Modeling and Analysis of the Reliability of Digital Networked Control Systems Considering Networked Degradations

Huadong Mo, *Student Member, IEEE*, Wei Wang, Min Xie, *Fellow, IEEE*, and Junlin Xiong, *Member, IEEE*

***Abstract*—Digital networked control systems are of growing importance in safety-critical systems and perform indispensable function in most complex systems today. Networked degradations such as transmission delay and packet dropout cause such systems to fail to satisfy performance requirements, and eventually affect the overall reliability. It is necessary to get a model to verify and evaluate the system reliability in early design phase, prior to its implementation. However, existing probabilistic models only provide partial descriptions of such coupled networks and control system. In this paper, a new stochastic model represented by linear discrete-time approach is proposed, considering data packet transmissions in both channels: controller-to-actuator and sensor-to-controller. Different from pervious works, the historical behaviors of networked degradations are modeled by multistate Markov chains with uncertainties, releasing the assumption that faults of all periods are independent of each other. The concept of domain requirements for such systems is considered here, contributing to the integration of control and reliability engineering. Methodologies for quantitatively assessing the reliability of the single- and sequential-control goal are derived from the Monte Carlo method. An example of an industrial heat exchanger digital networked control system is provided to illustrate the effectiveness of the model and method.**

***Note to Practitioners*—Digital control systems are widely used for safety-critical systems today, and for such a system, the reliability has become an important topic. It is a difficult issue due to its complexity, time-dependence, and degradation. The proposed framework in this paper enables dynamic reliability modeling and statistical analysis for digital control systems subject to networked degradations. The novelty of this paper is the modeling and analysis that link the control system and reliability engineering. The control systems are regarded as failures determined by whether the performances satisfy all operational requirements and the reliability concerns the ability of system or component to perform its required functions under stated conditions for a specified period of time. Therefore, the reliability of the digital networked control systems can be defined as the ability of the control systems to maintain operational requirements in the presence of networked degradations. Monte Carlo simulation can be used to quantitatively assess such ability. Case study shows that this framework is applicable in helping the designers fully understand the systems and make decisions.**

***Index Terms*—Digital networked control systems (DNCSs), Monte Carlo, networked degradations, reliability.**

I. Introduction

MOTIVATED by the fast widespread communication networks, digital networked control systems (DNCSs), showed in Fig. 1, which refer to a class of spatially distributed digital control systems (DCSs) in which the networks provide data exchanges among controllers, actuators, sensors and other subsystems in the systems, have been widely employed in complex and safety-critical systems [1]–[6]. Compared with traditional point-to-point DCSs, the DNCSs are more cost-effective and bring huge functionalities, which are inconceivable in the past, such as greater flexibility in system maintenance and fault diagnosis, lower installation fee, less system wiring as well as higher system reliability [3], [7]. There are many potential applications of DNSCs, including nuclear power plant, smart power grids, intelligent traffic control systems, automatic warehouse management systems, and remote surgery [8]–[13]. Though above applications are in different areas, they share some common features–large scale, openness, time-critical and safety-critical [14].

In the DNCSs, feedback control loops are closed through real-time communication networks just as shown in Fig. 1 [6], [15], [16]. The operations of the DNCSs in one period obey the following process: the sensor records the system output every period [16], [17]. Then, the AD converter converts the physical output into digital signal and sends the data packet of output signal to controller, via communication networks. The received data packet is stored at buffer, and then the controller unpacks the newest packet and computes the control signal according to preset control strategy. Next, the control signal is transferred to actuator via communication networks, and stored in the buffer. Finally, the actuator performs according to the control signal which has been converted into analog signal.

The operations indicate that the DNCSs are highly time-dependent and easily affected by the time-varying aspects. Degradations in the communication networks which have arisen from

Manuscript received April 11, 2015; accepted June 03, 2015. This paper was recommended for publication by Associate Editor J. Gao and Editor Editor D. Tilbury upon evaluation of the reviewers' comments. Date of publication June 26, 2015; date of current version June 29, 2017. This work was supported in part by a grant from the City University of Hong Kong (Project No. 9380058) and in part by a grant from NSFC (Project No. 61374026).

H. Mo and M. Xie are with the City University of Hong Kong, System Engineering and Engineering Management, Hong Kong, China (e-mail: huadongmo2-c@my.cityu.edu.hk; minxie@cityu.edu.hk).

W. Wang are J. Xiong with the University of Science and Technology of China, Automation, Hefei, China (e-mail: wangwei2-c@my.cityu.edu.hk; xiong77@ustc.edu.cn).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TASE.2015.2443132

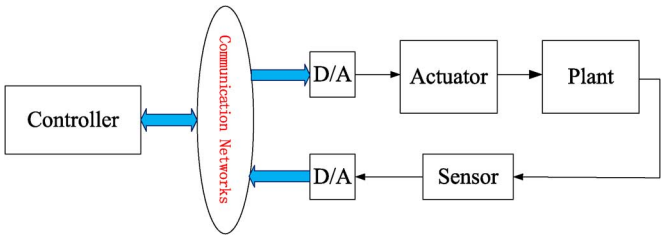


Fig. 1. A digital networked control system.

some inherent and inevitable sophistication [18], [45]: induced transmission delays and packet dropouts, definitely jeopardize the performance of the entire DNCSs by forcing the system to use inaccurate information to make a decision or take action [19]–[22]. How to build the stochastic model and quantitatively assess the effects of these two faults on the performance of the DNCSs is still an open discussion.

Previous work can be categorized into two types based on the contributions: reliability modeling design and performance assessment methodology. Traditional reliability modeling and assessment methodologies, such as static Event Tree and Fault Tree approach, are impractical in evaluating the reliability of DNCSs for the inability to provide an accurate state evolution as a function of time. Reference [23] proposes the Dynamic Flowgraph Methodology (DFM) to model and analyze a DCS in a "systems" framework in which the behaviors of systems are modeled by transfer boxes, causality edges, and process variable nodes. Then, [16] adopts the DFM to model the time dependency, multistate behavior and interaction in the DCSs which used PI control strategy, integrated with communication networks. In this work, there only exist constant transmission delays in the sensor-to-controller channel. Reference [24] improves the computational efficiency of DFM for the reliability assessment of DNCSs by using the binary decision diagrams to increase the scalability to avoid the combinatorial explosion. There exist other works which apply uniform distribution and Markov chains subject to uncertainties to describe transmission delays [25], [26].

It noticed that the literatures have paid much attention to transmission delays and ignored the packet dropouts. Several works about designing optimal control strategy consider both transmission delays and packet dropouts simultaneously. The proposed model are represented by differential equations and have three types categorized based on the final close-loop DNCSs: switching systems [27]–[29], asynchronous dynamical systems [19], [28], and jump linear systems in which the packet dropouts are modeled by Markov chains [30]–[32].

