comparatively new probabilistic technique that solves combinatorial optimization search problems by selecting good paths through graphs [147]. Liang *et al.* have applied for optimal solutions of RAP in series-parallel systems [111]. Zhao *et al.* [112] have developed a multi-objective Ant Colony System (ACS) meta-heuristic for the same problem of redundancy allocation. PSO is a meta-heuristic used in reliability analysis as well as for optimization of electrical power systems. Robinson [109] have used PSO to identify critical elements in an electrical grid system. Their method is applicable for performing the reliability analysis of bulk supply systems. Mitra *et al.* have used PSO in calculating an optimal load reconfiguration strategy for the power system in an electric ship [108]. Bashir *et al.* have used PSO in the calculation of weights for their adaptive ANN that predicts hourly electric load demand in a grid. Khan *et al.* [19] have used PSO in optimizing their autopilot system for aerospace CPS to improve resilience against faults.

TS is a metaheuristic optimization technique that attempts to iterate through local optima efficiently with the aim of finding a better optimum in the process. It employs the concept of adaptive memory programming [73] and is suited for large scale problems in reliability analysis where exact solutions are not viable. TS offers an efficient solution for the general optimization of reliability in RAPs [114]. Caserta and Uribe [113] have used TS for software reliability optimization. Other noteworthy uses of TS in CPS related areas can be found in [115] and [116]. CS is a relatively recent [71] optimization algorithm inspired by the parasitic breeding among cuckoos. It is gaining significance, especially for solving redundancy allocation and reliability optimization problems [117]. Teske *et al.* have used CS in locating faults in parallel and distributed systems [118]. Applications of EC in improving system dependability or in modeling dependability are summarized in Table 6. This table reveals that GAs have been used for solving various problems in optimization in addition to the modeling of CPS dependability. Notable applications in Table 6 include parameter estimation for dependability optimization, redundancy allocation problems, electrical grid reliability optimization, and fault prediction.

SA is an algorithm of iterative search that was influenced by the physics of annealing of metals [148]. It is a probabilistic inference technique [72] that can approximate the global optimum of functions. This technique is especially suited to find a solution from a large search space. Instead of iterating through combinations, it can randomly jump to potential new solutions in an efficient manner. Attiya and Hamam [120] have discussed task allocation

TABLE 6. Applications of evolutionary computation (EC) and metaheuristics for improving system performance and system dependability modeling of CPS.

Paper Reference	Soft Computing Technique	Description	Dependability Attribute
Echtle et al. 2003 [100]	GA	Estimating reliability of component-based software systems. Custom fitness function similar to reachability analysis used	Reliability, Availability, Maintainability
Coit et al. 1996 [101]	GA	GA for allocation of redundancy in series-parallel systems	Reliability, Availability
Lapa et al. 2006 [102]	GA	Optimum preventive maintenance policies based on constraints	Reliability, Availability, Maintainability
Duan et al. 2015 [103]	GA	Power distribution network reconfiguration for reduction in losses and improved reliability	Reliability, Availability
Tian et al. 2005 [104]	GA, ANN	Adaptive on-line modeling of software reliability prediction through "evolutionary connectionist" approach. Dependability modeling through Bayesian regularization and ANN+Levenberge-Marquardt algorithm	Reliability, Availability
Tian et al. 2005 [105]	GA, ANN	Modeling of Software failure time prediction. ANN+Levenberge-Marquardt algorithm with Bayesian regularization for modeling dependability.	Reliability, Availability
Zhao and Liu 2003 [106]	GA, ANN	Stochastic Simulation, GA and ANN for solving general resource allocation problem (RAP)	Reliability, Availability
Aljahdali et al. 2009 [107]	GA	Ensemble models trained though GA to predict software reliability	Reliability, Availability
Elkoujok et al. 2013 [108]	GA	Isolation of sensor faults in non-linear systems. GA and evolving Takagi-Sugeno algorithm for depend. modeling.	Reliability, Maintainability
Lin et al. 2006 [99]	GA, FL	GA for modeling of communication networks reliability	Reliability, Availability
Mitra et al. 2009 [109]	PSO	Intelligent strategies for generator and load reconfiguration of nautical electric power systems	Availability, Maintainability
Robinson et al. 2005 [110]	PSO	Reliability analysis of (bulk) power delivery systems (electrical grids). PSO in identifying critical elements	Reliability, Availability, Maintainability
Bashir et al. 2009 [111]	PSO, ANN	Predicting hourly electric load demand	Availability, Maintainability
Khan et al. 2014 [19]	PSO	Fault tolerant autonomous control of aircraft CPS	Reliability, Maintainability
Liang et al. 2004 [112]	ACO	Redundancy allocation problem using ACO	Reliability, Availability
Zhao et al. 2007 [113]	ACO	Multi-objective ACO to optimize reliability of series-parallel systems	Reliability, Availability
Caserta et al. 2009 [114]	TS	Design of reliable software systems with optimization of redundancy	Reliability, Availability, Maintainability
Kulturel et al. 2003 [115]	TS	TS as an efficient alliterative to GAs for RAP	Reliability, Availability, Maintainability
Ramirez et al. 2006 [116]	TS	Planning optimal parameters for power distribution systems using Tabu search and FL	Reliability, Availability, Maintainability
Pierre et al. 1997 [117]	TS	Network reliability and redundancy allocation	Reliability, Availability, Maintainability
Valian et al. 2013 [118]	CS	Reliability optimization and redundancy allocation	Reliability, Availability Maintainability
Teske et al. 2015 [119]	CS	Fault detection in parallel and distributed systems	Reliability, Maintainability
Pai et al. 2006 [120]	SA	Software reliability prediction. SA, SVM used for dependability modeling	Reliability, Availability
Attiya et al. 2006 [121]	SA	System reliability optimization through task allocation in distributed systems	Reliability
Peng et al. 2018, Ni et al. 2019 [122]–[124]	RL	Smart Grids	Security, Reliability
shakeel et al. 2018 [125]	RL	Healthcare Systems	Security, Confidentiality
Ferdowsi et al. 2018 [126]	RL	Vehicular CPS	Security

in a heterogeneous distributed system to maximize system reliability using simulated annealing. Similar work by Ravi *et al.* have discussed the same problem using non-equilibrium SA [149]. Jeon *et al.* have used an SA based algorithm to optimize power distribution systems [150]. Fushuan *et al.* have applied the same technique for fault section estimation in power systems [151]. Pai and Hong [119] have used SA to calculated parameters for their support vector machine (SVM) for forecasting software reliability.

Reinforcement learning, which is an extension of dynamic programming, can also be considered in the same class as GA since both solve similar kinds of problems. It can find paths and solutions efficiently from a larger space by using a training mechanism built upon rewards of actions.

The inclusion of deep neural networks in the RL process—using deep reinforcement learning (DRL)—opens new possibilities for solving all kinds of problems efficiently and CPS dependability is no exception. RL has been applied for the detection of attacks in smart grids [121]–[123], security in healthcare CPS [124] and security in vehicular CPS [125].

C. ARTIFICIAL NEURAL NETWORKS

ANNs have been used in the analysis and optimization of reliability. They have been applied for parameter estimation for other algorithms. Their learning and prediction capability make them an indispensable tool in robust control and reliability optimization of CPS. Altiparmak *et al.* [127] have used ANNs to model the reliability of communication networks with links that have identical reliability. The node and link can vary in size in their model. Srivaree-ratana *et al.* [132] have used ANNs to learn from existing topologies and predict network reliability in an all-terminal network. Bhowmik *et al.* [133] have used ANNs in conjunction with discrete wavelet transform (DWT) to predict and classify transmission line faults. Zhang *et al.* [135] have used ANNs to forecast load demand in smart grids. Mora *et al.* [134] have used neuro-fuzzy classifiers for locating faults in smart grids. ANNs have been used to analyze and forecast software reliability. Cai *et al.* [128] have discussed the effectiveness of neural networks for handling dynamic software reliability data. Other noticeable works in this domain include Su *et al.* [129], Hu *et al.* [130], [131], Singh and Kumar [159]. ANNs have been used in combination with optimization techniques (e.g., GAs) to predict initial values for optimization. Lee *et al.* [160] have proposed a hybrid GA/ANN with FL controller for RAP.

