Received October 16, 2017, accepted November 11, 2017, date of publication November 24, 2017,
date of current version December 22, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2777438

Trustworthiness Modeling and Analysis of Cyber-physical Manufacturing Systems

ZHENHUA YU[1], LIJUN ZHOU[2], ZHIQIANG MA[1], AND MOHAMMED A. EL-MELIGY[3]

[1]School of Information and Navigation, Air Force Engineering University, Xi'an 710077, China
[2]Xi'an Institute of Applied Optics, Xi'an 710065, China
[3]Advanced Manufacturing Institute, King Saud University, Riyadh 12372, Saudi Arabia

Corresponding author: Zhenhua Yu (zhenhua_yu@163.com)

This work was supported by the National Natural Science Foundation of China under Grant 61202128 and Grant 71571190.

ABSTRACT Cyber-physical manufacturing systems (CPMSs) are a new paradigm of manufacturing systems that integrate cyber systems and physical systems to aid smart manufacturing. CPMSs can improve the system's flexibility and productivity and adapt to new market demands. However, CPMSs are susceptible to cyber-attacks, which can modify manufacturing intents to produce parts incorrectly and cause hazards to equipment, employees, and consumers. Therefore, the trustworthiness of CPMSs is critical to the entire systems. In order to describe and analyze the trustworthiness of CPMSs, generalized stochastic Petri nets are adopted to model CPMSs and the trustworthiness is measured from three metrics, i.e., the reliability, availability and security. To study the trustworthiness evolution of CPMSs, a malicious software spreading dynamics model is presented, and its dynamic behaviors are analyzed. Finally, the CPMS trustworthiness evolution model is constructed depending on the proposed dynamics model. The simulation results demonstrate that the proposed approach is effective to model and analyze the CPMS trustworthiness.

INDEX TERMS Cyber-attack, cyber-physical systems, generalized stochastic Petri net, manufacturing systems, trustworthiness.

I. INTRODUCTION

Cyber-Physical systems (CPSs) represent a new generation of intelligent engineering systems [1], where computation processes and physical processes are integrated towards a set of common goals. Computation processes monitor and control physical processes via communication networks, while physical processes affect computation processes and vice versa [2]. CPSs are complex engineered systems with computation, communication and control capabilities. The ultimate aim of CPSs is to construct controllable, dependable, extendable, efficient and real-time systems. CPSs can change every aspect of our life and have been applied to many different fields, including weapon systems, intelligent transportation systems, avionics, smart manufacturing systems, industrial process control, nuclear power plants, smart grid, and medical devices [3]–[5].

With the development of computer science, information and communication technology and manufacturing science and technology, many types of manufacturing systems have emerged, such as the assembly line, computer integrated manufacturing systems, flexible manufacturing systems, reconfigurable manufacturing systems, distributed manufacturing systems, and cloud-based manufacturing [6]. In order to further improve the flexibility and productivity of manufacturing systems so that they can meet market demands, a new technology paradigm should be applied to manufacturing systems. CPSs are expected to tackle the challenges in the design and development of future manufacturing systems, as they can connect seamlessly cyber and physical components, enhance the interactions among machines, sensors and information systems, and improve the autonomy, reliability, agility and responsiveness of future manufacturing systems. Therefore CPSs are introduced into manufacturing systems [7] and then cyber-physical manufacturing systems (CPMSs) are formed.

In recent years, CPMSs have become a hot research topic in the field of manufacturing systems [8]. CPMSs include cyber parts and physical parts. Cyber parts are composed of computer aided engineering (CAE) tools, material requirements planning (MRP) systems, quality control/inspection reporting systems, communication systems, enterprise resource planning systems and supervisory control and data acquisition systems. Cyber parts acquire data using radio-frequency identification devices/sensors/measurement devices deployed on manufacturing entities [9], and transmit the data to the corresponding computing systems through communication systems. The computing systems save, process and analyze the data to make decisions to control the actions of machines and achieve high quality products. Physical parts are composed of different kinds of machines, industrial robots, materials, automatic guided vehicles (AGVs), etc. CPMSs deal with the actual operations in the physical parts while simultaneously monitor and control them in the cyber parts. As CPMSs make manufacturing systems more flexible to adapt to new market demands, they have been increasingly adopted by academy and industry. Driven by CPMSs, they will lead today's factories into Industry 4.0 factories, which integrate all involved resources into smart, self-organized and autonomous systems to aid smart manufacturing [7].

CPMSs are typical distributed systems where physical entities and different kinds of services can be accessed through communication networks, which increase the chances of cyber-attacks against systems. CPMSs are becoming susceptible to cyber-attacks [10], which may pose a significant threat to the product quality and equipment safety. In addition, some malicious software may modify anti-virus software or quality control systems to prevent the detection of malicious attacks [11]. Therefore CPMSs must be trustworthy, and they should perform their operations as expected, under a variety of hostile attacks, environmental disruptions and human and operator errors [4]. To address cyber-attacks, it is crucial to model and analyze the trustworthiness of CPMSs and investigate the trustworthiness evolution when malicious software penetrates CPMSs.

Trustworthiness means CPMSs will perform as expected although cyber-attacks occur. Trustworthiness and dependability are essentially equivalent in their goals and address similar threats [12]. Trustworthiness is a composite of reliability, availability, safety, integrity, maintainability, etc. As CPMSs bear no disruptions, trustworthiness should also include security. Therefore, we evaluate the CPMS trustworthiness from three metrics, i.e., reliability, availability and security, which are CPMS design goals. In this paper, we use generalized stochastic Petri nets (GSPNs) to specify CPMSs and analyze CPMS trustworthiness. To study the trustworthiness evolution of CPMSs at run-time, we describe the malicious software spreading mechanism in CPMSs and analyze its dynamic behaviors based on the stability theorem, and then the trustworthiness evolution model of CPMSs is presented.

II. RELATED WORK

CPSs make applications more faster, highly efficient, autonomous and precise, consequently there is an extraordinary significance for the future of CPS applications. Smart grids are a new paradigm for energy supply and are typical CPSs, which employ computing, communication and control technologies to deliver secure, efficient, effective and reliable energy supply and improve operation efficiency for generators and distributors [13]. Smart grids regard the power network infrastructure as physical systems, sensing, transmitting, processing, fusion and control as cyber systems, and seamlessly integrate the cyber systems with the physical systems. They exhibit typical characteristics of CPSs, such as self-adaption, self-organization and self-learning. Smart grids also require six key functionalities, namely, high dependability, high reliability, high predictability, high sustainability, high security and high interoperability.