All the models given in the aforementioned references are derived from the assumption that the transmission delays and packet dropouts only exist in sensor-to-controller channel. The influence of faults in the controller-to-actuator channel on the performance of the DNCSs is neglected due to the complicated modeling. Recently, Bernoulli or a two-state Markov chain process is introduced to model the DNCSs as stochastic parameter systems, with packet dropouts on both channels [20], [28], [33]–[35].

The packet dropouts described by Bernoulli or a two-state Markov chain have two states: missed and sent successfully. Such models are based on the assumption that each period is independent of each other. In fact, packet dropout more likely happens if packet dropouts have happened at the previous ones. References [15], [20], [32], [48], and [49] improve the modeling of the DNCSs by introducing a multistate Markov chain to describe the historical behavior of packet dropouts. By describing the quantity of packet dropouts between current period and its latest successful transmission other than the historical information of a packet is missed or not, multistate Markov chain is defined and the relationship between adjacent periods can be presented clearly. This model releases the assumption that each period is independent of each other. Nevertheless, compared with the effort spent on the reliability modeling, how to quantitatively evaluate the influence of the transmission delays and packet dropouts on the performance of DNCSs should receive more attentions.

The ability of the feedback DNCSs to compensate the consequences of the inherent faults redefines the concept of failures: the reliability of the DNCSs is dependent not only on which kind of fault that may occur, but also on the evolving states of system output and control signal of each period [36], [37]. Classical reliability evaluation methods, i.e., Fault Tree or Failure Mode and Effect Analysis are not appropriate to be applied to these evolving states, due to the dynamic aspects of DNCSs. Reference [38] proposes Structured Analysis and Design Techniques based on Monte Carlo simulation for the reliability evaluation [43]. This method explicitly formalizes the functional interactions between subsystems, identifies the characteristic values affecting the reliability of DNCSs, and quantifies the RAMS parameters related to operational architecture. As the remaining ability of system to maintain the expected control goal after faults occurring is crucial [37], apply ordered sequences of multifailure method to assess the reliability of all possible DNCSs' architectures. A new methodology called multifault tree is proposed and the time-ordered sequences of failures is discussed.

The reliability of DNCSs is evaluated as a function of required performances from a control viewpoint [25]. The DNCSs will be regarded as a failure if the performances do not satisfy all requirements. The difference equations are used to describe the stochastic model of the DNCSs, explicitly illustrating the influence of the transmission delays and packet dropouts on changing the model parameters. The linear discrete-time dynamic approach for modeling the flow of signal in, out, and among all subsystems promotes straightforward calculation of fundamental dynamic aspects such as times and faults characteristics [39]. The transmission delays and packet dropouts are described by Uniform distribution and Bernoulli distribution, respectively. Reference [14] summarizes the domain requirements used in the performance analysis, which are not formed as basic definitions in [25]. The performance of DNCSs not only needs to satisfy all operational requirements relevant to the real-time operation, but also needs to maintain a high level of reliability to satisfy the nonfunctional requirement.

The reliability models and evaluation methods provided by previous references just consider partial aspects of the realistic DNCSs. The analysis and design based on these may be inef-

fective when applied to realistic applications, though it is easy to deduce close-form solutions. A more comprehensive model and assessment method are necessary to narrow the gap between theoretical works and real applications.

As this is the first attempt to study the reliability of this type of system, the linear systems is used to avoid unnecessary complexity for clarity. For other more complex systems, a similar idea can be used and extensions are usually straightforward with complicated expressions. In general, a mathematic model of the DNCSs is derived, considering the networked degradations. For example, for nonlinear systems, one widely adopted method is the linearization, such as exact/approximate input–output and neural network-based linearization, which work well up to some accuracy and certain range for the input values [52], [61]–[64]. As nonlinear systems could be approximated by linear equations, the proposed model can be extended to this special case easily.

Although the problem for DNCSs with discrete-time delays has been well studied, there exists very little literature on continuous time delays, comprising distributed ones and the ones obeying Markov process [52], [56], [57]. Continuous time delays are more of practical significance since the network induced delay may propagate in a distributed way or Markov process during a certain time period. Different from the common assumptions on discrete-time delays, it is assumed here the statistic information of the continuous time delay taking values is known. In general, the variation range of the continuous time delay is available. The lower bound of the delay is not zero and upper bound is known as the maximum allowable bound, which ensures the stability of the DNCSs [58], [59]. Therefore, in this paper, one common used Markov process-reflected Wiener process is introduced to model the continuous time delays. The statistic characters of the reflected Wiener process can be easily estimated from collected data by the Maximum-Likelihood Estimation method.

Multistate Markov chains subject to uncertainties are used to describe the packet dropouts. It is an improvement compared with existing works, which have always assumed that the statistic information about the packet dropouts is complete known and its Markov chain usually has constant transition probability [15], [25]. However, it is always the case that the statistic information on the characteristic of the networked degradation is inadequate or partially unknown, due to limited observations. The description of packet dropout with a Markov chain subject to partially unknown transition probabilities is more practical and general.

It is well known that there are two kinds of uncertainties, the polytopic and norm-bounded uncertainties [65]. The polytopic representation is the most common one to describe the physical parameter uncertainty without any conservatism [48]. In this method, the uncertain Markov transition probability matrix belongs to a polytope which is the convex hull of the parameters of a set of vertices [26], [49]. Polytopic uncertainties method is applicable for the well-known interval, linear and multimodel parameter uncertainty. It has various applications in DNCSs, reachable set analysis and fault detection filter design. The benefits of using this convex combination method is that the parameters can be easily estimated and further system optimization can be conducted through convex optimization [65]. Therefore, in this paper, the partially unknown transition probabilities are modeled using the polytopic uncertainties method.

There have been quite a bit of research on the degradation modeling and this paper is to make use of this in the study of reliability of networked control systems [3], [15], [21], [25], [32], [48], [50]. It is not always easy to collect enough operation data of a realistic networked system, so information from design and development might be needed.

How to capture the degradation behavior has been studied by many literatures in detail. They mainly focused on estimating the transition probability of multistate Markov chain, subject to full or partial observations from realistic or laboratory networked systems. One popular method to estimate the unknown parameters of the Markov chain is derived from the Maximal Likelihood Estimation method, which is conditional on the starting state of the Markov chain [50]–[53].

Since the Markov chain is used to describe the networked degradation, these methods can be easily generalized to this paper. Therefore, assumption that each period is independent of each other is released. By adopting the difference equations to describe the reliability model, the effect of the transmission delays and packet dropouts on the evolution of system state can be presented more clearly and reliability can be estimated.