The learning capability of ANN makes them particularly suited for IDS. They also have found multiple applications in computer networks, SCADA systems, smart grids, and other CPS-related systems. Gao *et al.* [136] discussed an IDS for smart utilities that use a three-stage back-propagation ANN. Linda *et al.* [137] have used a supervised ANN based IDS for power grid applications. Youbiao He *et al.* have used deep belief networks to detect false data injection in smart grids [161]. Kang and Kang [126] have used Deep Neural Network (DNN) structure for intrusion detection in order to improve the security of in-vehicular networks (e.g., CAN: Controller Area Network). Moya *et al.* [138] have used Self Organizing Maps (SOM) for improving the security of sensor data in SCADA systems. In recent years Long Short-Term Memory (LSTM) Neural Networks are being used to predict future values in time series data. Since they can model complex multivariate sequences and learn long-term correlations in data, they can also predict anomalies in time series data [162]. Jonathan Goh *et al.* have used LSTMs to predict anomalies and cyber attacks against CPS [139]. Zhenyu Wu *et al.* have applied LSTMs for fault prediction in CPS [140]. Jongho Shin *et al.* have used them to identify sensor attacks in automotive CPS [163]. Cheng Feng *et al.* have used LSTMs to detect anomalies and cyber attacks in Industrial control systems [164]. The application of ANN and DNN to detect intrusions in computer network traffic (Network IDS or NIDS) is an active area of research where cutting-edge research from image processing is being applied. This is in part due to their potential to detect zero-day attacks [165]. Niu *et al.* [166] have also used ANNs for fault prediction in Network Controlled Systems. Autoencoders are becoming a promising technique for IDS in IoT networks with the potential to detect attacks with an accuracy of 99 percent [167]. Applications of ANN for dependability analysis or optimization in CPS are summarized in Table 7. A glance at Table 7 indicates that ANNs have been used mainly for early fault prediction, fault localization, and intrusion detection.

D. PROBABILISTIC REASONING

The emerging paradigm of probabilistic programming and probabilistic programming languages provide a formal framework to apply probabilistic inference to uncertainty related problems [175]. Recent literature reveals a growing interest in reliability modeling using BNs, particularly to complex systems [176]. BNs estimate the distribution probabilities of a given set of variables by observing of some variables and using prior knowledge of others. BNs allow us to merge knowledge of diverse nature into a single data [55]. This is particularly suitable for complex systems. BNs establish cause-effect relationships and model their interactions. Weber *et al.* [55] have reviewed applications of BNs in dependability and risk analysis and maintenance. They report an 800% increase in interest in the use of BNs for dependability analysis.

BNs can be used to represent local dependencies as well as for predictive and diagnostic reasoning. BNs are superior to classical methods like FT analysis of complex systems [177]. Bobbio *et al.* [56] presented an algorithm for mapping FTs into BNs. Montani *et al.* [178] have developed software for this purpose. A formal analysis of this conversion for dynamic fault trees was discussed in [179]. In most engineering problems, known statistics about the reliability of a component or systems are insufficient for predicting their random behavior. Further subjective human analysis needs to be considered. Wang *et al.* [155] have used BNs for reliability modeling and prediction with subjective data sets with insufficient or incomplete information.

Weber and Jouffe [152] have introduced Dynamic Object Oriented Bayesian Networks (DOOBNs) as an alternative technique to conventional reliability analysis tools like MC and FTA for modeling the reliability of complex industrial systems. An object-oriented version of BN allows for an elegant, smaller representation of the otherwise complex BNs. BNs are suitable to model the propagation of failures in a complex system [152] because of the way they capture cause and effect relationships. Weidl *et al.* [153] have used Object Oriented Bayesian Networks (OOBNs) for isolation of faults in complex industrial systems and for decision support. They have used BNs to handle uncertainty in measured sensor data.

TABLE 7. Applications of ANN for improving system performance and system dependability modeling of CPS.

Paper Reference	Soft Computing Technique	Description	Dependability Attribute
Kang et al. 2016 [127]	ANN	Intrusion detection system (IDS) for in-vehicular networks (e.g., CAN)	Security, Confidentiality
Altiparmak et al. 2009 [128]	ANN	Estimation of reliability of telecom network with identical link reliability using encoding into ANN	Reliability, Availability
Cai et al. 2001 [129]	ANN	Software reliability modeling	Reliability, Availability
Su et al. 2005 [130]	ANN	Software reliability assessment and modeling	Reliability, Availability
Hu et al. 2006 [131]	ANN	Early software reliability prediction	Reliability, Availability
Hu et al. 2007 [132]	ANN	Software fault detection, and prediction of correction time	Reliability, Availability, Maintainability
Srivaree et al. 2002 [133]	ANN	Estimation of all-terminal network reliability	Reliability, Availability
Bhowmik et al. 2009 [134]	ANN	Transmission line fault diagnosis and classification	Reliability, Availability
Mora et al. 2006 [135]	ANN, FL	Fault localization in power distribution systems	Reliability, Availability
Zhang et al. 2010 [136]	ANN	Load forecasting in smart grids	Reliability
Gao et al. 2010 [137]	ANN	SCADA Intrusion Detection and Response Injunction	Security, Confidentiality
Linda et al. 2009 [138]	ANN	IDS for Critical Infrastructures, SCADA, etc.	Security, Confidentiality
Moya et al. 2009 [139]	ANN	SCADA sensor networks security with Self-Organizing Maps (unsupervised ANNs) and reputation systems	Security, Confidentiality
J Goh et al. 2017 [140]	ANN, LSTM	Anomaly and cyber attack detection in CPS	Security, Confidentiality
Z Wu et al. 2018 [141]	ANN, LSTM	Fault diagnosis in CPS	Reliability, Availability, Maintainability
Niu et al. 2019 [141]	ANN	IDS in Networked Control Systems	Security, Confidentiality

TABLE 8. Applications of PR for improving system performance and system dependability modeling of CPS.

Paper Reference	Soft Computing Technique	Description	Dependability Attribute
Weber et al. 2006 [153]	BN	Dynamic modeling of complex manufacturing processes using "Dynamic Object-Oriented Bayesian Networks" (DOOBNs). DOOBN (with FTA) used for dependability modeling.	Reliability
Weidl et al. 2005 [154]	BN	"Object-Oriented Bayesian Networks" (OOBNs) for isolation of faults in complex industrial systems and for decision support	Reliability, Availability, Maintainability
McNaught et al. 2009 [155]	BN	Prognostic Modeling and Maintenance Decision Making. Dynamic BNs for dependability modeling	Reliability, Maintainability
Huang et al. 2006 [98]	BN, FL, GA	Bayesian reliability analysis with parameters found using FL and GA. Estimation of pdfs of reliability using FL and Bayesian analysis	Reliability, Availability
Wang et al. 2009 [156]	BN	Reliability Analysis from incomplete and insufficient data sets. BNs for dependability modeling	Reliability, Availability
Liu et al. 2009 [157]	BN	Quantification of scalability of network resilience upon failures. BNs used for dependability modeling.	Reliability, Availability, Maintainability, Survivability
Queiroz et al. 2013 [158]	BN	Modeling and quantification of overall resilience of networked systems. MLN and MRF used for dependability modeling	Reliability, Availability, Maintainability, Survivability
Lalropuia et al. 2019 [159]	Continous MC, semi-Markov Process	Modeling attacks in CPS	Reliability, Availability, Confidentiality

McNaught and Zagorecki [154] have discussed dynamic BNs in the prognostic modeling of a component's state. Liu and Ji [156] have used BNs to model network failure. BNs show dependencies among different link failures explicitly. An MLN, or Markov Random Field (MRF), is a probabilistic logic that applies the concepts of a Markov Network (MN) to first-order logic. It is similar to a BN in the representation of dependencies. However, BNs are acyclic and directed, whereas MNs may even be cyclic and undirected. An MN can, therefore, constitute cyclic dependencies, something not possible with a BNs. On the flip side, it cannot represent dependencies such as induced dependencies that are possible with BN. Queiroz *et al.* [157] have used MN to model and quantify the overall resilience of networked systems on the basis of their adaptation and inter-dependencies of services. Applications of PR in terms of system dependability modeling and optimization are summarized in Table 8. The table shows that BNs are by far the most used PR technique. PR has also been used to model the dependability and for the prediction of faults in a variety of systems. MC and its continuous extension have been used to model the dependability of systems. Lalropuia and Gupta [158] have used semi-Markov Process, stochastic games and continuous time Markov processes to estimate dependability measures

TABLE 9. Applications of rough set theory for improving system performance and system dependability modeling of CPS.

Paper Reference	Soft Computing Technique	Description	Dependability Attribute
Peng et al. 2004 [169]	RST	Data mining for fault diagnosis in electric power distribution feeders. RS used for dependability modeling.	Reliability, Availability, Maintainability
H Su et al. 2005 [170]	RST, ANN	Substation fault diagnosis based on RST and ANN model (in electric power systems)	Reliability, Availability, Maintainability
Chen et al. 1998 [171]	RST	Software safety evaluation (for safety-critical systems)	Reliability, Safety
Li, Bo, and Yang Cao 2009 [92]	RS	A comprehensive model for software dependability evaluation using RST. RST based modeling of dependability attributes	Availability, Reliability, Safety, Confidentiality, Maintainability and Integrity
Yuan et al. 2007 [172]	RS	Multi-state system reliability estimation using RST and Petri Nets. SPN and RST for dependability modeling	Reliability
Wang et al. 2004 [173]	RS	An RS based system that improves upon FMEA and ranks potential faults, designed for uncertain environments	Reliability, Maintainability
Joslyn et al. 2003 [174]	RS	Construction of random intervals for reliability analysis	Reliability
Song et al. 2014 [175]	RS	Reliability Modeling using FMEA and RST in uncertain environments	Reliability, Availability

like reliability, availability and condentiality. Their state-based model captures the dynamics between the attacker and a compromised CPS system and then predicts the behavior of the attacker. Chen *et al.* [180] have used MCs to model attacks in smart grids.