Medical devices have become distributed systems that simultaneously monitor and control multiple aspects of the patient's physiology. Modern medical device systems integrate embedded software, physical devices and networks. They can be regarded as typical cyber-physical systems, which are called medical cyber-physical systems (MCPSs) [14]. MCPSs have been applied in hospitals to provide high-quality continuous care for patients. CPSs can also be employed to model implantable cardiac medical devices [5]. Sztipanovits *et al.* [15] present some challenges in modeling and verifying complex CPSs in the design phase, and layer decoupling approaches are employed to develop unmanned aerial vehicles. CPS applications in both automobile sectors and aviation are discussed in the high-confidence transportation CPS workshop [16].

In recent years, German government has proposed the term Industry 4.0 that can be regarded as the 4th industrial revolution [7]. Industry 4.0 is driven by CPSs and Internet of things. CPSs can bridge the gaps among isolated devices and have promising potential applications in manufacturing. Through CPSs, we can monitor manufacturing systems in real time and acquire the real-time data from the physical world. We transmit the data to the cyber world to save, process and make decisions. CPSs improve the flexibility of manufacturing systems to meet new market demands.

Esmaeilian *et al.* [17] review the manufacturing and remanufacturing related work, and discuss the definitions of manufacturing, classifications and taxonomies in manufacturing systems, technologies and engineering aspects, and new manufacturing paradigms. The advanced manufacturing paradigms originated from data analytics consist of sustainable manufacturing, smart manufacturing, social manufacturing, nano-manufacturing, semiconductor manufacturing, additive manufacturing and cloud manufacturing. Manufacturing based on CPSs is one of the new manufacturing paradigms, which can employ prediction tools to process data and make real-time decisions. Data security is very important for manufacturing based on CPSs and requires further research.

Lee *et al.* [18] propose a cyber-physical system architecture for Industry 4.0 manufacturing systems that guides manufacturing industry with more intelligent and resilient manufacturing equipment to make better products. Lee *et al.* [19] present the cyber manufacturing that translates industrial big data from interconnected systems into predictive and prescriptive operations to make decisions to achieve the resilient performance. The cyber-physical interfaces are important for cyber security in cyber manufacturing, and a fundamental framework for cyber manufacturing systems is proposed. Jeschke *et al.* [20] propose modeling and architectural design patterns for cyber manufacturing systems, and point out that cyber manufacturing systems are advanced mechatronic production systems and their intelligence is improved by the industrial Internet of things. Wang *et al.* [8] review the current status and the latest advancement of CPSs in manufacuring. They discuss the definitions and characteristics of CPSs and Industry 4.0. CPSs provide supporting methods and tools to cost-efficiently design and develop the future manufacturing systems. Some examples of CPSs in manufacturing are illustrated.

Song *et al.* [21] propose a service-oriented manufacturing cyber-physical system that aims to provide high-quality products for customers. Babiceanua and Seker [10] propose manufacturing cyber-physical systems (M-CPS) that process operations in the physical world and monitor them in the cyber world, and review the use of big data analytics for planning and control operations in M-CPS. As M-CPS operations are close to the cloud manufacturing paradigm, cyber attacks may occur. The cyber-physical devices in M-CPS are potential access points for intruders perpetuating to the entire systems. Cyber threats may attack on sensors, actuators, communication networks, maintenance mechanisms and physical equipment. To make M-CPS become a reality in real world manufacturing systems, the modeling guidelines for developing M-CPS are presented. Liu and Jiang [9] present a CPS architecture for the shop floor to make manufacturing systems more intelligent. The proposed architecture guides developers to construct a CPMS from physical parts and cyber parts. A small-scale flexible automated production line is studied based on the proposed CPS architecture. Putnik *et al.* [22] study the design and operation scalability in manufacturing systems. CPSs are introduced to improve the scalability to meet challenges of manufacturing systems. Jiang *et al.* [23] introduce CPSs and social media into manufacturing industry, and present a new social manufacturing paradigm.

Computer integrated manufacturing, distributed manufacturing, agile manufacturing, cyber-physical systems and cloud manufacturing emerge as new paradigms of manufacturing systems, Yu *et al.* [24] compare the key differences among them. Monostori *et al.* [7] propose the cyber-physical production systems (CPPS) that are regarded as an important step in the fourth industrial revolution, and they will bring a big jump for Industry 4.0. CPPS include autonomous and cooperative elements and subsystems, whose main characteristics are intelligence, connectedness and responsiveness. CPPS introduce the 5C architecture that consists of five levels to construct a system. Some case studies are exemplified to show that CPPS are an important step to develop future manufacturing systems. Wang and Haghighi [25] use holons, agents and function blocks to implement CPSs. A CPS can be regarded as a holarchy of multiple holons, and each holon consists of cyber parts and physical parts. The cyber parts are implemented using multi-agent systems, and the physical parts include machines, robots and materials and are controlled by function blocks. A cyber-physical system prototype of Wise-ShopFloor is developed using this approach. Cupek *et al.* [26] present a hierarchical manufacturing execution system (MES) architecture based on multi-agent systems and CPSs. CPSs can improve the information availability for MESs, whereas MESs can help CPSs plan and organize the manufacturing processes. The proposed architecture has been applied to the short-series production schedule. According to the above analysis, the manufacturing based on CPSs is the most significant advance in manufacturing paradigms.

Formal methods have widely used to model and analyze manufacturing systems to detect errors at the modeling phase and repair them at the high level [27]–[33]. Therefore, the use of a formal representation in CPSs and CPMSs is indispensable for improving the CPS and CPMS trustworthiness. We utilize object-oriented Petri nets to model and analyze CPMSs from the perspective of multi-agent systems [34]. Lu *et al.* [35] use hybrid Petri nets to model a microgrid system, and generate its reachability graph to analyze its properties. Timed automata is used to model medical cyber-physical systems [14] and their requirements are described by computation tree logic. The UPPAAL model checker analyzes and verified the medical cyber-physical system model. Thacker *et al.* [36] propose an extended labeled hybrid Petri net (LHPN) to model CPSs. Discrete valued variables are used to represent software variables and a rich expression syntax describes the mathematical operations performed in CPSs. Finally, a translation system is proposed to translate LHPN models to the assembly language. Jiang *et al.* [5] employ timed automata to model, analyze and verify medical cyber-physical systems with the patient in the loop. Susuki *et al.* [37] use hybrid automaton to model power grid, and compute the reachable set to analyze its dynamic performance.

For trustworthiness analysis of CPMSs, the trustworthiness analysis methods of CPSs can be referred to in analyzing the trustworthiness of CPMSs. Avizienis *et al.* [12] give exact definitions of dependability, high confidence, survivability, and trustworthiness. Their attributes consist of reliability, availability, safety, integrity, maintainability, etc. Nicol *et al.* [38] survey dependability and security modeling methods. Stochastic Petri nets (SPNs) have been widely employed to analyze the dependability, which provide a great advantage over Markov chain and other state-space models. Zeng *et al.* [39] use SPNs to analyze the dependability of control center networks in smart grid. They construct SPN models of control center networks, and then analyze the dependability from two metrics, i.e., reliability and availability. Cho *et al.* [40] use generalized stochastic Petri nets to quantitatively evaluate the intrusion probability of digital control systems in nuclear power plants. A new cyber framework is proposed to prevent cyber attacks, and a physical framework is presented to prevent potential physical attacks. The dependability of digital control systems is analyzed through three metrics, i.e., reliability, maintainability, and availability. GSPNs are adopted to model the dependability for the proposed cyber framework. Through a case study, the proposed framework demonstrates that the dependability analysis of control networks in nuclear power plants is feasible.