Having obtained the stochastic model, it is not trivial to derive the exact reliability function of the DNCSs. Monte Carlo simulation has been proved to be a straightforward, yet accurate approach for such systems [25], [38], [43], [47]. The general approach in Monte Carlo simulation for reliability assessment needs to generate the operational requirements which would lead to the failure of entire system. However, it is not always the case since this would require knowledge of the system requirements-to-failure distribution in advance. Reference [46] first proposes an event-based Monte Carlo simulation method for multicomponent system, in which the failure time for each component is generated and then used to verify the success or failure of the system subject to required operational time. Since no attempt is made on generating the failure time for the entire system and the distribution approximation is at the component level, it can reduce the possible error and computation effort in estimating the system reliability.

Reference [25] extends this method to estimate the reliability of DNCSs and replaces the constraint on the number of replications used by [46], by another two constraints–a precision interval and a percentage of simulations belonging to this interval. The networked degradations are generated and then used to determine the success or failure of the DNCSs for one given combination of operational requirements. Therefore, the reliability of the DNCSs is then estimated as a tabulated function of the operational requirements. The result obtained from [25] can guarantee the estimated reliability to satisfy a given precision compared with the result in [46].

The rest of this paper is organized as follows. Section II presents the preliminary model of the DNCSs and describes the behaviors of the transmission delays and packet dropouts. Section III conducts the analysis of the domain requirements and illustrates the method for evaluating the reliability of the DNCSs. Section IV illustrates the application

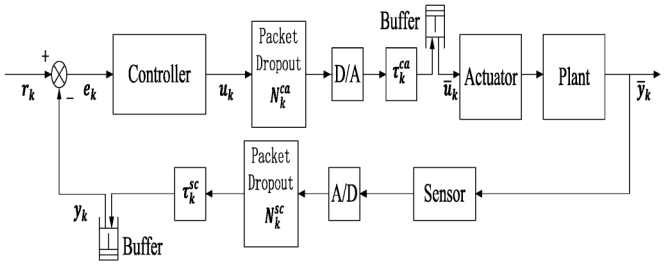


Fig. 2. DNCSs with transmission delays and packet dropouts.

of the proposed framework on an industrial heat exchanger system. Finally, Section V gives the conclusion.

II. Reliability Modeling of the DNCSs

A. Preliminary Model

First, the DNCSs showed in Fig. 2 are considered, where the controller, sensor, actuator and plant are clock-drive with sampling interval T.

In this period, the sensor samples the actual output $\overline{y}_{k-1}$ of the systems at the last period $k-1$ and then sends it to the controller through the communication networks. The buffer at the controller side is assumed to be large enough to store all received data packets which are used to compute the control signal by the controller, according to the last-in–first-out law. If not packet dropout, the buffer can receive the new data packet containing output $\overline{y}_{k-1}$, and then the controller picks it out as y_k and uses in computing the control signal; otherwise, the controller has to pick up the most recent data packet $\overline{y}_{k-N_k^{sc}-1}$ as y_k in the buffer. Thus, the system output recorded by the controller is

$$y_k = \begin{cases} \overline{y}_{k-1}, & \text{if } N_k^{sc} = 0 \\ \overline{y}_{k-N_k^{sc}-1}, & \text{otherwise} \end{cases} \tag{1}$$

where N_k^{sc} is the quantity of packet dropped at the period k in the sensor-to-controller channel, which is recorded from the current period to the last successful packet transmission at the period $k - N_k^{sc}$.

Thus, for the controller-to-actuator channel, the relationship between control signal u_k and the control signal $\overline{u}_k$ used by actuator is given as:

$$\overline{u}_k = \begin{cases} u_k, & \text{if } N_k^{ca} = 0 \\ u_{k-N_k^{ca}}, & \text{otherwise} \end{cases} \tag{2}$$

where N_k^{ca} is the quantity of packet dropped at the period k in the controller-to-actuator channel, which is recorded from the current period k to the last successful packet transmission at the period $k - N_k^{ca}$.

Therefore, the error e_k between the expected system control goal and the actual output of the DNCSs recorded by the controller at the period k is

$$e_k = r_k - y_k \tag{3}$$

where r_k is the expected control goal set at period k.

In this paper, the controller is assumed to use Proportion Integration Differentiation (PID) control strategy to compute the control signal. Therefore, the control signal u_k is given as

$$u_k = K_p \left[e_k + \frac{T}{T_i} \sum_{j=1}^{k} e_j + \frac{T_d}{T}(e_k - e_{k-1}) \right] \tag{4}$$

where K_p is the proportional gain, T_i is the integral time constant and T_d is the derivative time constant.

Since the effects of the transmission delays on the DNCSs are more complicated, the case without transmission delays is considered first. As the sensor measures the system output every period T, the control signal $\overline{u}_k$ remains the same during the interval $[(k-1)T, T]$. Thus, the control signal can be represented by a sum of steps

$$\overline{u}_k = \overline{u}_1 + (\overline{u}_2 - \overline{u}_1) I(t-T) + \cdots + (\overline{u}_k - \overline{u}_{k-1}) I\left(t-(k-1)T\right) + \cdots, t \geq 0 \tag{5}$$

where the $I(t)$ is defined as $I(t) = \begin{cases} 1, & \text{if } t \geq 0 \\ 0, & \text{else} \end{cases}$.

The mathematic representation of the $\overline{u}_k$ in the complex frequency domain $\overline{\mathrm{U}}(\mathrm{s})$ is obtained by Laplace transform

$$\overline{\mathrm{U}}(\mathrm{s}) = \overline{u}_1 + (\overline{u}_2 - \overline{u}_1)\frac{e^{-Ts}}{S} + \cdots + (\overline{u}_k - \overline{u}_{k-1})\frac{e^{-(k-1)Ts}}{s} + \cdots \tag{6}$$

When considering transmission delays τ_k^{sc} and τ_k^{ca} in both channels, the time for the actuator acting according to the control signal $\overline{u}_k$ is $(k-1)T + \tau_k^{sc} + \tau_k^{ca}$. The effects of the transmission delays on the model are introducing a time shifting $e^{-(\tau_k^{sc}+\tau_k^{ca})s}$ in each period. Thus, (6) is modified as

$$\overline{\mathrm{U}}(\mathrm{s}) = \overline{u}_1 e^{-\tau_1^{ca} s} + (\overline{u}_2 - \overline{u}_1)\frac{e^{-(T+\tau_2^{sc}+\tau_2^{ca})s}}{s} + \cdots + \times(\overline{u}_k - \overline{u}_{k-1})\frac{e^{-((k-1)T+\tau_k^{sc}+\tau_k^{ca})s}}{s} + \cdots \tag{7}$$

where τ_1^{sc} equals to 0 as there is no communication in the sensor-to-controller channel at the first period.

As the common mechanism for detecting the packet dropout is checking whether the buffer can receive it before exceeding the maximum allowable transmission time. To develop a more general model, the influence of the transmission delay and packet dropout on each other is further considered. In most current works about DNCSs, there always exists a maximum allowable value of time delay that guarantees the stabilizability of the system. The maximum allowable transmission time is generally assumed to be same as the maximum allowable transmission delay. The time for computing the control signal is negligible, compared to transmission delay. The red point in time axis of Fig. 3 represents the maximum allowable transmission delay in each period.