E. ROUGH SET THEORY

RST has been exploited to analyze the dependability of various systems. It has been used for reliability analysis of electrical power systems and mechanical systems. More recently RST has found applications in dependability analysis of software systems. Li and Cao [91] have presented a comprehensive evaluation model for software dependability using RS. The earlier fuzzy model required objective weight calculation from statistical data on software dependability. In a newer method proposed by Li *et al.*, an approach is proposed that uses a combination weight that takes an expert's subjective knowledge as well in addition to objective data. In particular, objective weight is calculated from statistical data using RST.

RST is used as a tool for knowledge extraction, to learn from and analyze past fault diagnosis records, expert diagnosis, and to extract minimal diagnostic rules. RS are then also used to rank or order these faults [172]. Joslyn [173] has discussed RS analysis to calculate random intervals from simple multi-intervals. Such intervals are required for some reliability analysis techniques [181], [182]. The aim of such analysis is to find the system failure probability interval from available statistical parameter intervals of the underlying variables [181]. Random intervals offer the advantage of representing randomness via probability theory while imprecision and non-specificity via intervals at the same time. This can complement probabilistic analysis with other techniques such as FL, plausibility and belief measure [173]. RST allows researchers to construct representations of complex random intervals and also to elicit "simple multi-interval information" [173]. Other applications of RST include the prediction of feeder faults and localization in smart grids [168] and safety-critical software systems [170].

Applications of RST in CPS dependability analysis and optimization are summarized in Table 9. This table shows that RST has been used mainly for modeling of dependability and also as a data analysis technique for fault prediction.

IV. OPEN ISSUES AND FUTURE WORKS

An extensive study of literature (summarized in Tables 5–9) reveals that among the attributes of dependability, *reliability* and *availability* have found the most applications. This is followed by *maintainability* (i.e. fault tolerance and repairability) and *confidentiality* (security). It was also noted that soft computing techniques have been used mostly for the optimization of performance or reliability of systems. Soft computing has been used in aiding reliability and dependability analysis of systems as well. Soft computing cannot be a substitute for other rigorous methods of reliability analysis. In most instances, soft computing has been used in classification or to dig out extra information about the dependability of a system or to approximate reliability measures. The application of soft computing in reconfiguring a failing system or exploring a viable action from a partially collapsed system still needs to be investigated. While there is plenty of literature on dependability analysis of electrical, mechanical and even networked systems that make up a CPS, we find a general lack of literature specific to dependability analysis of CPS or synthesis of reliability analysis for CPS in terms of its components. The need for such work will increase as efforts to standardize the architecture for CPS gathers momentum [30]. Following are a few facets of CPS that are not addressed satisfactorily in literature.

A. LACK OF A UNIFIED MODELING OR ANALYSIS FRAMEWORK

The design of CPS is challenging in terms of physical systems and hardware, and even in a programming language to implement the desired level of computational behavior. A unified framework is required for consistent component-level modeling of CPS. Such a framework should be interoperable with existing simulation and verification tools [183]. This will cause an effective modeling of asynchronous dynamics by integrating event and time-based computation.

B. DESIGN METHODOLOGIES

CPSes are being deployed on a wide scale in diverse kinds of applications. Many systems including smart homes and power systems are being operated in new ways that were never intended for them [20]. Novel design methodologies are required for their seamless integration with new systems while avoiding disruption in new systems, and also to ensure dependable operation while providing new extensions of capabilities. The design of a reliable communication middleware is also an important consideration for time-sensitive CPS. This can be done through the addition of a middle-ware that actively monitors the communicating nodes and adapts them dynamically and also provides valid parameters for the design of these elements [184].

C. SECURITY

One of the major obstacles that CPS must overcome is ensuring security while maximizing mutual coordination among cyber and physical components. Reliability and security are very crucial in mission-critical CPS like healthcare, smart power grids, and networking systems. Future CPS must operate with enhanced security and reliability. There is a crucial need to develop such intelligent architectures that can ensure real-time security-state monitoring and remediation. Security performance metrics must be developed and standardized to evaluate the security of the systems. Security in CPS is a real concern since the feedback loop signals and control commands are often transported over the public networks and use open standards [185] in order to minimize costs. Intrusion Detection Systems (IDS) is a hot area of research in CPS dependability. Researchers plan to improve the CPS survivability by modeling and predicting attacks using game theory [48].

D. NETWORK INDUCED CONSTRAINTS

To the best of our knowledge, except a couple of new contributions [186], [187], little or no work exists that addresses or models the dependability of entire CPS under network constraints. Reliability in large-scale and complex network control systems (NCS) is often very difficult to model because of unpredictable random delays in the underlying communication links. Current control, communications, and software theory have not matured enough to solve problems caused by the heterogeneity in CPS. CPS can contain control loops separated by geographical scale distances. The impact that the communication network can have on closed-loop system performance [188], stability [189], and ultimately on reliability, is another area that remains to be looked at. The significance of combining control specifications and communication constraints has not been addressed [188]. NCS must cope with network induced constraints. Five different types of constraints induced by the network have been identified in the literature. These include time-variation in transmission intervals, competition among different nodes for accessing the same network, time delays, data quantization delays, and packet losses and disorder [190]. Delays in networked control systems cannot be modeled using conventional delay systems since data is transmitted in packets and scheduled through a system that is generally designed to package large amounts including the sequence of control commands. Comprehensive studies combining these constraints are not available [190]. The role of the network in closed-loop system performance [188], stability [189] and ultimately reliability remains to be explored in depth. Inserting a network in a control loop may cause deteriorated system performance or even instability [190]. In this regard, a unified theory on heterogeneous control and communication systems would help [28]. Efforts to this end must also contend with the complicated security challenges posed by CPS.

E. SOFT COMPUTING IN THE CONTROL LOOP

Soft computing is being used in improving the stability and fault tolerance of control systems. Control reconfiguration is an active approach for fault tolerant control of dynamic systems [191]. Soft computing techniques like FL and ANNs have been used in control of such adaptive systems while GAs have been used to design fault-tolerant systems. Fault-tolerant control impacts the reliability modeling and assessment of systems [192]. A discussion on soft computing directly in the control loop is another avenue to improve CPS dependability.

F. DISTRIBUTED COLLABORATIVE CONTROL

Distributed collaborative control in an unreliable wireless network [193] is yet another area where reliability analysis could be explored. The merger of reliability analysis and soft computing with modern research on distributed control systems would aid in designing more dependable CPS.

G. PROBABILISTIC COMPUTING AND CPS

The new paradigm of probabilistic computing offers a host of tools that will eventually facilitate reliability analysis. While the proponents of probabilistic programming have pointed out its use for this purpose [175], the literature on the subject is almost non-existent.

H. STANDARDIZATION REQUIREMENTS

The applications of CPS depend on various advanced technologies from different industries. This calls for standardization of different protocols that work across different CPS environments. This requirement for standardization is more than the requirement for the development of standards for traditional technologies [194]. These standardization efforts must inevitably address the stringent Quality of Service (QoS) and dependability requirements for CPS.

Soft computing can help in alleviating the shortcomings of CPS. They can predict uncertain behavior, plan for contingencies, and even assist in the design phase. Their importance in the CPS paradigm is bound to increase with the passage of time.

V. CONCLUSION

In this paper, we provide a comprehensive in-depth review of the applications of soft computing for dependability analysis and dependability improvement of CPS and similar systems. We summarize applicable domains and scenarios where one or more soft computing technique has been used in reliability analysis or optimization. This study reveals a significant lack of literature available on comprehensive reliability analysis or optimization of CPS. Given the tremendous opportunities CPS will offer in the foreseeable future and given the interest in the applications of soft computing in recent years, it is only natural to conclude that interest in the subject explored in this survey will only grow with time.

REFERENCES

[1] T. Sanislav and L. Miclea, "Cyber-physical systems-concept, challenges and research areas," *J. Control Eng. Appl. Inform.*, vol. 14, no. 2, pp. 28–33, 2012.

[2] Y. Liu, Y. Peng, B. Wang, S. Yao, and Z. Liu, "Review on cyber-physical systems," *IEEE/CAA J. Autom. Sinica*, vol. 4, no. 1, pp. 27–40, 2017.

[3] E. A. Lee, "The past, present and future of cyber-physical systems: A focus on models," *Sensors*, vol. 15, no. 3, pp. 4837–4869, 2015.

[4] University of California. (2008). *Berkeley CPS*. Accessed: Jun. 12, 2017. [Online]. Available: http://cyberphysicalsystems.org

[5] E. A. Lee, "Cyber physical systems: Design challenges," in *Proc. 11th IEEE Int. Symp. Object Compon.-Oriented Real-Time Distrib. Comput. (ISORC)*, May 2008, pp. 363–369.

[6] S. J. Oks, A. Fritzsche, and K. M. Möslein, "An application map for industrial cyber-physical systems," in *Industrial Internet of Things*. Cham, Switzerland: Springer, 2017, pp. 21–46.

[7] G. Loukas, D. Gan, and T. Vuong, "A review of cyber threats and defence approaches in emergency management," *Future Internet*, vol. 5, no. 2, pp. 205–236, Jun. 2013.