Although CPSs provide many advantages for manufacturing systems, unfortunately they are vulnerable to cyber attacks [10]. The security of CPMSs is becoming a significant concern. The cyber systems and cyber-physical devices are potential access points which intruders can use to attack CPMSs, and cyber-attacks on physical systems are becoming a growing concern. In order to assess cyber-physical vulnerabilities for manufacturing systems, DeSmit *et al.* [41] propose an assessment framework, which uses the intersection mapping to identify cyber physical vulnerabilities and employs decision trees to analyze a cyber-physical vulnerability impact. Vincent *et al.* [42] study the cyber security in cyber-physical manufacturing systems. Cyber-attacks can modify the manufacturing intents, thus defective products will be produced or CPMS performance will be reduced. Quality control systems cannot detect the effects of cyber attacks, therefore a novel product design approach for detecting cyber attacks is presented for CPMSs. Wells *et al.* [11] discuss the importance of the cyber-security tool design for manufacturing systems. Cyber attacks may cause hazards to equipment, employees, and consumers. A case study is used to illustrate the feasibility of a cyber-attack on a manufacturing system. In order to describe the CPS dependability, Sanislav *et al.* integrate a primary dependability analysis technique and the knowledge representation to model the system dependability at run-time [43].

CPMSs integrate cyber and physical components to promote the interactions among different entities. To make CPMSs produce desired products, cyber security is a critical aspect of CPMSs [34]. Consequently it is important to develop trustworthy CPMSs to address cyber-attacks. In this paper, we firstly adopt GSPNs to analyze the trustworthiness of CPMSs. When CPMSs are attacked by malicious software, we will study the trustworthiness evolution of CPMSs.

III. TRUSTWORTHINESS MODELING OF CYBER-PHYSICAL MANUFACTURING SYSTEMS

In this section, we review Petri nets and generalized stochastic Petri nets, and then discuss and model CPMSs using GSPNs. Finally, we analyze the trustworthiness of CPMSs.

A. GENERALIZED STOCHASTIC PETRI NETS

Petri nets are a graphical mathematical modeling tool that can describe the structure and behaviors of a system. They can describe distributed, asynchronous and concurrent systems. Petri nets consist of a set of places drawn by circles, a set of transitions drawn by rectangles, a set of arcs, and a set of tokens drawn by dots. Tokens can simulate the dynamic and concurrent actions of systems. Petri nets have behavioral properties, i.e., reachability, boundedness, liveness, home state, coverability [44]–[48]. Analysis methods for Petri nets can be classified into three groups: the reachability tree method, the matrix-equation approach, and reduction techniques [49]–[53]. Petri nets are defined as follow [54].

Definition 1: A Petri net is a 5-tuple, $PN = (P, T, F, W, M_0)$, where

(1) P is a finite set of places, $P = \{p_1, p_2, \ldots, p_i\}$;

(2) T is a finite set of transitions, $T = \{t_1, t_2, \ldots, t_j\}$;

(3) $F \subseteq (P \times T) \cup (T \times P)$ is an arc set connecting different transitions and places;

(4) $W : F \to \{1, 2, 3, \ldots\}$ is a weight function;

(5) $M_0 : P \to \{0, 1, 2, 3, \ldots\}$ is the initial marking.

Generalized stochastic Petri nets are an extension of Petri nets, which have been widely applied to the performance evaluation and dependability analysis of various distributed systems. GSPNs include two types of transitions: 1) timed transitions (drawn as empty bars) and 2) immediate transitions (drawn as solid bars). In GSPNs, when a timed transition enables, it fires after an exponentially distributed firing time; when an immediate transition enables, it fires immediately. Therefore, the state space is then classified into two subsets: a set of tangible states, which are enabled by timed transitions; a set of vanishing states, which are enabled by immediate transition. The definition of GSPNs is given as follows.

Definition 2: A GSPN is a 4-tuple, $GSPN = (PN, T_T, T_I, \lambda)$, where

(1) PN is an ordinary Petri net;

(2) T_T is a finite set of timed transitions;

(3) T_I is a finite set of immediate transitions;

(4) $T_T \cap T_I = \phi, T_T \cup T_I = T$;

(5) $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k)$ is a set of firing rates associated with transitions, which are nonnegative real numbers.

GSPNs can visually describe the relationships between actions and states of systems, which provide advantages over Markov chain and other state-space models.

B. MODELING CYBER-PHYSICAL MANUFACTURING SYSTEMS BY USING GENERALIZED STOCHASTIC PETRI NETS

Driven by a highly volatile market, the traditional manufacturing systems and information systems are integrated into CPMSs. CPMSs perform the actual operations in the physical domain, meanwhile monitor them in the cyber domain by using the corresponding information systems. CPMSs acquire data from sensors embedded on physical entities, transmit the data to computing entities through communication networks, and then process the data and make decisions. CPMSs are more intelligent, responsive, cooperative and flexible. To meet the new market requirements, CPMS structure can be changed over time to produce new products [34].

In this section, we study the trustworthiness issue from three metrics: reliability, availability, and security. Reliability means the probability that the systems continuously provide correct services [12]. The reliability is defined as follows.

$$R(t) = Pr(X > t) = e^{-\lambda t} \tag{1}$$

where X is the continuous random variable and the failure distribution is exponentially distributed. Availability means the readiness for correct services that is defined as follows [12].

$$A(t) = Pr\{Services\ are\ readiness\ at\ time\ t\} \tag{2}$$

For the above definitions of reliability and availability, they are the values at time t. In most cases we are interested in the steady-state reliability and availability [39]. The steady-state reliability is zero that is defined as

$$Rel = \lim_{t\to\infty} R(t) = 0 \tag{3}$$

To obtain high steady-state availability, we should design the mean time to failure (MTTF) as high as possible. For CPMSs, the steady-state availability should focus on providing correct and continuous services for producing parts. Given the steady-state probability vector $\Pi = (\pi_1, \pi_2, \ldots, \pi_n)$, the steady-state availability [40] is defined as

$$Ava = \sum_n \pi_n \tag{4}$$

where π_n is the steady-state value corresponding to the state n where CPMSs can provide correct services. The infinitesimal generator $Q = [q_{ij}]$ is defined as the transition rates between states, then π_n can be got in the following [39]:

$$\begin{cases} \Pi Q = 0 \\ \sum_{i=0}^{n} \pi_i = 1 \end{cases} \tag{5}$$

To get the transient probability of each state, we define $\pi(t) = (\pi_1(t), \pi_2(t), \ldots, \pi_n(t))$ and then get the transient probability [39] in the following:

$$\begin{cases} \frac{d\pi(t)}{dt} = \pi(t)Q \\ A(t) = \sum_n \pi_n(t) \end{cases} \tag{6}$$