It is commonly assumed that upon the maximum allowable transmission delay, if the controller or the actuator does not receive the corresponding data packet, to ensure certain degree of real-time control and stabilizability, they would consider that the packet dropout has happened [54], [55]. That is to say, if data packet arrives at the buffer after the maximum allowable transmission time, the buffer will not accept such packet and consider

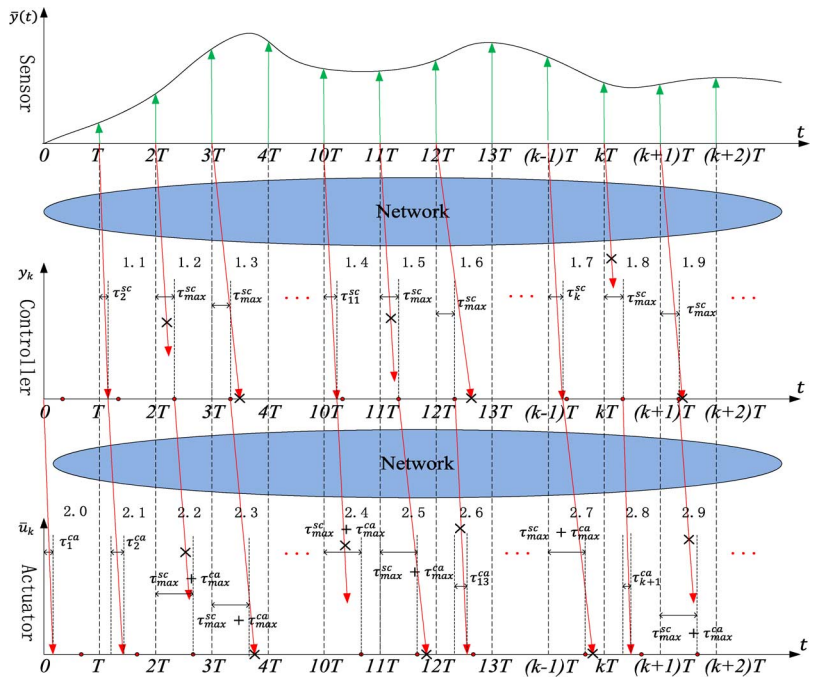


Fig. 3. The activation time of subsystems in DNCSs.

that packet dropout has happened. Therefore, they have to use the last successful transmitted packet to compute control signal or take action [15].

Therefore, there exist three transmission modes for each channel: successful transmission; packet dropout; cannot receive before the maximum allowable transmission time. Also, the exact activation time for controller and actuator can be determined and clarified, as shown in Fig. 3. If the buffer of controller receives data packet before the maximum allowable transmission time, the exact activation time will be $(k-1)T + u_k$ and the controller will send out the control signal immediately, see Arrows 1.1, 1.4 and 1.7 in Fig. 3. Arrows 1.2 and 1.3 give the case that packet dropout and received after maximum allowable transmission time, respectively. For such cases, the buffer does not receive $\overline{y}_{k-1}$ or receive beyond the permissible time $(k-1)T + \tau^{sc}_{\max}$. The exact activation time will be time. The controller will compute and send out the control signal u_k by regarding $\overline{y}_{k-N^{sc}_k-1}$ as y_k according to (1).

From Fig. 3, the exact activation time of the actuator depends on the exact activation time of the controller. For example, if packet dropout happen in the sensor-to-controller channel and the actuator can receive the packet with time τ^{ca}_k less than maximum allowable delay, the exact activation time will be $(k-1)T + \tau^{sc}_{\max} + \tau^{ca}_k$, see Arrows 1.8 and 2.8. Other cases, such as packet dropouts both happen in the sensor-to-controller channel and controller-to-actuator channel, successful transmission in the sensor-to-controller channel and the actuator receives the packet after permissible time, have also been illustrated by Fig. 3.

Assume the mathematic model of actuator and plant are $\mathrm{G_A(s)}$ and $\mathrm{G_P(s)}$, the actual system output $\overline{\mathrm{Y}}(\mathrm{s})$ equals to

$$\overline{\mathrm{Y}}(\mathrm{s}) = \overline{\mathrm{U}}(\mathrm{s})\mathrm{G_A(s)G_P(s)}. \tag{8}$$

Substituting (7) into (8) and applying the inverse Laplace transform, the system output $\overline{y}_k$ in time domain is deduced as

$$\begin{aligned}\overline{y}_k = {} & \overline{u}_1 I\left(t-\tau^{ca}_1\right) g\left(t-t^{ca}_1\right) + \left(\overline{u}_2-\overline{u}_1\right) \\ & I\left(t-T-\tau^{sc}_2-\tau^{ca}_2\right) f\left(t-T-\tau^{sc}_2-\tau^{ca}_2\right)+\cdots \\ & +\left(\overline{u}_k-\overline{u}_{k-1}\right) I\left(t-(k-1)T-\tau^{sc}_k-\tau^{ca}_k\right) \\ & f\left(t-(k-1)T-\tau^{sc}_k-\tau^{ca}_k\right)+\cdots\end{aligned} \tag{9}$$

where $g(t)$ and $f(t)$ are the inverse Laplace transform of $\mathrm{G_A(s)G_P(s)}$ and $\mathrm{G_A(s)G_P(s)/s}$.

Therefore, the system output $\overline{y}_k$ can be obtained by computing (9) with $t = kT$. The model described by the difference equations not only reflects the interactions between system output and control signal, but also shows the influences of the two faults on changing the model parameters. The model directly observes all historical states of DNCSs, different from the model represented by differential equations.

B. Models of Networked Degradations

In this paper, the continuous transmission delays τ^{sc}_k and τ^{ca}_k take place in both channels, showed in Fig. 2. Transmission delays are usually bounded [26], [40], [56]–[59]

$$\tau^{sc}_{\min} \le \tau^{sc}_k \le \tau^{sc}_{\max}, \text{ and } \tau^{ca}_{\min} \le \tau^{ca}_k \le \tau^{ca}_{\max} \tag{10}$$

where $\tau^{sc}_{\min}$ and $\tau^{ca}_{\min}$ are lower bound of the delay which are not zero, and are upper bound, known as the maximum allowable bound [58], [59].

In practice, the transmission delay in each channel can be easily measured by using the time-stamp method. Different from previous models which consider discrete transmission delay as constant or obeying the uniform distribution, the transmission delay are regarded as continuous value. It is more general for practical applications [52], [56], [57].