[8] V. Gunes, S. Peter, T. Givargis, and F. Vahid, "A survey on concepts, applications, and challenges in cyber-physical systems," *KSII Trans. Internet Inf. Syst.*, vol. 8, no. 12, pp. 4242–4268, 2014.

[9] M. García-Valls, A. Dubey, and V. Botti, "Introducing the new paradigm of social dispersed computing: Applications, technologies and challenges," *J. Syst. Archit.*, vol. 91, pp. 83–102, Nov. 2018.

[10] W. R. Ashby, *An Introduction to Cybernetics*. London, U.K.: Chapman & Hall, 1961.

[11] X. Koutsoukos, G. Karsai, A. Laszka, H. Neema, B. Potteiger, P. Volgyesi, Y. Vorobeychik, and J. Sztipanovits, "SURE: A modeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems," *Proc. IEEE*, vol. 106, no. 1, pp. 93–112, Jan. 2018.

[12] D. K. Chaturvedi, *Soft Computing: Techniques And Its Applications In Electrical Engineering*, vol. 103. New York, NY, USA: Springer, 2008.

[13] S. Chakraborty, R. K. Sharma, and P. Tewari, "Application of soft computing techniques over hard computing techniques: A survey," *Int. J. Indestructible Math. Comput.*, vol. 1, no. 1, pp. 8–17, 2017.

[14] L. A. Zadeh, "Soft computing and fuzzy logic," *IEEE Softw.*, vol. 11, no. 6, pp. 48–56, Nov. 1994.

[15] X. Yu and M. Gen, *Introduction to Evolutionary Computing*. New York, NY, USA: Springer, 2010.

[16] R. Baheti and H. Gill, "Cyber-physical systems," *Impact Control Technol.*, vol. 12, pp. 161–166, Mar. 2011.

[17] J. Shi, J. Wan, H. Yan, and H. Suo, "A survey of cyber-physical systems," in *Proc. Int. Conf. Wireless Commun. Signal Process. (WCSP)*, Nov. 2011, pp. 1–6.

[18] R. R. Rajkumar, I. Lee, L. Sha, and J. Stankovic, "Cyber-physical systems: The next computing revolution," in *Proc. 47th Design Autom. Conf.*, Jun. 2010, pp. 731–736.

[19] Z. Khan, S. Ali, and Z. Riaz, *Computational Intelligence for Decision Support in Cyber-Physical Systems*, vol. 540. New York, NY, USA: Springer, 2014.

[20] S. K. Khaitan and J. D. McCalley, "Design techniques and applications of cyberphysical systems: A survey," *IEEE Syst. J.*, vol. 9, no. 2, pp. 350–365, Jun. 2015.

[21] R. Mitchell and I.-R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surv.*, vol. 46, no. 4, p. 55, 2014.

[22] J. Wan, H. Yan, H. Suo, and F. Li, "Advances in cyber-physical systems research," *KSII Trans. Internet Inf. Syst.*, vol. 5, no. 11, pp. 1891–1908, 2011.

[23] A. Humayed, J. Lin, F. Li, and B. Luo, "Cyber-physical systems security—A survey," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1802–1831, Dec. 2017.

[24] D. Ding, Q.-L. Han, Y. Xiang, C. Ge, and X.-M. Zhang, "A survey on security control and attack detection for industrial cyber-physical systems," *Neurocomputing*, vol. 275, pp. 1674–1683, Jan. 2018.

[25] R. Mitchell and I. R. Chen, "Effect of intrusion detection and response on reliability of cyber physical systems," *IEEE Trans. Rel.*, vol. 62, no. 1, pp. 199–210, Mar. 2013.

[26] R. M. Lee, M. J. Assante, and T. Conway. *Analysis of the Cyber-Attack on the Ukrainian Power Grid*. Accessed: Dec. 12, 2017. [Online]. Available: https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf

[27] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," in *Critical Infrastructure Protection*. New York, NY, USA: Springer, 2007, pp. 73–82.

[28] Y. Wang, M. C. Vuran, and S. Goddard, "Cyber-physical systems in industrial process control," *ACM SIGBED Rev.*, vol. 5, no. 1, 2008, Art. no. 12.

[29] J. Lee, E. Lapira, S. Yang, and A. Kao, "Predictive manufacturing system—Trends of next-generation production systems," *IFAC Proc. Vol.*, vol. 46, no. 7, pp. 150–156, 2013.

[30] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manuf. Lett.*, vol. 3, pp. 18–23, Jan. 2015.

[31] H. Garg, M. Rani, and S. Sharma, "An approach for analyzing the reliability of industrial systems using soft-computing based technique," *Expert Syst. Appl.*, vol. 41, no. 2, pp. 489–501, 2014.

[32] A. Rotshtein, D. Katielnikov, and L. Pustylnik, "Reliability modeling and optimization using fuzzy logic and chaos theory," *Int. J. Qual., Statist. Rel.*, vol. 2012, Sep. 2012, Art. no. 847416.

[33] G. Mahapatra and T. K. Roy, "Reliability optimisation of complex system using intuitionistic fuzzy optimisation technique," *Int. J. Ind. Syst. Eng.*, vol. 16, no. 3, pp. 279–295, 2014.

[34] J. Wan, D. Zhang, S. Zhao, L. T. Yang, and J. Lloret, "Context-aware vehicular cyber-physical systems with cloud support: Architecture, challenges, and solutions," *IEEE Commun. Mag.*, vol. 52, no. 8, pp. 106–113, Aug. 2014.

[35] B. Ghena, W. Beyer, A. Hillaker, J. Pevarnek, and J. A. Halderman, "Green lights forever: Analyzing the security of traffic infrastructure," in *Proc. WOOT*, vol. 14, 2014, p. 7.

[36] I. Lee, O. Sokolsky, S. Chen, J. Hatcliff, E. Jee, B. Kim, A. King, M. Mullen-Fortino, S. Park, A. Roederer, and K. K. Venkatasubramanian, "Challenges and research directions in medical cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012.

[37] J. Wang, H. Abid, S. Lee, L. Shu, and F. Xia, "A secured health care application architecture for cyber-physical systems," 2011, *arXiv:1201.0213*. [Online]. Available: https://arxiv.org/abs/1201.0213

[38] Y. Zhang, M. Qiu, C.-W. Tsai, M. M. Hassan, and A. Alamri, "Health-CPS: Healthcare cyber-physical system assisted by cloud and big data," *IEEE Syst. J.*, vol. 11, no. 1, pp. 88–95, Mar. 2017.

[39] A. Glaser. *U.S. Hospitals Have Been Hit by the Global Ransomware Attack*. Accessed: Dec. 12, 2017. [Online]. Available: https://goo.gl/n4uEk5

[40] A. Avizienis, J. C. Laprie, and B. Randell, "Fundamental concepts of dependability," Comput. Sci., Univ. Newcastle upon Tyne, Newcastle upon Tyne, U.K., 2001, pp. 7–12.

[41] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, "A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability," *IEEE Commun. Surveys Tuts.*, vol. 11, no. 2, pp. 106–124, 2nd Quart., 2009.

[42] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, pp. 11–33, Jan./Mar. 2004.

[43] J.-C. Laprie, "Dependable computing: Concepts, limits, challenges," in *Proc. 25th Int. Symp. Fault-Tolerant Comput.*, 1995, pp. 42–54.

[44] Q. Zhu and T. Basar, "Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems," *IEEE Control Syst.*, vol. 35, no. 1, pp. 46–65, Feb. 2015.