Security means that the unauthorized actions cannot access systems, and the unauthorized disclosure and deletion of information can be prevented. Therefore we use the intrusion probability to represent security. The higher the intrusion probability is, the lower the security of CPMSs is. We define the intrusion probability as $I(t)$, and security $\mathscr{S}(t)$ is defined as

$$\mathscr{S}(t) = 1 - I(t) \tag{7}$$

The trustworthiness is a generic concept that includes reliability, availability and security. In order to quantitatively evaluate the trustworthiness, its value $Tr(t)$ is defined as

$$Tr(t) = w_1 R(t) + w_2 A(t) + w_3 \mathscr{S}(t) \tag{8}$$

where w_1, w_2 and w_3 are weight values of reliability, availability and security, respectively, and $w_1 + w_2 + w_3 = 1$. We can set different weight values according to the CPMS requirements.

A typical CPMS is shown in Fig. 1. As all entities in CPMSs are connected together by communication networks, there are many ways to intrude CPMSs. The malicious attackers can intrude CPMSs through numerical machines, sensors, local networks or Internet.

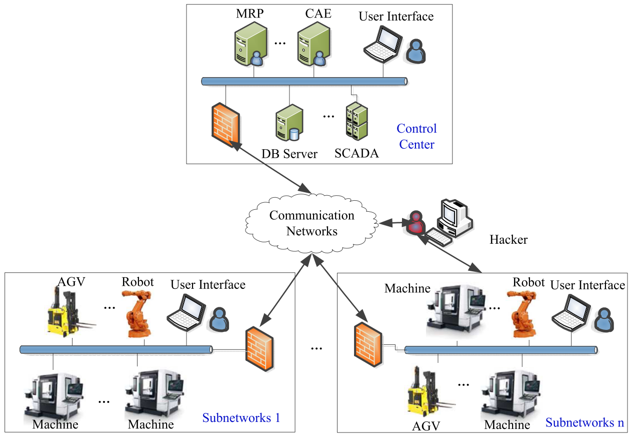


FIGURE 1. A typical CPMS model.

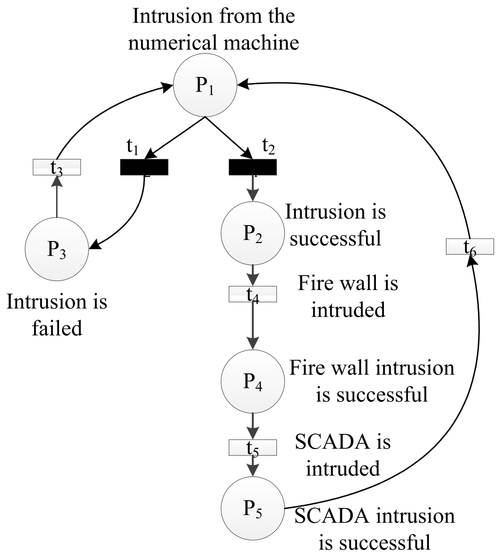


FIGURE 2. Modeling intrusion from a machine in the CPMS.

Inspired by the cyber security in nuclear power plants [40], in this section, we suppose the malicious attackers penetrate CPMSs through a numerical machine and do severe damage. The intrusion model is shown in Fig. 2 by using GSPNs. Communication systems are protected by fire walls. If the attacker can penetrate fire walls, the different subsystems or networks are intruded as well. The firing rates of transitions can be given according to the requirements, and then we can obtain the intrusion probability and security. In Fig. 3 derived from Fig. 1, we present the GSPN model to get the reliability and availability values, which consist of a numerical machine, a fire wall, MRP, CAE and SCADA. Finally, according to (8), we can get the CPMS trustworthiness.

IV. TRUSTWORTHINESS EVOLUTION OF CYBER-PHYSICAL MANUFACTURING SYSTEMS

When CPMSs face the threats of cyber-attacks, the malicious software can spread from one machine to another

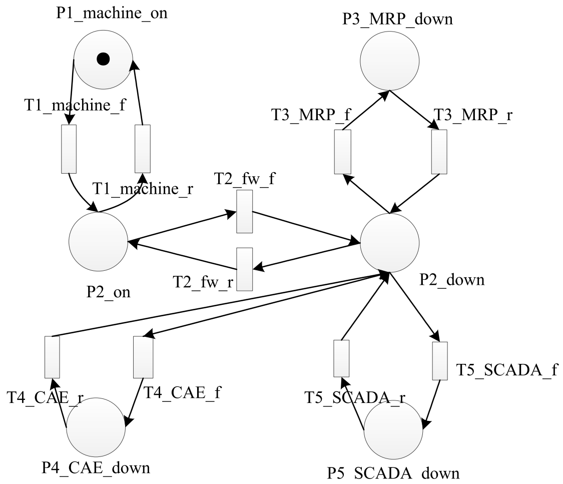


FIGURE 3. The GSPN model of the case.

machine or subsystems through communication networks [34]. The malicious software may destroy the data or disturb manufacturing operations through industrial Ethernet, therefore inferior-quality products are produced.

CPMSs may either resist cyber-attacks or co-exist with the malicious software and reach a low trustworthiness level [34]. When the malicious software spreads in CPMSs, the bifurcations and chaotic states may occur [55], which make CPMSs not stable and disturb their operations. Therefore the CPMS trustworthiness will evolve. In this section, to reveal the CPMS trustworthiness evolution mechanism, the malicious software spreading model in CPMSs is studied, its dynamic behaviors analyzed, and the trustworthiness evolution model proposed.

A. MODELING AND ANALYZING MALICIOUS SOFTWARE SPREADING IN CYBER-PHYSICAL MANUFACTURING SYSTEMS

Let us consider a large scale CPMS. The malicious software has infected some nodes (such as machines, sensors, robots, AGVs) and spread to other susceptible nodes, which are referred to as nodes that are most vulnerable to the malicious software attacks. As a result, these nodes turn into the exposed nodes that can remain in a sleep mode. Until they are activated, the exposed nodes turn into the infectious nodes. Once the malicious software in infectious nodes is removed, they can change into recovered nodes [34]. We denote the susceptible nodes, exposed nodes, infectious nodes, and recovered nodes as S, E, I and R, respectively [56]. The other parameters are described as follows.

1) The initial state of each node is considered as susceptible state.
2) New nodes can join CPMSs, and some nodes may log out CPMSs. We regard the join and drop-out rate as the same value μ.
3) The E and I nodes can infect S nodes.