The τ_k^{sc} and τ_k^{ca} are modeled as Markov process-reflected Wiener process, which take values from predefined bounds in (10). According to the reflection principle of a Wiener process which is based on a symmetry principle, if the path of a Wiener process $w(t)$ reaches a bound B^+ ($\tau_{\max}$ or $\tau_{\min}$) at time $t = t_c$, then the subsequent path after time t_c has the same distribution as the reflection of the subsequent path about the bound [60].

This new process is defined in a stronger form as follows:

$$\widetilde{w}(t) = \begin{cases} w(t), & \text{for } t \le t_c \\ 2B^+ - w(t), & \text{for } t \le t_c \end{cases} \tag{11}$$

where standard Wiener process $w(t)$ has increments with $w(t) - w(s) \sim a\sqrt{t-s}N(0,1)$ for $0 \le s \le t$ and a is the power coefficient. In this paper, the time and can only take value as kT.

It is noticed that there may exist multiple reflections since there may exist lower and upper bound. Right after the reflection, the new process has the probability to reach the other bound B^-. What is more, right after reflected by the other bound, the process can still reach bound B^+ again. Thus, the multireflection case is considered here and (11) should be modified as follows.

For $t \le t_c$

$$\widetilde{w}(t) = w(t).$$

For $\ge t_c$

$$\begin{aligned} \widetilde{w}(t) &= (-1)^v \left[\varphi(v)(v+2) + (1-\varphi(v))\,(v+1)\right] B^+ \\ &-(-1)^v \left[\varphi(v)v + (1-\varphi(v))\,(v+1)\right] B^- - (-1)^v w(t) \end{aligned} \tag{12}$$

where $v = \lfloor |(w(t) - B^+)/(B^+ - B^-)| \rfloor$ and $\lfloor x \rfloor$ stands for the greatest integer which does not exceed x. $\varphi(v)$ is defined as $\varphi(v) = \begin{cases} 1, & \text{if } v \text{ is even number} \\ 0, & \text{otherwise} \end{cases}$.

Here, the modeling of the packet dropouts N_k^{sc} and N_k^{ca} are generally bounded

$$0 \le N_k^{sc} \le N_{\max}^{sc}, \text{ and } 0 \le N_k^{ca} \le N_{\max}^{ca}$$

where $N_{\max}^{sc}$ and $N_{\max}^{ca}$ are nonnegative integers.

In practice, the packet dropout can be detected whether the buffer can receive the data packet before the maximal allowed transmission time. To relax the assumption that packet dropout in each period is independent of others, the packet dropouts are described by two multistate Markov chains [15], [32].

The Markov chains take values in $N_{sc} = \{0, 1, \ldots, N_{\max}^{sc}\}$ and $N_{ca} = \{0, 1, \ldots, N_{\max}^{ca}\}$ with the transition probability matrix $P^{N_{sc}} = [\lambda_{ij}]$ and $P^{N_{ca}} = [\rho_{mn}]$, respectively. The transition probability matrix of N_k^{sc} (jumping from mode i to j) and N_k^{ca} (jumping from mode m to n) are defined as

$$\begin{aligned} \lambda_{ij} &= \Pr\left(N_{k+1}^{sc} = i | N_k^{sc} = j\right) \\ \rho_{mn} &= \Pr\left(N_{k+1}^{ca} = m | N_k^{ca} = n\right) \end{aligned} \tag{13}$$

where $\lambda_{ij} \ge 0$, $i, j \in N_{sc}$, $\rho_{mn} \ge 0$, $m, \mathrm{n} \in N_{ca}$, $\sum_j \lambda_{ij} = 1$ and $\sum_n \rho_{mn} = 1$. According to the definition, the transition probabilities should satisfy

$$\begin{aligned} \lambda_{ij} &= 0 \text{ if } j \ne i+1 \text{ and } j \ne 0 \\ \rho_{mn} &= 0 \text{ if } n \ne m+1 \text{ and } n \ne 0. \end{aligned}$$

The homogenous Markov chains with constant transition probability matrix are only applicable for the case where the statistic information about the packet dropouts is complete known. However, in real applications, due to insufficient observations, the statistic characters of packet dropout are partially known or unknown. Thus, the Markov chain of packet dropout should consider such uncertainties.

The general polytopic uncertainties method is used here to describe the partially unknown transition probability [26], [48], [49].Thus, denote P_i be the ith row of the transition probability matrix P ($P^{N_{sc}}$ and $P^{N_{ca}}$), which is partially unknown but belongs to a convex set with known vertices $P_i^{s_i}$

$$P_i \in \left\{ \sum_{j=1}^{s_i} \alpha_j P_i^j, \sum_{j=1}^{s_i} \alpha_j = 1, \alpha_j \ge 0 \right\} \tag{14}$$

where $P_i^j (j = 1, 2, 3, \ldots, s_i)$ are the vertices of P_i indicating the polytope of the ith row, α_j is the corresponding coefficient indicating the proportion of this vertices on determining the P_i, s_i is the total number of the vertices in the ith row which depends on the number of the unknown or uncertain elements.

For example, consider the following partially known transition probability matrix:

$$P = \begin{bmatrix} 0.3 & 0.4 & ? \\ ? & ? & 0.4 \\ ? & 0.3 & ? \end{bmatrix}$$

One reasonable combination for each row of the uncertain polytope vertices can be determined as

$$\begin{aligned} P_1^1 &= [0.3\ 0.4\ 0.3],\ s_1 = 1 \\ P_2^1 &= [0.6\ 0\ 0.4],\ P_2^2 = [0\ 0.6\ 0.4],\ s_2 = 2 \\ P_3^1 &= [0.7\ 0.3\ 0],\ P_3^2 = [0\ 0.3\ 0.7],\ s_3 = 2 \end{aligned}$$

Therefore, based on (14), P_i can be represented as

$$\begin{aligned} P_1 &= [0.3\ 0.4\ 0.3] = P_1^1 \\ P_2 &= [?\ ?\ 0.4] = \alpha_1 P_2^1 + \alpha_2 P_2^2 \\ &\quad \sum_{i=1}^{2} \alpha_i = 1,\ \alpha_i \ge 0,\ i = 1, 2 \\ P_3 &= [?\ 0.3\ ?] = \beta_1 P_3^1 + \beta_2 P_3^2 \\ &\quad \sum_{j=1}^{2} \beta_j = 1,\ \beta_j \ge 0,\ j = 1, 2 \end{aligned}$$

Remark 1: As illustrated above, if a row has none or one "?", based on the normalization constraint, only one vertices can be generated. Furthermore, if a row contains two or more "?", the same number of vertices is generated.