[45] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
[46] L. Sha, S. Gopalakrishnan, X. Liu, and Q. Wang, "Cyber-physical systems: A new frontier," in *Proc. IEEE Int. Conf. Sensor Netw., Ubiquitous Trustworthy Comput. (SUTC)*, Jun. 2008, pp. 1–9.
[47] M. Rausand and H. Arnljot, *System Reliability Theory: Models, Statistical Methods, and Applications*, vol. 396. Hoboken, NJ, USA: Wiley, 2004.
[48] R. Mitchell and I. R. Chen, "Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems," *IEEE Trans. Rel.*, vol. 65, no. 1, pp. 350–358, Mar. 2016.
[49] X. Liu, W. He, and L. Zheng, "Transportation cyber-physical systems: Reliability modeling and analysis framework," in *Proc. Nat. Workshop Res. High-Confidence Transp. Cyber-Phys. Syst., Automot., Aviation Rail*, Washington, DC, USA, Nov. 2008, pp. 18–20. [Online]. Available: https://labs.ece.uw.edu/nsl/aar-cps/
[50] K. R. Davis, C. M. Davis, S. A. Zonouz, R. B. Bobba, R. Berthier, L. García, and P. W. Sauer, "A cyber-physical modeling and assessment framework for power grid infrastructures," *IEEE Trans. Smart Grid*, vol. 6, no. 5, pp. 2464–2475, Sep. 2015.
[51] M. Engel, F. Schmoll, A. Heinig, and P. Marwedel, "Unreliable yet useful-reliability annotations for data in cyber-physical systems," in *GI-Jahrestagung*, 2011, p. 334.
[52] W. Ahmad, O. Hasan, U. Pervez, and J. Qadir, "Reliability modeling and analysis of communication networks," *J. Netw. Comput. Appl.*, vol. 78, pp. 191–215, Jan. 2017.
[53] S. Bernardi, J. Merseguer, and D. C. Petriu, *Model-Driven Dependability Assessment of Software Systems*. New York, NY, USA: Springer, 2013.
[54] S. Fernandes, E. Tavares, M. Santos, V. Lira, and P. Maciel, "Dependability assessment of virtualized networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Jun. 2012, pp. 2711–2716.
[55] P. Weber, G. Medina-Oliva, C. Simon, and B. Iung, "Overview on Bayesian networks applications for dependability, risk analysis and maintenance areas," *Eng. Appl. Artif. Intell.*, vol. 25, no. 4, pp. 671–682, 2012.
[56] A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla, "Improving the analysis of dependable systems by mapping fault trees into Bayesian networks," *Rel. Eng. Syst. Saf.*, vol. 71, no. 3, pp. 249–260, 2001.
[57] L. Maddalena, A. Petrosino, and S. K. Pal, *Handbook on Soft Computing for Video Surveillance*. London, U.K.: Chapman & Hall, 2012.
[58] R. A. Aliev, B. Fazlollahi, and R. R. Aliev, *Soft Computing and its Applications in Business and Economics*, vol. 157. New York, NY, USA: Springer, 2012.
[59] E. Frias-Martinez, G. Magoulas, S. Chen, and R. Macredie, "Modeling human behavior in user-adaptive systems: Recent advances using soft computing techniques," *Expert Syst. Appl.*, vol. 29, no. 2, pp. 320–329, 2005.
[60] P. P. Bonissone, "Soft computing: The convergence of emerging reasoning technologies," *Soft Comput.*, vol. 1, no. 1, pp. 6–18, 1997.
[61] E. K. Juuso, "Integration of intelligent systems in development of smart adaptive systems," *Int. J. Approx. Reasoning*, vol. 35, no. 3, pp. 307–337, 2004.
[62] R. Bello and J. L. Verdegay, "Rough sets in the soft computing environment," *Inf. Sci.*, vol. 212, pp. 1–14, Dec. 2012.
[63] V. Ebrahimipour, S. M. Asadzadeh, and A. Azadeh, "An emotional learning-based fuzzy inference system for improvement of system reliability evaluation in redundancy allocation problem," *Int. J. Adv. Manuf. Technol.*, vol. 66, pp. 1657–1672, Jun. 2013.
[64] V. Ravi, P. J. Reddy, and H. J. Zimmermann, "Fuzzy global optimization of complex system reliability," *IEEE Trans. Fuzzy Syst.*, vol. 8, no. 3, pp. 241–248, Jun. 2000.
[65] L. A. Zadeh, "Some reflections on soft computing, granular computing and their roles in the conception, design and utilization of information/intelligent systems," *Soft Comput.*, vol. 2, no. 1, pp. 23–25, 1998.
[66] M. Negnevitsky, *Artificial Intelligence: A Guide to Intelligent Systems*. London, U.K.: Pearson, 2005.
[67] L. A. Zadeh, "Fuzzy sets as a basis for a theory of possibility," *Fuzzy Sets Syst.*, vol. 1, no. 1, pp. 3–28, 1978.
[68] A. Z. Keller and C. Kara-Zaitri, "Further applications of fuzzy logic to reliability assessment and safety analysis," *Microelectron. Rel.*, vol. 29, no. 3, pp. 399–404, 1989.
[69] C. Kai-Yuan, W. Chuan-Yuan, and Z. Ming-Lian, "Fuzzy variables as a basis for a theory of fuzzy reliability in the possibility context," *Fuzzy Sets Syst.*, vol. 42, no. 2, pp. 145–172, 1991.
[70] D. E. Goldberg, *Genetic Algorithms*. New Delhi, India: Pearson, 2006.
[71] X.-S. Yang and S. Deb, "Cuckoo search via Lévy flights," in *Proc. World Congr. Nature Biologically Inspired Comput. (NaBIC)*, Dec. 2009, pp. 210–214.
[72] P. Myllymäki, "Massively parallel probabilistic reasoning with Boltzmann machines," *Appl. Intell.*, vol. 11, no. 1, pp. 31–44, 1999.
[73] F. Glover, "Tabu search and adaptive memory programming—Advances, applications and challenges," in *Interfaces in Computer Science and Operations Research*. Boston, MA, USA: Springer, 1997, pp. 1–75.
[74] L. De Raedt and K. Kersting, "Probabilistic logic learning," *ACM SIGKDD Explor. Newslett.*, vol. 5, no. 1, pp. 31–48, 2003.
[75] L. He, C. W. Chan, G. H. Huang, and G. M. Zeng, "A probabilistic reasoning-based decision support system for selection of remediation technologies for petroleum-contaminated sites," *Expert Syst. Appl.*, vol. 30, no. 4, pp. 783–795, 2006.
[76] S. C. K. Shiu and S. K. Pal, "Case-based reasoning: Concepts, features and soft computing," *Appl. Intell.*, vol. 21, no. 3, pp. 233–238, 2004.
[77] R. Kindermann and J. L. Snell, *Markov Random Fields and Their Applications*. Providence, RI, USA: American Mathematical Society, 1980.
[78] M. Richardson and P. Domingos, "Markov logic networks," *Mach. Learn.*, vol. 62, no. 1, pp. 107–136, Feb. 2006.
[79] S. Huiling, M. Jun, and Z. Fengyi, "Software dependability evaluation model based on fuzzy theory," in *Proc. Int. Conf. Comput. Sci. Inf. Technol. (ICCSIT)*, Aug./Sep. 2008, pp. 102–106.
[80] A. N. Toosi and M. Kahani, "A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers," *Comput. Commun.*, vol. 30, no. 10, pp. 2201–2212, 2007.
[81] J. Knezevic and E. R. Odoom, "Reliability modelling of repairable systems using Petri nets and fuzzy Lambda–Tau methodology," *Rel. Eng. Syst. Saf.*, vol. 73, no. 1, pp. 1–17, 2001.
[82] G. S. Mahapatra and T. K. Roy, "Fuzzy multi-objective mathematical programming on reliability optimization model," *Appl. Math. Comput.*, vol. 174, no. 1, pp. 643–659, 2006.
[83] S.-B. Cho, "Incorporating soft computing techniques into a probabilistic intrusion detection system," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 32, no. 2, pp. 154–160, May 2002.
[84] A. K. Pandey and N. K. Goyal, "A fuzzy model for early software fault prediction using process maturity and software metrics," *Int. J. Electron. Eng.*, vol. 1, no. 2, pp. 239–245, 2009.
[85] K. Tyagi and A. Sharma, "An adaptive neuro fuzzy model for estimating the reliability of component-based software systems," *Appl. Comput. Inform.*, vol. 10, nos. 1–2, pp. 38–51, 2014.
[86] Z. Pawlak, *Rough Sets: Theoretical Aspects of Reasoning about Data*, vol. 9. Amsterdam, The Netherlands: Elsevier, 2012.
[87] Y. Y. Yao, "A comparative study of fuzzy sets and rough sets," *Inf. Sci.*, vol. 109, nos. 1–4, pp. 227–242, 1998.
[88] I. Düntsch and G. Gediga, *Rough Set Data Analysis: A Road to Non-Invasive Knowledge Discovery* (Methodos Primers), vol. 2. Bangor, U.K.: Methodos Publishers (UK), 2000. [Online]. Available: http://www.cosc.brocku.ca/~duentsch/archive/nida.pdf
[89] S. Rissino and G. Lambert-Torres, "Rough set theory—Fundamental concepts, principals, data extraction, and applications," in *Proc. Data Mining Knowl. Discovery Real Life Appl.*, vol. 438, 2009, pp. 36–58.
[90] Z. Pawlak, "Rough sets," *Int. J. Comput. Inf. Sci.*, vol. 11, no. 5, pp. 341–356, Oct. 1982.
[91] B. Li and Y. Cao, "An improved comprehensive evaluation model of software dependability based on rough set theory," *JSW*, vol. 4, no. 10, pp. 1152–1159, 2009.
[92] K.-Y. Cai, "Fuzzy methods in probist systems," in *Introduction to Fuzzy Reliability*. Boston, MA, USA: Springer, 1996, pp. 71–85.
[93] K.-Y. Cai, "System failure engineering and fuzzy methodology an introductory overview," *Fuzzy Sets Syst.*, vol. 83, no. 2, pp. 113–133, 1996.
[94] T. Onisawa, "An application of fuzzy concepts to modelling of reliability analysis," *Fuzzy Sets Syst.*, vol. 37, no. 3, pp. 267–286, 1990.
[95] A. Kaufmann and D. L. Swanson, *Introduction to the Theory of Fuzzy Subsets*, vol. 1. New York, NY, USA: Academic, 1975.
[96] G. S. Mahapatra, M. Mitra, and T. K. Roy, "Intuitionistic fuzzy multi-objective mathematical programming on reliability optimization model," *Int. J. Fuzzy Syst.*, vol. 12, no. 3, pp. 259–266, 2010.
[97] H.-Z. Huang, M. J. Zuo, and Z.-Q. Sun, "Bayesian reliability analysis for fuzzy lifetime data," *Fuzzy Sets Syst.*, vol. 157, no. 12, pp. 1674–1686, 2006.