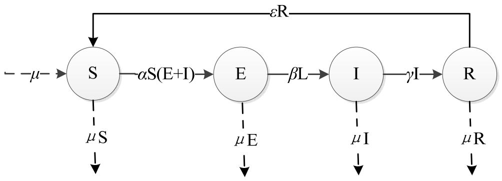


FIGURE 4. The state transition process of different nodes.

4) The infection rate α, the outbreak rate β, the recovery rate γ, the restore rate ϵ, the join or drop-out rate μ are non-negative constant.

The state transition process of different nodes in the CPMS is shown in Fig. 4. We denote $S(t)$, $E(t)$, $I(t)$, and $R(t)$ as the probability of susceptible, exposed, infectious and recovered nodes, and then we can get the susceptible-exposed-infected-removed-susceptible (SEIRS) model of the malicious software spreading in the CPMS.

$$\begin{cases} \dfrac{dS(t)}{dt} = \mu - \alpha S(t)(E(t)+I(t)) + \epsilon R(t) - \mu S(t) \\ \dfrac{dE(t)}{dt} = \alpha S(t)(E(t)+I(t)) - \beta E(t) - \mu E(t) \\ \dfrac{dI(t)}{dt} = \beta E(t) - \gamma I(t) - \mu I(t) \\ \dfrac{dR(t)}{dt} = \gamma I(t) - \epsilon R(t) - \mu R(t) \end{cases} \tag{9}$$

As $S(t)+E(t)+I(t)+R(t) = 1$, then the SEIRS model can be changed as follows.

$$\begin{cases} \dfrac{dE(t)}{dt} & = \alpha(1-E(t)-I(t)-R(t))(E(t)+I(t)) \\ & \quad -\beta E(t) - \mu E(t) \\ \dfrac{dI(t)}{dt} & = \beta E(t) - \gamma I(t) - \mu I(t) \\ \dfrac{dR(t)}{dt} & = \gamma I(t) - \epsilon R(t) - \mu R(t) \end{cases} \tag{10}$$

where $E(t) \geq 0, I(t) \geq 0, R(t) \geq 0$, its state space $\Omega = \{(E(t), I(t), R(t)) : E(t) \geq 0, I(t) \geq 0, R(t) \geq 0, E(t) + I(t) + R(t) \leq 1\}$.

To reveal the malicious software spreading mechanism in the CPMS, we should analyze the dynamic behaviors of the SEIRS model, such as the stability, equilibriums and bifurcations [34].

Basic reproductive number [57] R_0 is defined as the threshold that determines whether the malicious software can spread in the CPMS. The basic reproductive number in (10) is

$$R_0 = \alpha \frac{\beta+\gamma+\mu}{(\beta+\mu)(\gamma+\mu)}$$

and we always have non-trivial equilibriums $E_0 = (0, 0, 0)$, $E_1 = (k, 0, k)$ and an endemic equilibrium $E^* = (E_*, I_*, R_*)$, where

$$E_* = A(\gamma+\mu)(\epsilon+\mu), I_* = A\beta(\epsilon+\mu), R_* = A\beta\gamma,$$
$$A = \frac{(\beta+\mu)(\gamma+\mu)(R_0-1)}{\alpha(\beta+\gamma+\mu)[\mu(\beta+\epsilon+\mu)+(\beta+\mu)(\epsilon+\mu)]}$$

Theorem 1: The system in (10) is locally asymptotically stable at the equilibrium E_0 iff $R_0 < 1$.

Proof: The Jacobian matrix of (10) at E_0 is

$$J_{E_0} = \begin{bmatrix} \alpha-\beta-\mu & \alpha & 0 \\ \beta & -\mu-\gamma & 0 \\ 0 & \mu & -\mu-\epsilon \end{bmatrix}$$

Its characteristic equation is

$$\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 = 0,$$

where

$$\begin{aligned} a_1 &= \beta + 3\mu + \gamma + \epsilon - \alpha, \\ a_2 &= (\mu+\epsilon)(\beta + 2\mu + \epsilon - \alpha) + (\mu+\gamma)(\beta + \mu - \alpha) - \alpha\beta, \\ a_3 &= (\mu+\epsilon)[(\mu+\gamma)(\beta+\mu-\alpha) - \alpha\beta] \end{aligned}$$

then we can get $\Delta_1 = a_1 = \beta + 3\mu + \gamma + \epsilon - \alpha$, $\Delta_2 = a_1a_2 - a_3$.

According to the Routh-Hurwitz stability criterion, if and only if $R_0 < 1$ and $\Delta_1 > 0$, $\Delta_2 > 0$, the system in (10) is locally asymptotically stable. □

Theorem 2: If $R_0 > 1$, the system in (10) is locally asymptotically stable at the equilibrium E^*.

Proof: We can obtain the Jacobian matrix J_{E^*} of (10) at E^*.

Its characteristic equation is

$$\lambda^3 + a_1\lambda^2 + a_2\lambda + a_3 = 0,$$

where

$$\begin{aligned} a_1 &= \alpha(E_* + I_* + \frac{S_*I_*}{E_*}) + \beta\frac{E_*}{I_*} + \gamma\frac{I_*}{R_*}, \\ a_2 &= \frac{\beta\gamma E_* + \alpha\beta(E_*+I_*)^2}{I_*} + \alpha\gamma\frac{I_*E_*^2 + I_*^2E_* + S_*I_*^2}{R_*E_*}, \\ a_3 &= \alpha\beta\gamma\frac{(R_*+E_*+I_*)(L_*+I_*)}{R_*} \end{aligned}$$

then we can obtain $\Delta_1 = a_1 > 0, a_2 > 0, a_3 > 0, \Delta_2 = a_1a_2 - a_3 > 0$.

According to the Routh-Hurwitz stability criterion, we conclude that the system in (10) is locally asymptotically stable. □

We set the parameters as $\alpha = 0.12$, $\beta = 0.5$, $\gamma = 0.1$, $\mu = 0.1$, $\epsilon = 0.3$, and $R_0 = 0.7 < 1$. The simulation results are shown in Fig. 5, which represents Theorem 1 holds. The system in (10) is locally asymptotically stable at $E_0 = (1, 0, 0, 0)$.

According to Theorem 2, we set the parameters as $\alpha = 0.3$, $\beta = 0.5$, $\gamma = 0.1$, $\mu = 0.1$, $\epsilon = 0.3$, and $R_0 = 1.75 > 1$. The different initial values are chosen to do simulations, and the simulation results are shown in Fig. 6. Fig. 6 represents that Theorem 2 holds, and the system in (10) is locally asymptotically stable at $E^* = (0.57, 0.1, 0.26, 0.07)$.