Remark 2: It should be pointed out that transmission delay and packet dropout has influence on each other, showed by

TABLE I
DOMAIN REQUIREMENTS AND DESCRIPTIONS

Domain requirements		Descriptions
Operational	Maximal Rising/declining time RT_{max}/DT_{max}	The time taken by the system output to rise from a specified low/high value to a specified high/low value.
	Maximal percentage overshoot PO_{max}	The maximal value of the system output minus the expected system output divided by the expected system output.
	Maximal settling time ST_{max}	The time elapsed from the application of the control goal to the time at which the system output has entered and remained within a specified error band.
Nonfunctional	Reliability	The ability of the DNCSs to maintain the expected performance in the presence of the faults.

Fig. 3. If the value of transmission delay is maximum allowable delay, packet dropout will happen and *vice versa*. If there is no maximum allowable delay or packet dropout happening in the channels, their state transitions will follow their Wiener process or Markov chain, based on (11)–(14). Such cases can be represented by

$$\begin{aligned} \Pr\left(\tau_k^{sc} = \tau_{max}^{sc} | N_k^{sc} > 0\right) &= 1 \\ \Pr\left(N_k^{sc} = N_{k-1}^{sc} + 1 | \tau_k^{sc} = \tau_{max}^{sc}\right) &= 1 \\ \Pr\left(\tau_k^{ca} = \tau_{max}^{ca} | N_k^{ca} > 0\right) &= 1 \\ \Pr\left(N_k^{ca} = N_{k-1}^{ca} + 1 | \tau_k^{ca} = \tau_{max}^{ca}\right) &= 1. \end{aligned} \tag{15}$$

III. PERFORMANCE ANALYSIS OF THE DNCSS

A. Domain Requirement Analysis

Table I summarizes the domain requirements considered in the performance analysis of the DNCSs. As showed in Table I, the performance of the DNCSs needs to satisfy many important domain requirements, especially the requirements relevant to the real-time operation. However, it still needs to maintain a high level of reliability to satisfy the nonfunctional requirement.

For the single-control goal problem, the failure of the DNCSs is defined as the performance cannot satisfy all operational requirements

$$\mathrm{P}(x=0) = \mathrm{P}(\mathrm{PF} > RT_{\max} \cup \mathrm{PF} > PO_{\max} \cup \mathrm{PF} > ST_{\max}) \tag{16}$$

where PF stands for the performance of the system output and $x = 0$ means the DNCSs fails in a simulation.

The sequential-control goal problem consists of several sequential control goals which all need to be satisfied. Each control goal has corresponding operational requirements.

In this paper, the entire operation time is divided into several time slices according to the time domain of each control goal. Then, whether the DNCSs with M control goals fails or not in a simulation can be determined by following

$$\mathrm{P}(\mathrm{X} = 0) = \mathrm{P}(x_1 = 0 \cup x_2 = 0 \cup \ldots \cup x_{\mathrm{M}} = 0) \tag{17}$$

where $\mathrm{P}(x_i = 0)(i \in \{1, 2, \ldots, \mathrm{M}\})$ is determined by (16), and means that the DNCSs with sequential-control goal fails in a simulation.

B. Evaluation of the Nonfunctional Requirement-Reliability

As defined in the domain requirements, the reliability is related to the ability of the DNCSs to maintain the expected performance in the presence of the faults. The Monte Carlo simulation is applicable to estimate this ability under different situations of the faults, without knowing the reliability function of system in advance. Since the faults are probabilistic and the success or failure of the DNCSs is determined by (16) or (17), an event-based Monte Carlo simulation is introduced here to obtain a degree of confidence of the estimated reliability of DNCSs, subject to performance requirements.

In this paper, the event-based Monte Carlo method derived from [25] has two main parameters–a precision interval and a percentage of simulations belonging to this interval. When a new simulation marked is conducted, this simulation fails or not are determined by (16) or (17). Then, the reliability of the DNCSs-R_j is updated, which is determined by the number of failed simulations and the total number of simulations

$$R_j = 1 - \frac{N_f}{N_t}. \tag{18}$$

If the difference between two consecutive simulations $d_j = R_j - R_{j-1}$ is within this interval, the simulation s_j is effective and the number of simulations belonging to this interval N_e increases 1. When the percentage of simulations belonging to this interval N_e/N_t exceeds a nominal threshold, the simulation is terminated and the final reliability of the DNCSs is obtained, with required precision. A precision interval $\pm 2\%$ and 95% of simulations belonging to this interval means that 95% of d_j belongs to $\pm 2\%$ of R_{j-1}.

IV. AN APPLICATION EXAMPLE

In this paper, an industrial heat exchanger system used in the chemical industry and power plants is given to illustrate the application of the proposed framework [41], [42]. Fig. 4 shows a typical industrial heat exchanger digital networked control system, which consists of a control valve, a controller, a stirring tank reactor, a heat exchanger, a temperature sensor, an electric boiler and the communication networks.

A. System Description and Mathematical Model

The top inlet pipe delivers fluid to be reacted in the stirring tank. In order to promote the chemical reactions, the controller needs to maintain the temperature of the liquid in the tank to a constant value by adjusting the amount of steam supplied to the heat exchanger (bottom pipe) via controlling the control valve. Details of the subsystems are:

- Control Valve: is the actuator and implements the decisions from controller. The electropneumatic globe valve aperture is installed here and adjusts the steam flow through an orifice by controlling the plug appropriately. The capacity is 1.6 kg/s for steam flow and the control valve can be throttled from 5% to 95% open which has linear relationship

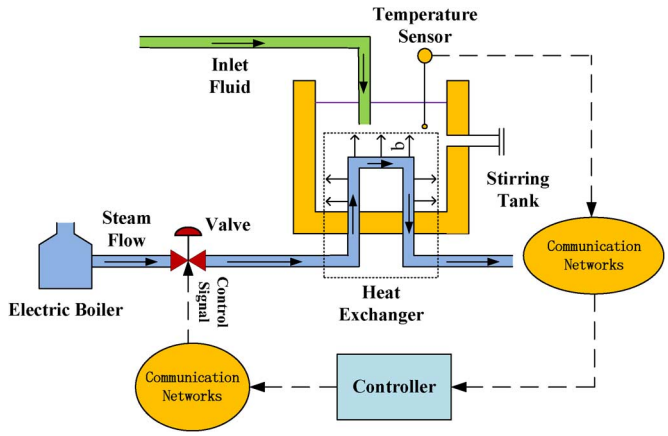


Fig. 4. The structure of industrial heat exchanger system.

with capacity. The time constant is 3 s. The gain of control valve is 1 and thus the mathematic model $\mathrm{G_A(s)}$ is $1/3s + 1$.