[98] L. Lin and M. Gen, "A self-controlled genetic algorithm for reliable communication network design," in *Proc. IEEE Congr. Evol. Comput. (CEC)*, Jul. 2006, pp. 640–647.

[99] K. Echtle and I. Eusgeld, "A genetic algorithm for fault-tolerant system design," in *Latin-American Symposium on Dependable Computing*. Berlin, Germany: Springer, 2003, pp. 197–213.

[100] D. W. Coit and A. E. Smith, "Reliability optimization of series-parallel systems using a genetic algorithm," *IEEE Trans. Rel.*, vol. 45, no. 2, pp. 254–260, Jun. 1996.

[101] C. M. F. Lapa, C. M. N. A. Pereira, and M. P. de Barros, "A model for preventive maintenance planning by genetic algorithms based in cost and reliability," *Rel. Eng. Syst. Saf.*, vol. 91, no. 2, pp. 233–240, 2006.

[102] D.-L. Duan, X.-D. Ling, X.-Y. Wu, and B. Zhong, "Reconfiguration of distribution network for loss reduction and reliability improvement based on an enhanced genetic algorithm," *Int. J. Elect. Power Energy Syst.*, vol. 64, pp. 88–95, Jan. 2015.

[103] L. Tian and A. Noore, "On-line prediction of software reliability using an evolutionary connectionist model," *J. Syst. Softw.*, vol. 77, no. 2, pp. 173–180, 2005.

[104] L. Tian and A. Noore, "Evolutionary neural network modeling for software cumulative failure time prediction," *Rel. Eng. Syst. Saf.*, vol. 87, no. 1, pp. 45–51, 2005.

[105] R. Zhao and B. Liu, "Stochastic programming models for general redundancy-optimization problems," *IEEE Trans. Rel.*, vol. 52, no. 2, pp. 181–191, Jun. 2003.

[106] S. H. Aljahdali and M. E. El-Telbany, "Software reliability prediction using multi-objective genetic algorithm," in *Proc. IEEE/ACS Int. Conf. Comput. Syst. Appl. (AICCSA)*, May 2009, pp. 293–300.

[107] M. Elkoujok, M. Benammar, N. Meskin, M. Al-Naemi, and R. Langari, "Application of genetic algorithm in selection of dominant input variables in sensor fault diagnosis of nonlinear systems," in *Proc. IEEE Conf. Prognostics Health Manage. (PHM)*, Jun. 2013, pp. 1–7.

[108] P. Mitra and G. K. Venayagamoorthy, "Real-time implementation of an intelligent algorithm for electric ship power system reconfiguration," in *Proc. IEEE Electr. Ship Technol. Symp. (ESTS)*, Apr. 2009, pp. 219–226.

[109] D. G. Robinson, "Reliability analysis of bulk power systems using swarm intelligence," in *Proc. Annu. Rel. Maintainability Symp.*, Jan. 2005, pp. 96–102.

[110] Z. A. Bashir and M. E. El-Hawary, "Applying wavelets to short-term load forecasting using PSO-based neural networks," *IEEE Trans. Power Syst.*, vol. 24, no. 1, pp. 20–27, Feb. 2009.

[111] Y.-C. Liang and A. E. Smith, "An ant colony optimization algorithm for the redundancy allocation problem (RAP)," *IEEE Trans. Rel.*, vol. 53, no. 3, pp. 417–423, Sep. 2004.

[112] J. H. Zhao, Z. Liu, and M. T. Daoa, "Reliability optimization using multiobjective ant colony system approaches," *Rel. Eng. Syst. Saf.*, vol. 92, pp. 109–120, 2017.

[113] M. Caserta and A. M. Uribe, "Tabu search-based metaheuristic algorithm for software system reliability problems," *Comput. Oper. Res.*, vol. 36, no. 3, pp. 811–822, 2009.

[114] S. Kulturel-Konak, A. E. Smith, and D. W. Coit, "Efficiently solving the redundancy allocation problem using tabu search," *IIE Trans.*, vol. 35, no. 6, pp. 515–526, 2003.

[115] I. J. Ramírez-Rosado and J. A. Domínguez-Navarro, "New multiobjective tabu search algorithm for fuzzy optimal planning of power distribution systems," *IEEE Trans. Power Syst.*, vol. 21, no. 1, pp. 224–233, Feb. 2006.

[116] S. Pierre and A. Elgibaoui, "A tabu-search approach for designing computer-network topologies with unreliable components," *IEEE Trans. Rel.*, vol. 46, no. 3, pp. 350–359, Sep. 1997.

[117] E. Valian, S. Tavakoli, S. Mohanna, and A. Haghi, "Improved cuckoo search for reliability optimization problems," *Comput. Ind. Eng.*, vol. 64, no. 1, pp. 459–468, 2013.

[118] A. Teske, R. Falcon, and A. Nayak, "Efficient detection of faulty nodes with cuckoo search in t-diagnosable systems," *Appl. Soft Comput.*, vol. 29, pp. 52–64, Apr. 2015.

[119] P.-F. Pai and W.-C. Hong, "Software reliability forecasting by support vector machines with simulated annealing algorithms," *J. Syst. Softw.*, vol. 79, no. 6, pp. 747–755, 2006.

[120] G. Attiya and Y. Hamam, "Task allocation for maximizing reliability of distributed systems: A simulated annealing approach," *J. Parallel Distrib. Comput.*, vol. 66, no. 10, pp. 1259–1266, 2006.

[121] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, to be published.

[122] H. Peng, Z. Kan, D. Zhao, J. Han, J. Lu, and Z. Hu, "Reliability analysis in interdependent smart grid systems," *Phys. A, Stat. Mech. Appl.*, vol. 500, pp. 50–59, Jun. 2018.

[123] Z. Ni and S. Paul, "A multistage game in smart grid security: A reinforcement learning solution," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published.

[124] P. M. Shakeel, S. Baskar, V. R. S. Dhulipala, S. Mishra, and M. M. Jaber, "Maintaining security and privacy in health care system using learning based deep-Q-networks," *J. Med. Syst.*, vol. 42, no. 10, p. 186, 2018.

[125] A. Ferdowsi, U. Challita, W. Saad, and N. B. Mandayam, "Robust deep reinforcement learning for security and safety in autonomous vehicle systems," in *Proc. 21st Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2018, pp. 307–312.

[126] M.-J. Kang and J.-W. Kang, "Intrusion detection system using deep neural network for in-vehicle network security," *PLoS ONE*, vol. 11, no. 6, 2016, Art. no. e0155781.

[127] F. Altiparmak, B. Dengiz, and A. E. Smith, "A general neural network model for estimating telecommunications network reliability," *IEEE Trans. Rel.*, vol. 58, no. 1, pp. 2–9, Mar. 2009.

[128] K.-Y. Cai, L. Cai, W.-D. Wang, Z.-Y. Yu, and D. Zhang, "On the neural network approach in software reliability modeling," *J. Syst. Softw.*, vol. 58, no. 1, pp. 47–62, 2001.

[129] Y.-S. Su, C.-Y. Huang, Y.-S. Chen, and J.-X. Chen, "An artificial neural-network-based approach to software reliability assessment," in *Proc. IEEE Region 10 Conf. TENCON*, Nov. 2005, pp. 1–6.

[130] Q. P. Hu, Y. S. Dai, M. Xie, and S. H. Ng, "Early software reliability prediction with extended ANN model," in *Proc. 30th Annu. Int. Comput. Softw. Appl. Conf. (COMPSAC)*, vol. 2, Sep. 2006, pp. 234–239.

[131] Q. P. Hu, M. Xie, S. H. Ng, and G. Levitin, "Robust recurrent neural network modeling for software fault detection and correction prediction," *Rel. Eng. Syst. Saf.*, vol. 92, no. 3, pp. 332–340, 2007.

[132] C. Srivaree-Ratana, A. Konak, and A. E. Smith, "Estimation of all-terminal network reliability using an artificial neural network," *Comput. Oper. Res.*, vol. 29, no. 7, pp. 849–868, 2002.

[133] P. Bhowmik, P. Purkait, and K. Bhattacharya, "A novel wavelet transform aided neural network based transmission line fault analysis method," *Int. J. Elect. Power Energy Syst.*, vol. 31, no. 5, pp. 213–219, 2009.

[134] J. J. Mora, G. Carrillo, and L. Perez, "Fault location in power distribution systems using ANFIS nets and current patterns," in *Proc. IEEE/PES Transmiss. Distrib. Conf. Expo., Latin Amer. (TDC)*, Aug. 2006, pp. 1–6.

[135] H.-T. Zhang, F.-Y. Xu, and L. Zhou, "Artificial neural network for load forecasting in smart grid," in *Proc. Int. Conf. Mach. Learn. (ICMLC)*, vol. 6, Jul. 2010, pp. 3200–3205.