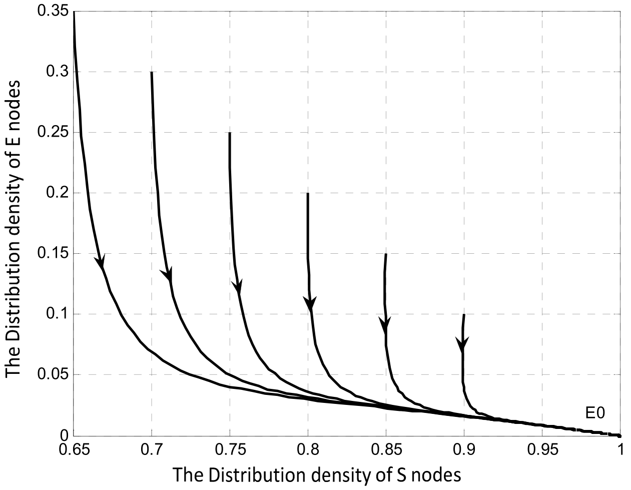


FIGURE 5. The trajectory of S and E nodes.

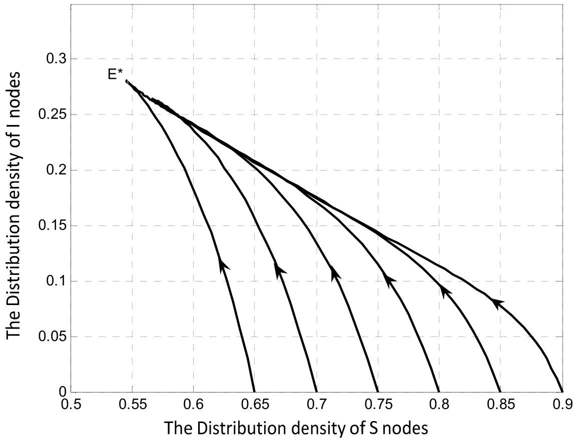


FIGURE 6. The trajectory of S and I nodes.

B. ANALYZING TRUSTWORTHINESS EVOLUTION OF CYBER-PHYSICAL MANUFACTURING SYSTEMS

A large scale CPMS consists of many nodes, and they are classified into the susceptible nodes, exposed nodes, infectious nodes, and recovered nodes. Since different types of nodes have different effects to the CPMS trustworthiness, we combine the distribution density of nodes with initial CPMS trustworthiness to obtain a trustworthiness evolution model, which is defined as follows.

$$Tr(t)' = Tr(t)(a_1S(t)' + a_2E(t)' + a_3I(t)' + a_4R(t)') \quad (11)$$

where a_1, a_2, a_3, a_4 represent the weight values of different nodes, and $a_1 + a_2 + a_3 + a_4 = 1$.

In the above model in (11), we can obtain the CPMS trustworthiness evolution process according to the malicious software spreading. In the proposed SEIRS model, the S nodes can provide the expected functions, so they have higher trustworthiness; the E and I nodes have lower trustworthiness; the R nodes can defend the malicious software, so they have the highest trustworthiness among the nodes.

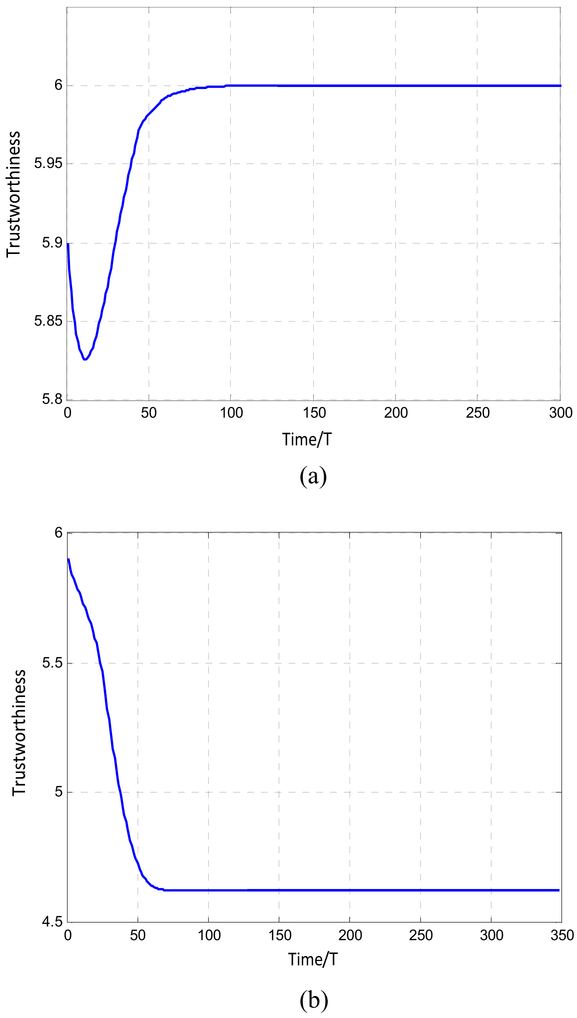


FIGURE 7. (a) The CPMS trustworthiness evolution process when the CPMS is stable at E_0. (b) The CPMS trustworthiness evolution process when the CPMS is stable at E^*.

According to the GSPN model and the trustworthiness evolution model, we can find the CPMS trustworthiness evolution process as shown in Fig. 7. In Fig. 7 (a), with the temporary increase of E and I nodes, the CPMS trustworthiness drops. When E and I nodes disappear and the CPMS is stable at the equilibrium E_0, the CPMS trustworthiness rises and eventually stabilizes at a high level. In Fig. 7 (b), the CPMS is stable at the equilibrium E^*. As the number of E and I nodes increases, the CPMS trustworthiness reduces and eventually stabilizes at a low level.

V. CONCLUSION

In order to meet new market demands and improve the produce quality, cyber-physical systems are introduced into manufacturing systems and cyber-physical manufacturing systems are constructed. As CPMSs are susceptible to cyber attacks, to model and analyze the trustworthiness of CPMSs, this work utilizes generalized stochastic Petri nets to model CPMSs. The trustworthiness can be measured from three metrics, i.e., the reliability, availability and security. As the malicious software may attack CPMSs at run-time, we propose the malicious software spreading model and analyze its behaviors. Finally, the CPMS trustworthiness evolution model is constructed. The simulation results show that the proposed approach is effective in analyzing the CPMS trustworthiness.

REFERENCES

[1] National Science Foundation of the United States. *Cyber-Physical System (CPS) Program Solicitation*. Accessed: Aug. 18, 2017. [Online]. Available: http://www.nsf.gov/pubs/2010/nsf10515/nsf10515.htm

[2] E. A. Lee and S. A. Seshia. (2011). *Introduction to Embedded Systems—A Cyber-Physical Systems Approach*. [Online]. Available: http://LeeSeshia.org

[3] X. Guan, B. Yang, C. Chen, W. Dai, and Y. Wang, "A comprehensive overview of cyber-physical systems: From perspective of feedback system," *IEEE/CAA J. Autom. Sinica*, vol. 3, no. 1, pp. 1–14, Jan. 2016.