- Heat Exchanger: is the controlled plant. In the heat exchanger, the fluid flows into stirring tank with constant velocity and is heated by steam from electric boiler. The response gain of fluid in stirring tank to steam flow is 5° C/(kg/s) and the time constant is 10 s. Thus, the mathematical model of heat exchanger $\mathrm{G_P(s)}$ is $5/10\ \mathrm{s} + 1$.
- Temperature Sensor: In this case study, a three-wire PT-100 RTD with a range of −200 °C to 600 °C is adopted here and samples the temperature of fluid every 0.5 s. It can withstand high temperature with excellent stability. The feedback mechanism is unity negative feedback.
- Electric Boiler: Constant temperature steam is generated at a rate–4 kg/s (maximal capacity) with a pressure which oscillates 7 and 10 bar.
- Controller: maintains the operational requirements of the temperature of the fluid in the stirring tank by throttling the control valve. The control signal of the position of the control valve is computed based on the PID strategy. The parameters will be provided in the section-"reliability analysis."
  Thus, the overall transfer function of the control process is $\mathrm{G(s)} = \mathrm{G_A(s)G_P(s)} = 5/30\ s^2 + 13\ s + 1$.
  And, $g(t) = (5/7) \times (e^{t/10} - e^{t/3})$, $f(t) = (15/7) \times e^{10(t/3)} + (50/7) \times e^{3(t/10)} + 5$ and $T = 0.5$ s can be computed for (9).
- Communication Networks: are based on the single-packet transmission protocol. The single-packet transmission refers to sample data or control signal is compressed into one packet and transmitted. Single-packet transmission is common in the communication networks with large packet size, e.g., WLAN (802.11) which can hold a maximum of 7981 B of data in a single packet and Ethernet which can hold a maximum of 1500 B of data in a single packet.

The existing degradation models which make use of information from design or development are acceptable in the study of reliability of DNCSs.

The transmission delays (ms) for both channels are

$$\tau_{\min}^{sc} = 10,\ \tau_{\max}^{sc} = 60,\ a_{sc} = 25$$
$$\tau_{\min}^{ca} = 10,\ \tau_{\max}^{ca} = 50 \text{ and } a_{ca} = 20$$

where $\sqrt{t-s} = T = 0.5$, a_{sc} and a_{ca} is the power coefficient based on (11).

Packet dropout $N_{sc} = \{0, 1, 2\}$ and $N_{ca} = \{0, 1, 2, 3\}$ have uncertain transition probability matrix as

$$P^{N_{sc}} = \begin{bmatrix} ? & ? & 0 \\ 0.7 & 0 & 0.3 \\ 1 & 0 & 0 \end{bmatrix} \text{ and } P^{N_{ca}} = \begin{bmatrix} ? & ? & 0 & 0 \\ 0.75 & 0 & 0.25 & 0 \\ ? & 0 & 0 & ? \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Based on (14), N_{sc} is represented by

$$P_1^1 = [1\ 0\ 0],\ P_1^2 = [0\ 1\ 0],\ s_1 = 2$$
$$P_1 = [?\ ?\ 0] = \alpha_1 P_1^1 + \alpha_2 P_1^2.$$

For N_{ca}, it can be determined by

$$P_1^1 = [1\ 0\ 0\ 0],\ P_1^2 = [0\ 1\ 0\ 0],\ s_1 = 2$$
$$P_1 = [?\ ?\ 0\ 0] = \alpha_1 P_1^1 + \alpha_2 P_1^2$$
$$P_3^1 = [1\ 0\ 0\ 0],\ P_3^2 = [0\ 0\ 0\ 1],\ s_3 = 2$$
$$P_3 = [?\ 0\ 0\ ?] = \beta_1 P_3^1 + \beta_2 P_3^2.$$

This representation has advantage on further topics about parameter estimation and reliability optimization. When focusing on the effects of networked degradations on system reliability, the degradations can be designed as: for N_{sc}, $\alpha_1 = 0.9$ and $\alpha_2 = 0.1$; for N_{ca}, $\alpha_1 = 0.85$, $\alpha_2 = 0.15$, $\beta_1 = 0.6$ and $\beta_2 = 0.4$.

Thus, the transition probability matrix can be determined as

$$P^{N_{sc}} = \begin{bmatrix} 0.9 & 0.1 & 0 \\ 0.7 & 0 & 0.3 \\ 1 & 0 & 0 \end{bmatrix}, P^{N_{ca}} = \begin{bmatrix} 0.85 & 0.15 & 0 & 0 \\ 0.75 & 0 & 0.25 & 0 \\ 0.6 & 0 & 0 & 0.4 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

B. Reliability Analysis

1) Case 1: In this case, the reliability of the DNCSs with single-control goal is studied. The initial temperature of the inlet fluid is 25 °C and the optimal reaction temperature is 28 °C. In order to ensure a satisfied reaction environment for the chemical process, the heating process needs to make the fluid have a 3 °C temperature increment in 30 s and satisfies following operational requirements:

- Maximal rising time: the time for the temperature increment rising from 10% and 90% of the expected temperature increment 3 °C is 9 s.
- Maximal percentage overshoot $PO_{\max}$: the maximal the temperature increment should not exceed 26% of expected temperature increment.
- Maximal settling time $ST_{\max}$: the time for the temperature increment has entered and remained within +5% of the expected temperature increment 3 °C is 24 s.

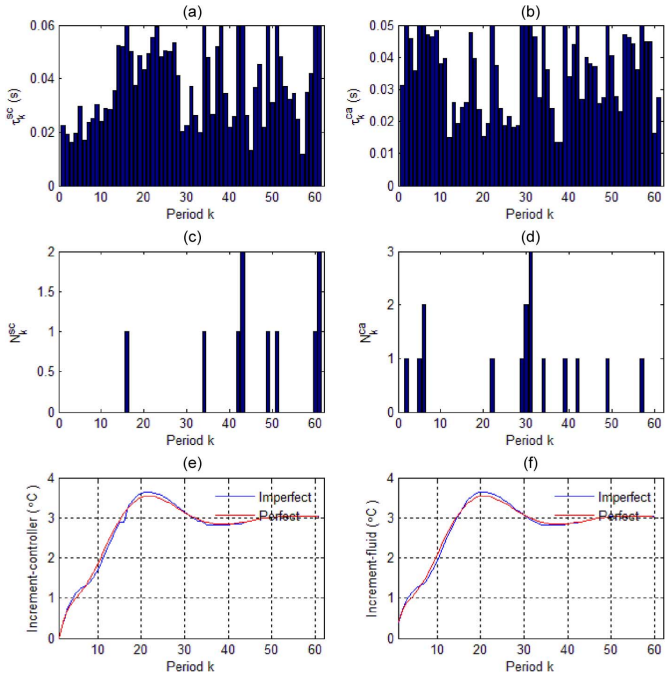


Fig. 5. Tracking performance of the industrial heat exchanger system.