[136] W. Gao, T. Morris, B. Reaves, and D. Richey, "On SCADA control system command and response injection and intrusion detection," in *Proc. eCrime Researchers Summit (eCrime)*, Oct. 2010, pp. 1–9.

[137] O. Linda, T. Vollmer, and M. Manic, "Neural network based intrusion detection system for critical infrastructures," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jun. 2009, pp. 1827–1834.

[138] J. M. Moya, A. Araujo, Z. Banković, J.-M. De Goyeneche, J. C. Vallejo, P. Malagón, D. Villanueva, D. Fraga, E. Romero, and J. Blesa, "Improving security for SCADA sensor networks with reputation systems and self-organizing maps," *Sensors*, vol. 9, no. 11, pp. 9380–9397, 2009.

[139] J. Goh, S. Adepu, M. Tan, and Z. S. Lee, "Anomaly detection in cyber physical systems using recurrent neural networks," in *Proc. IEEE 18th Int. Symp. High Assurance Syst. Eng. (HASE)*, Jan. 2017, pp. 140–145.

[140] Z. Wu, Y. Guo, W. Lin, S. Yu, and Y. Ji, "A weighted deep representation learning model for imbalanced fault diagnosis in cyber-physical systems," *Sensors*, vol. 18, no. 4, p. 1096, 2018.

[141] A. Munoz, S. Martorell, and V. Serradell, "Genetic algorithms in optimizing surveillance and maintenance of components," *Rel. Eng. Syst. Saf.*, vol. 57, no. 2, pp. 107–120, 1997.

[142] J.-E. Yang, T.-Y. Sung, and Y. Jin, "Optimization of the surveillance test interval of the safety systems at the plant level," *Nucl. Technol.*, vol. 132, no. 3, pp. 352–365, 2000.

[143] C. M. F. Lapa, C. Pereira, and P. F. F. F. e Melo, "An application of genetic algorithms to surveillance test optimization of a PWR auxiliary feedwater system," *Int. J. Intell. Syst.*, vol. 17, no. 8, pp. 813–831, 2002.

[144] C. M. F. Lapa, C. Pereira, and P. F. F. F. e Melo, "Surveillance test policy optimization through genetic algorithms using non-periodic intervention frequencies and considering seasonal constraints," *Rel. Eng. Syst. Saf.*, vol. 81, no. 1, pp. 103–109, 2003.

[145] D. W. Coit and A. E. Smith, "Use of a genetic algorithm to optimize a combinatorial reliability design problem," in *Proc. 3rd IIE Res. Conf.*, 1994, pp. 467–472.

[146] Y.-C. Hsieh, T.-C. Chen, and D. L. Bricker, "Genetic algorithms for reliability design problems," *Microelectron. Rel.*, vol. 38, no. 10, pp. 1599–1605, 1998.

[147] M. Dorigo and G. Di Caro, "Ant colony optimization: A new meta-heuristic," in *Proc. Congr. Evol. Comput. (CEC)*, vol. 2, Jul. 1999, pp. 1470–1477.

[148] S. Kirkpatrick, C. D. Gelatt, and M. P. Vecchi, "Optimization by simulated annealing," *Science*, vol. 220, no. 4598, pp. 671–680, 1983.

[149] V. Ravi, B. S. N. Murty, and J. Reddy, "Nonequilibrium simulated-annealing algorithm applied to reliability optimization of complex systems," *IEEE Trans. Rel.*, vol. 46, no. 2, pp. 233–239, Jun. 1997.

[150] Y.-J. Jeon, J.-C. Kim, J.-O. Kim, J.-R. Shin, and K. Y. Lee, "An efficient simulated annealing algorithm for network reconfiguration in large-scale distribution systems," *IEEE Trans. Power Del.*, vol. 17, no. 4, pp. 1070–1078, Oct. 2002.

[151] W. Fushuan and H. Zhenxiang, "Fault section estimation in power systems using genetic algorithm and simulated annealing," *Chin. Soc. Elect. Eng.*, vol. 3, 1994.

[152] P. Weber and L. Jouffe, "Complex system reliability modelling with dynamic object oriented Bayesian networks (DOOBN)," *Rel. Eng. Syst. Saf.*, vol. 91, no. 2, pp. 149–162, 2006.

[153] G. Weidl, A. L. Madsen, and S. Israelson, "Applications of object-oriented Bayesian networks for condition monitoring, root cause analysis and decision support on operation of complex continuous processes," *Comput. Chem. Eng.*, vol. 29, no. 9, pp. 1996–2009, 2005.

[154] K. R. McNaught and A. Zagorecki, "Using dynamic Bayesian networks for prognostic modelling to inform maintenance decision making," in *Proc. IEEE Int. Conf. Ind. Eng. Eng. Manage. (IEEM)*, Dec. 2009, pp. 1155–1159.

[155] P. Wang, B. D. Youn, Z. Xi, and A. Kloess, "Bayesian reliability analysis with evolving, insufficient, and subjective data sets," *J. Mech. Des.*, vol. 131, no. 11, 2009, Art. no. 111008.

[156] G. Liu and C. Ji, "Scalability of network-failure resilience: Analysis using multi-layer probabilistic graphical models," *IEEE/ACM Trans. Netw.*, vol. 17, no. 1, pp. 319–331, Feb. 2009.

[157] C. Queiroz, S. K. Garg, and Z. Tari, "A probabilistic model for quantifying the resilience of networked systems," *IBM J. Res. Develop.*, vol. 57, no. 5, pp. 3:1–3:9, 2013.

[158] K. C. Lalropuia and V. Gupta, "Modeling cyber-physical attacks based on stochastic game and Markov processes," *Rel. Eng. Syst. Saf.*, vol. 181, pp. 28–37, Jan. 2019.

[159] Y. Singh and P. B. Kumar, "Application of feed-forward neural networks for software reliability prediction," *ACM SIGSOFT Softw. Eng. Notes*, vol. 35, no. 5, pp. 1–6, 2010.

[160] C. Lee, M. Gen, and Y. Tsujimura, "Reliability optimization design using hybrid NN-GA with fuzzy logic controller," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. 85, no. 2, pp. 432–446, 2002.

[161] Y. He, G. J. Mendis, and J. Wei, "Real-time detection of false data injection attacks in smart grid: A deep learning-based intelligent mechanism," *IEEE Trans. Smart Grid.*, vol. 8, no. 5, pp. 2505–2516, Sep. 2017.

[162] P. Malhotra, L. Vig, G. Shroff, and P. Agarwal, "Long short term memory networks for anomaly detection in time series," in *Proc. Presses Universitaires de Louvain*, 2015, p. 89.

[163] J. Shin, Y. Baek, Y. Eun, and S. H. Son, "Intelligent sensor attack detection and identification for automotive cyber-physical systems," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Nov./Dec. 2017, pp. 1–8.

[164] C. Feng, T. Li, and D. Chana, "Multi-level anomaly detection in industrial control systems via package signatures and LSTM networks," in *Proc. 47th Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 261–272.

[165] A. Saied, R. E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using artificial neural networks," *Neurocomputing*, vol. 172, pp. 385–393, Jan. 2016.

[166] H. Niu, C. Bhowmick, and S. Jagannathan, "Attack detection and approximation in nonlinear networked control systems using neural networks," *IEEE Trans. Neural Netw. Learn. Syst.*, to be published.

[167] A.-H. Muna, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial Internet of Things based on deep learning models," *J. Inf. Secur. Appl.*, vol. 41, pp. 1–11, Aug. 2018.

[168] J. T. Peng, C. F. Chien, and T. L. B. Tseng, "Rough set theory for data mining for fault diagnosis on distribution feeder," *IEE Proc.-Gener., Transmiss. Distrib.*, vol. 151, no. 6, pp. 689–697, Nov. 2004.

[169] H.-S. Su and Q.-Z. Li, "Substation fault diagnosis method based on rough set theory and neural network model," *Power Syst. Technol.*, vol. 16, pp. 66–70, Aug. 2005.

[170] I. E. Chen-Jimenez, A. Kornecki, and J. Zalewski, "Software safety analysis using rough sets," in *Proc. Southeastcon*, Apr. 1998, pp. 15–19.

[171] J.-M. Yuan, C.-Z. Hou, L. Gao, and X.-Y. Wang, "Rough Petri net and its application in multi-state system reliability estimate," *Acta Armamentarii*, vol. 11, p. 019, Nov. 2007.

[172] Q. H. Wang and J. R. Li, "A rough set-based fault ranking prototype system for fault diagnosis," *Eng. Appl. Artif. Intell.*, vol. 17, no. 8, pp. 909–917, 2004.

[173] C. Joslyn, "Multi-interval elicitation of random intervals for engineering reliability analysis," in *Proc. 4th Int. Symp. Uncertainty Modeling Anal. (ISUMA)*, Sep. 2003, pp. 168–173.

[174] W. Song, X. Ming, Z. Wu, and B. Zhu, "A rough TOPSIS approach for failure mode and effects analysis in uncertain environments," *Qual. Rel. Eng. Int.*, vol. 30, no. 4, pp. 473–486, 2014.