[4] P. Marwedel, *Embedded System Design: Embedded Systems Foundations of Cyber-Physical Systems*. Dordrecht, The Netherlands: Springer, 2011.

[5] Z. Jiang, M. Pajic, and R. Mangharam, "Cyber–physical modeling of implantable cardiac medical devices," *Proc. IEEE*, vol. 100, no. 1, pp. 122–137, Jan. 2012.

[6] D. Wu, D. W. Rosen, L. Wang, and D. Schaefer, "Cloud-based design and manufacturing: A new paradigm in digital manufacturing and design innovation," *Comput.-Aided Des.*, vol. 59, pp. 1–14, Feb. 2015.

[7] L. Monostori *et al.*, "Cyber-physical systems in manufacturing," *CIRP Ann.–Manuf. Technol.*, vol. 65, no. 2, pp. 621–641, 2016.

[8] L. Wang, M. Törngren, and M. Onori, "Current status and advancement of cyber-physical systems in manufacturing," *J. Manuf. Syst.*, vol. 37, pp. 517–527, Oct. 2015.

[9] C. Liu and P. Jiang, "A cyber-physical system architecture in shop floor for intelligent manufacturing," *Procedia CIRP*, vol. 56, pp. 372–377, Mar. 2016.

[10] R. F. Babiceanua and R. Seker, "Big data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook," *Comput. Ind.*, vol. 81, pp. 128–137, Sep. 2016.

[11] L. Wells, J. A. Camelio, C. B. Williams, and J. White, "Cyber-physical security challenges in manufacturing systems," *Manuf. Lett.*, vol. 2, no. 2, pp. 74–77, Apr. 2014.

[12] 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. 2004.

[13] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," *Proc. IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016.

[14] I. Lee *et al.*, "Challenges and research directions in medical cyber–physical systems," *Proc. IEEE*, vol. 100, no. 1, pp. 75–90, Jan. 2012.

[15] J. Sztipanovits *et al.*, "Toward a science of cyber–physical system integration," *Proc. IEEE*, vol. 100, no. 1, pp. 29–44, Jan. 2012.

[16] (2009). *National Workshop for Research on High-Confidence Transporation Cyber-Physical Systems in Automotive, Aviation, and Rail*. [Online]. Available: http://www.ee.washington.edu/research/nsl/aar-cps

[17] B. Esmaeilian, S. Behdad, and B. Wang, "The evolution and future of manufacturing: A review," *J. Manuf. Syst.*, vol. 39, pp. 79–100, Apr. 2016.

[18] 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.

[19] J. Lee, B. Bagheri, and C. Jin, "Introduction to cyber manufacturing," *Manuf. Lett.*, vol. 8, pp. 11–15, Apr. 2016.

[20] S. Jeschke, C. Brecher, H. Song, and D. B. Rawat, Eds., *Industrial Internet of Things: Cybermanufacturing Systems*. Cham, Switzerland: Springer, 2017.

[21] Z. Song, Y. Sun, J. Wan, and P. Liang, "Data quality management for service-oriented manufacturing cyber-physical systems," *Comput. Elect. Eng.*, to be published. [Online]. Available: http://dx.doi.org/10.1016/j.compeleceng.2016.08.010

[22] G. Putnik *et al.*, "Scalability in manufacturing systems design and operation: State-of-the-art and future developments roadmap," *CIRP Ann.–Manuf. Technol.*, vol. 62, no. 2, pp. 751–774, 2013.

[23] P. Jiang, K. Ding, and J. Leng, "Towards a cyber-physical-social-connected and service-oriented manufacturing paradigm: Social manufacturing," *Manuf. Lett.*, vol. 7, pp. 15–21, Jan. 2016.

[24] C. Yu, X. Xu, and Y. Lu, "Computer-integrated manufacturing, cyber-physical systems and cloud manufacturing—Concepts and relationships," *Manuf. Lett.*, vol. 6, pp. 5–9, Oct. 2015.

[25] L. Wang and A. Haghighi, "Combined strength of holons, agents and function blocks in cyber-physical systems," *J. Manuf. Syst.*, vol. 40, pp. 25–34, Jul. 2016.

[26] R. Cupek, A. Ziebinski, L. Huczala, and H. Erdogan, "Agent-based manufacturing execution systems for short-series production scheduling," *Comput. Ind.*, vol. 82, pp. 245–258, Oct. 2016.

[27] J. Zhang, M. Khalgui, Z. Li, G. Frey, O. Mosbahi, and H. Ben Salah, "Reconfigurable coordination of distributed discrete event control systems," *IEEE Trans. Control Syst. Technol.*, vol. 23, no. 1, pp. 323–330, Jan. 2015.

[28] Y. Tong, Z. Li, C. Seatzu, and A. Giua, "Verification of state-based opacity using Petri nets," *IEEE Trans. Autom. Control*, vol. 62, no. 6, pp. 2823–2837, Jun. 2017.

[29] Y. Chen, Z. Li, A. Al-Ahmari, N. Wu, and T. Qu, "Deadlock recovery for flexible manufacturing systems modeled with Petri nets," *Inf. Sci.*, vol. 381, pp. 290–303, Mar. 2017.

[30] Z. Ma, Z. Li, and A. Giua, "Design of optimal Petri net controllers for disjunctive generalized mutual exclusion constraints," *IEEE Trans. Autom. Control*, vol. 60, no. 7, pp. 1774–1785, Jul. 2015.

[31] M. Uzam, Z. Li G. Gelen, and R. S. Zakariyya, "A divide-and-conquer-method for the synthesis of liveness enforcing supervisors for flexible manufacturing systems," *J. Intell. Manuf.*, vol. 27, no. 5, pp. 1111–1129, Oct. 2016.

[32] Q. Zhu, M. Zhou, Y. Qiao, and N. Wu, "Petri net modeling and scheduling of a close-down process for time-constrained single-arm cluster tools," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published, doi: 10.1109/TSMC.2016.2598303.

[33] Q. Zhu, N. Wu, Y. Qiao, and M. Zhou, "Optimal scheduling of complex multi-cluster tools based on timed resource-oriented Petri nets," *IEEE Access*, vol. 4, pp. 2096–2109, 2016.

[34] Z. Yu, J. Ouyang, S. Li, and X. Peng, "Formal modeling and control of cyber-physical manufacturing systems," *Adv. Mech. Eng.*, vol. 9, no. 10, pp. 1–12, 2017.

[35] X. Lu, M. Zhou, A. C. Ammari, and J. Ji, "Hybrid Petri nets for modeling and analysis of microgrid systems," *IIEEE/CAA J. Autom. Sinica*, vol. 3, no. 4, pp. 349–356, Oct. 2016.

[36] R. A. Thacker, K. R. Jones, C. J. Myers, and H. Zheng, "Automatic abstraction for verification of cyber-physical systems," in *Proc. Int. Conf. Cyber-Phys. Syst.*, 2010, pp. 12–21.

[37] Y. Susuki *et al.*, "A hybrid system approach to the analysis and design of power grid dynamic performance," *Proc. IEEE*, vol. 100, no. 1, pp. 225–239, Jan. 2012.

[38] D. M. Nicol, W. H. Sanders, and K. S. Trivedi, "Model-based evaluation: From dependability to security," *IEEE Trans. Depend. Sec. Comput.*, vol. 1, no. 1, pp. 48–65, Jan. 2004.

[39] R. Zeng, Y. Jiang, C. Lin, and X. Shen, "Dependability analysis of control center networks in smart grid using stochastic Petri nets," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1721–1730, Sep. 2012.

[40] C.-S. Cho, W.-H. Chung, and S.-Y. Kuo, "Cyberphysical security and dependability analysis of digital control systems in nuclear power plants," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 46, no. 3, pp. 356–369, Mar. 2016.

[41] Z. DeSmit, A. E. Elhabashy, L. J. Wells, and J. A. Camelio, "Cyber-physical vulnerability assessment in manufacturing systems," *Procedia Manuf.*, vol. 5, pp. 1060–1074, Jun./Jul. 2016.

[42] H. Vincent, L. Wells, P. Tarazaga, and J. Camelio, "Trojan detection and side-channel analyses for cyber-security in cyber-physical manufacturing systems," *Procedia Manuf.*, vol. 1, pp. 77–85, Jun. 2015.

[43] T. Sanislav, G. Mois, and L. Miclea, "An approach to model dependability of cyber-physical systems," *Microprocess. Microsyst.*, vol. 41, pp. 67–76, Mar. 2016.

[44] Z. Li and M. Zhou, "Elementary siphons of Petri nets and their application to deadlock prevention in flexible manufacturing systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 34, no. 1, pp. 38–51, Jan. 2004.

[45] Y. Chen, Z. Li, and A. Al-Ahmari, "Nonpure Petri net supervisors for optimal deadlock control of flexible manufacturing systems," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 43, no. 2, pp. 252–265, Mar. 2013.

[46] S. Wang, D. You, M. Zhou, and C. Seatzu, "Characterization of admissible marking sets in Petri nets with uncontrollable transitions," *IEEE Trans. Autom. Control*, vol. 61, no. 7, pp. 1953–1958, Jul. 2016.

[47] D. You, S. Wang, and M. Zhou, "Computation of strict minimal siphons in a class of Petri nets based on problem decomposition," *Inf. Sci.*, vols. 409–410, pp. 87–100, Oct. 2017.

[48] S. Wang, D. You, and M. Zhou, "A necessary and sufficient condition for a resource subset to generate a strict minimal siphon in S^{4}PR," *IEEE Trans. Autom. Control*, vol. 62, no. 8, pp. 4173–4179, Aug. 2017.

[49] Z. Li, G. Liu, H.-M. Hanisch, and M. Zhou, "Deadlock prevention based on structure reuse of Petri net supervisors for flexible manufacturing systems," *IEEE Trans. Syst., Man, Cybern. A, Syst., Humans*, vol. 42, no. 1, pp. 178–191, Jan. 2012.

[50] Y. Chen, Z. Li, K. Barkaoui, and M. Uzam, "New Petri net structure and its application to optimal supervisory control: Interval inhibitor arcs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 44, no. 10, pp. 1384–1400, Oct. 2014.

[51] Y. Chen, Z. Li, K. Barkaoui, and A. Giua, "On the enforcement of a class of nonlinear constraints on Petri nets," *Automatica*, vol. 55, pp. 116–124, May 2015.

[52] Y. Tong, Z. Li, and A. Giua, "On the equivalence of observation structures for Petri net generators," *IEEE Trans. Autom. Control*, vol. 61, no. 9, pp. 2448–2462, Sep. 2016.

[53] Y. Chen, Z. Li, K. Barkaoui, N. Wu, and M. Zhou, "Compact supervisory control of discrete event systems by Petri nets with data inhibitor arcs," *IEEE Trans. Syst., Man, Cybern., Syst.*, vol. 47, no. 2, pp. 364–379, Feb. 2017.

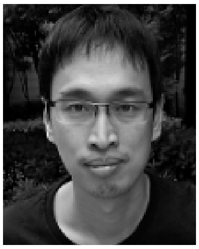
[54] T. Murata, "Petri nets: Properties, analysis and applications," *Proc. IEEE*, vol. 77, no. 4, pp. 541–580, Apr. 1989.

[55] G. Chen, J. L. Moiola, and H. O. Wang, "Bifurcation control: Theories, methods, and applications," *Int. J. Bifurcation Chaos*, vol. 10, no. 3, pp. 511–548, Mar. 2000.

[56] B. K. Mishra and D. K. Saini, "SEIRS epidemic model with delay for transmission of malicious objects in computer network," *Appl. Math. Comput.*, vol. 188, no. 2, pp. 1476–1482, May 2007.

[57] F. Brauer, P. van den Driessche, and J. Wu, Eds., *Mathematical Epidemiology*. Springer-Verlag, 2008.

ZHENHUA YU received the B.S. and M.S. degrees from Xidian University, Xi'an, China, in 1999 and 2003, respectively, and the Ph.D. degree from Xi'an Jiaotong University, Xi'an, China, in 2006. He is currently an Associate Professor with the School of Information and Navigation, Air Force Engineering University, Xi'an, China. He has authored over 20 technical papers for conferences and journals, and holds two invention patents. His research mainly focuses on cyber-physical systems, trusted computing and formal methods.



LIJUN ZHOU received the B.S. degree from Harbin Engineering University, Harbin, China, in 2005, the M.S. degree from the Xi'an Institute of Applied Optics, Xi'an, China, in 2010, where he has been a Senior Engineer since 2009. He is currently pursuing the Ph.D. degree with the Xi'an Institute of Applied Optics. He has authored over ten technical papers and technical reports, and holds three invention patents. His research mainly focuses on cyber-physical systems, and communication networks.

ZHIQIANG MA received the B.S. degree from the College of Air Force Telecommunication Engineering, Xi'an, China, in 1993, and the M.S. degree from Navy Engineering University, Wuhan, China, in 2003. He is currently an Associate Professor with the School of Information and Navigation, Air Force Engineering University, Xi'an, China. He has authored over ten technical papers for conferences and journals. His research mainly focuses on communication systems.

MOHAMMED A. EL-MELIGY received the B.S. degree in Information Technology from Menoufia University of Egypt, in 2005. He has been a Software Engineer with King Saud University, Riyadh, Saudi Arabia, since 2009. His research interests include Petri nets, supervisory control of discrete event systems, database software, and network administration.