[175] A. D. Gordon, T. A. Henzinger, A. V. Nori, and S. K. Rajamani, "Probabilistic programming," in *Proc. Future Softw. Eng.*, 2014, pp. 167–181.

[176] H. Langseth, *Bayesian Networks in Reliability: The Good, the Bad, and the Ugly* (Advances in Mathematical Modeling for Reliability), vol. 1. Amsterdam, The Netherlands: IOS Press, 2008.

[177] H. Boudali and J. B. Duga, "A new Bayesian network approach to solve dynamic fault trees," in *Proc. Annu. Rel. Maintainability Symp.*, Jan. 2005, pp. 451–456.

[178] S. Montani, L. Portinale, A. Bobbio, and D. Codetta-Raiteri, "Radyban: A tool for reliability analysis of dynamic fault trees through conversion into dynamic Bayesian networks," *Rel. Eng. Syst. Saf.*, vol. 93, no. 7, pp. 922–932, Jul. 2008.

[179] H. Boudali and J. B. Dugan, "A discrete-time Bayesian network reliability modeling and analysis framework," *Rel. Eng. Syst. Saf.*, vol. 87, no. 3, pp. 337–349, 2005.

[180] Y.-C. Chen, T. Gieseking, D. Campbell, V. Mooney, and S. Grijalva, "A hybrid attack model for cyber-physical security assessment in electricity grid," in *Proc. IEEE Texas Power Energy Conf. (TPEC)*, Feb. 2019, pp. 1–6.

[181] Z. Qiu, D. Yang, and I. Elishakoff, "Probabilistic interval reliability of structural systems," *Int. J. Solids Struct.*, vol. 45, no. 10, pp. 2850–2860, 2008.

[182] L. Cui, S. Du, and B. Liu, "Multi-point and multi-interval availabilities," *IEEE Trans. Rel.*, vol. 62, no. 4, pp. 811–820, Dec. 2013.

[183] K. Wan, K. L. Man, and D. Hughes, "Specification, analyzing challenges and approaches for cyber-physical systems (CPS)," *Eng. Lett.*, vol. 18, no. 3, pp. 1–8, 2010.

[184] M. García-Valls, C. Calva-Urrego, J. A. de la Puenteand, and A. Alonso, "Adjusting middleware knobs to assess scalability limits of distributed cyber-physical systems," *Comput. Standards Interfaces*, vol. 51, pp. 95–103, Mar. 2017.

[185] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems.," in *Proc. HotSec*, 2008, Art. no. 6.

[186] Y. Yang, S. Wang, M. Wen, and W. Xu, "Reliability modeling and evaluation of cyber-physical system (CPS) considering communication failures," *J. Franklin Inst.*, Sep. 2018.

[187] Z. Fang, H. Mo, Y. Wang, and M. Xie, "Performance and reliability improvement of cyber-physical systems subject to degraded communication networks through robust optimization," *Comput. Ind. Eng.*, vol. 114, pp. 166–174, Dec. 2017.

[188] G. C. Walsh, H. Ye, and L. G. Bushnell, "Stability analysis of networked control systems," *IEEE Trans. Control Syst. Technol.*, vol. 10, no. 3, pp. 438–446, May 2002.

[189] X. Li and C. E. De Souza, "Criteria for robust stability and stabilization of uncertain linear systems with state delay," *Automatica*, vol. 33, no. 9, pp. 1657–1662, 1997.

[190] L. Zhang, H. Gao, and O. Kaynak, "Network-induced constraints in networked control systems—A survey," *IEEE Trans Ind. Informat.*, vol. 9, no. 1, pp. 403–416, Feb. 2013.

[191] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems," *Annu. Rev. Control*, vol. 32, no. 2, pp. 229–252, 2008.

[192] M. Blanke, R. Izadi-Zamanabadi, S. A. Bøgh, and C. P. Lunau, "Fault-tolerant control systems—A holistic view," *Control Eng. Pract.*, vol. 5, no. 5, pp. 693–702, 1997.

[193] J. Chen, X. Cao, P. Cheng, Y. Xiao, and Y. Sun, "Distributed collaborative control for industrial automation with wireless sensor and actuator networks," *IEEE Trans. Ind. Electron.*, vol. 57, no. 12, pp. 4219–4230, Dec. 2010.

[194] A. K. Tyagi, "Cyber physical systems (CPSS)—Opportunities and challenges for improving cyber security," *Int. J. Comput. Appl.*, vol. 137, no. 14, 2016.

MUHAMMAD ATIF received the bachelor's degree in electrical engineering from the National University of Sciences and Technology (NUST), Pakistan. He is currently working on his M.S. thesis at the School of Electrical Engineering (SEECS), NUST. He has worked in the industry on embedded systems design and in data networks. His research interests include the Internet of Things (IoT) and machine learning.

SIDDIQUE LATIF received the M.S. degree in electrical engineering from the National University of Sciences and Technology, Islamabad, Pakistan, in 2018. He is currently pursuing the Ph.D. degree with the University of Southern Queensland (USQ), Australia. He was a Research Associate with the IHSAN Lab, Information Technology University, Lahore, Pakistan. His research interests include deep machine learning, signal processing, and healthcare.

RIZWAN AHMAD received the M.Sc. degree in communication engineering and media technology from the University of Stuttgart, Stuttgart, Germany, in 2004, and the Ph.D. degree in electrical engineering from Victoria University, Melbourne, VIC, Australia, in 2010. From 2010 to 2012, he was a Postdoctoral Research Fellow with Qatar University under the support of a QNRF grant. He is currently an Assistant Professor with the School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Pakistan. He also leads the Communication Systems and Networking (CSN) Research Group at NUST. His research interests include medium access control protocols, spectrum and energy efficiency, energy harvesting, and performance analysis for wireless communication and networks. He has published and has served as a Reviewer for IEEE journals and conferences. He was a recipient of the prestigious International Postgraduate Research Scholarship from the Australian Government. He serves on the TPC of leading conferences in the communication and networking field, including the IEEE VTC, the IEEE ICC, and the IEEE Globecom.

ADNAN K. KIANI received the M.Sc. and Ph.D. degrees from Brunel University, U.K., in 2005 and 2009, respectively. He is currently a Lecturer (Assistant Professor) with London South Bank University. He is also with the National University of Sciences and Technology, Pakistan. His research interests include network communications, looking at topics ranging from infrastructure-less routing to network virtualization, and medium access control issues. He serves as a Reviewer for a number of prominent journals and conferences, including *Telecommunication Systems* - Springer, the IEEE INTERNET OF THINGS, the IEEE VTC, the IEEE WCNC, and the IEEE IWCMC.

JUNAID QADIR received the bachelor's degree in electrical engineering from the University of Engineering and Technology, Lahore, Pakistan, in 2000, and the Ph.D. degree from the University of New South Wales, Australia, in 2008. He is an Associate Professor with the Information Technology University (ITU)—Punjab, Lahore, since 2015, where he directs the ICTD, Human Development, Systems, Big Data Analytics, Networks (IHSAN) Research Lab. His primary research interests include computer systems and networking, applied machine learning, and using ICT for development (ICT4D). He is the author of more than 100 peer-reviewed research papers that have been published at various top conferences and journals. He is a member of ACM.

ADEEL BAIG (M'07–SM'14) received the B.E. degree from the NED University of Engineering and Technology, Karachi, Pakistan, and the M.Eng.Sc. and Ph.D. degrees in computer science and engineering from the University of New South Wales (UNSW), Australia. He is currently an Assistant Professor with the College of Engineering and Architecture, Al-Yamamah University, Saudi Arabia. He is also with the School of Electrical Engineering and Computer Science, National University of Sciences and Technology (NUST), Pakistan. His research interests include cognitive and mobile networks, cross-layer optimization for wireless networks, and IPv6 deployments and transition issues. He has been a member of technical program committees of several local/international conferences. He is also a member of the ACM, PEC, and ISOC.

HISAO ISHIBUCHI (M'93–SM'10–F'14) received the B.S. and M.S. degrees in precision mechanics from Kyoto University, Kyoto, Japan, in 1985 and 1987, respectively, and the Ph.D. degree in computer science from Osaka Prefecture University, Osaka, Japan, in 1992. He was with Osaka Prefecture University, from 1987 to 2017. Since 2017, he has been a Chair Professor with the Southern University of Science and Technology, China. His research interests include fuzzy rule-based classifiers, evolutionary multi-objective and many-objective optimization, memetic algorithms, and evolutionary games. He was the Vice-President for Technical Activities, IEEE Computational Intelligence Society (CIS), from 2010 to 2013. He is currently an AdCom Member of the IEEE CIS (2014–2019) and the Editor-in-Chief of the *IEEE Computational Intelligence Magazine* (2014–2019).

WASEEM ABBAS received the M.Sc. and Ph.D. degrees in electrical and computer engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2010 and 2013, respectively. He is currently an Assistant Professor with the Department of Electrical Engineering, Information Technology University, Lahore, Pakistan. Prior to that, he was a Postdoctoral Research Scholar with Vanderbilt University, Nashville, TN, USA. His research interests include network control systems, graph-theoretic methods for large networked systems, and resilience of cyber-physical systems.