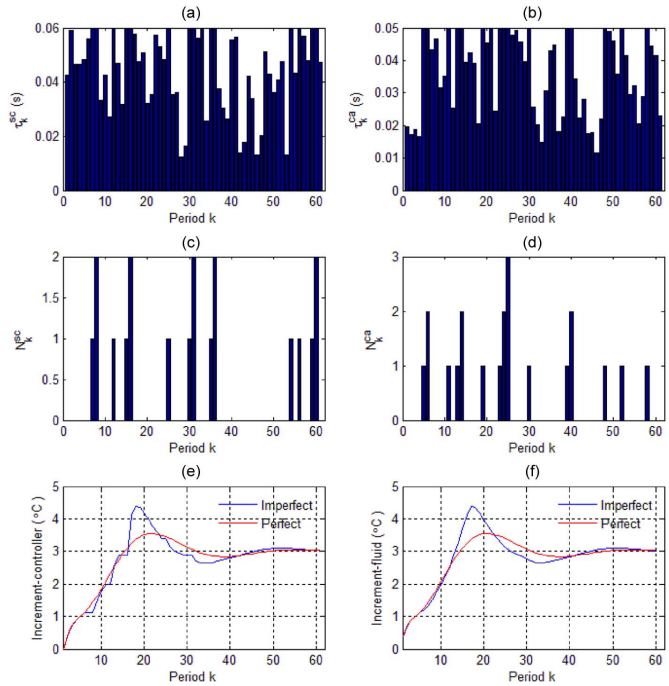


Fig. 6. Tracking performance of the industrial heat exchanger system.

The parameters of PID control strategy are computed as $K_p = 1.7$, $T_i = 2.5$ and $T_d = 2$ to satisfy above operational requirements without considering networked degradations. The performances of the industrial heat exchanger system with perfect communication networks are, $RT = 6.0$ s, $PO = 18.1\%$ and $ST = 19.8$ s. Thus, the predesign PID control strategy is able to ensure a required quality of the heating process.

With above PID controller and the proposed framework in this paper, Fig. 5 shows the real-time performances of industrial heat exchanger system at a random simulation run. Fig. 5(a) and (b) gives the distributions of transmission delay of each period in both channels. Fig. 5(c) and (d) gives the changes in packet dropout numbers in both channels. Fig. 5(e) shows the temperature increment recorded by the controller and Fig. 5(f) shows the tracking performance of the heating process, represented by the temperature increment of the fluid. The operational performances of the heating process are $RT = 5.8$ s, $PO = 21.3\%$ and $ST = 20.7$ s, which all satisfy the operational requirements. Therefore, the DNCSs in this random simulation are successful in delivering expected performance based on (16), even though there exist performance degradations in communication networks. However, compared with the performances of the heating process with perfect communication networks, see Fig. 6(e) and (f), the transmission delays and packet dropouts cause obvious degradation in the real-time performance. The essential reason is that the delayed or lost data makes the controller unable to obtain the actual state of the heating process and leads to the heating process under false control signal or out of control.

Fig. 6 shows the real-time performances of the industrial heat exchanger system at another random simulation run. The actual performances of the heating process are $RT = 5.4$ s, $PO = 46.4\%$ and $ST = 20.4$ s, which do not meet the operational requirement-maximal percentage overshoot. Based on (16), it can be concluded that the DNCSs in this simulation fail and the heating process is of bad quality to ensure a satisfied chemical reaction. Fig. 6(e) and (f) show that the temperature increment is dramatically changed which is caused by severe transmission delays and packet dropouts.

It is also noticed that Figs. 5 and 6 show the relationship between transmission delay and packet dropout. If there is packet dropout happening, the delay should always equal to maximum allowable transmission delay and *vice versa*. These relationships have been illustrated by Fig. 3 and formula (15). Aforementioned analysis emphasizes that it is critical to maintain a high level of reliability to increase the ability of the DNCSs to tolerate the degradations and be error-free, so as to satisfy operational requirements in most situations of the communication networks. Since above discussions have also showed that the system fails or is not probabilistic, with the event-based Monte Carlo method, the reliability of the heat exchanger system can be estimated.

Table II gives the reliability analysis of the industrial heat exchanger system subject to different operational requirements with a precision interval $\pm 2\%$ and 98% of simulations belonging to this interval. 0.6360 indicates that the DNCSs in the case study have 63.60% probability to ensure the system output to satisfy the operational requirement-maximal settling time. 0.7775 indicates that the DNCSs have 77.75% probability to fulfill all operational requirements.

The second line shows that the DNCSs have very low ability to maintain the real-time performances which are achieved in the case where there are no networked degradations. It can be concluded that the networked degradations have significant influence on system reliability. When more strict operational requirements are imposed on the DNCSs, the ability of the DNCSs to maintain expected system output decreases sharply.

TABLE II
RELIABILITY ANALYSIS OF THE INDUSTRIAL HEAT EXCHANGER SYSTEM

Operational Requirements	*RT*	*PO*	*ST*	*RT* ∪ *PO* ∪ *ST*
[6s,18.1%,19.8s]	0.6139	0.1782	0.2673	0.0495
[7s,22%,22s]	0.9945	0.6340	0.8355	0.6248
[9,26%,24s]	1	0.7420	0.8382	0.7277
[11s,30%,26s]	1	0.8051	0.9613	0.7945
[13s,34%,28s]	1	0.8201	0.9869	0.8176

TABLE III
OPERATIONAL REQUIREMENT FOR EACH CONTROL GOAL

Operational Requirements	Goal 1	Goal 2	Goal 3
RT_{max}	9s	9s	9s
PO_{max}	15%	20%	25%
ST_{max}	20s	25s	30s

From Table II, the ability of the DNCSs to make real-time performance satisfying all three operational requirements is closest to the ability of the DNCSs to make system performance only satisfying the requirement-maximal percentage overshoot. Based on (16), the smallest one will become the bottleneck in evaluating and improving system reliability. Therefore, based on this criterion, the percentage overshoot is the most critical one in determining the reliability of the DNCSs among the three operational requirements.

2) Case 2: In this case, the reliability of the DNCSs with sequential-control goal is studied. The initial temperature of the inlet fluid is 25 °C. The first control goal is that the DNCSs need to have an optimal reaction temperature–27 °C in 30 s. The second control goal is that in the next 30 s, the optimal reaction temperature needs to be decreased to 26 °C. The third control goal is that in the next 40 s, the optimal reaction temperature needs to be increased to 28 °C.

Thus, there are three sequential control goals in total operation time 100 s (the number of period is 200). If all the three control goals cannot be satisfied, the DNCSs will be regarded as unable to maintain expected performance, based on (17). The operational requirements for each control goal are shown in Table III. For the second goal, the $RT_{\max} = 9$ s indicates that it needs the temperature decreases from 27 °C to 26.1 °C in 9 s in the second time domain–30 s, that is 39 s of the total operation time. For the third control goal, the $PO_{\max} = 25\%$ means that the maximal temperature increment minus the expected increment 2 °C divided by the expected increment 2 °C should not exceed 25%.

The parameters of PID control strategy have been computed in advance which are $K_p = 1.5$, $T_i = 10/3$, and $T_d = 1.8$.

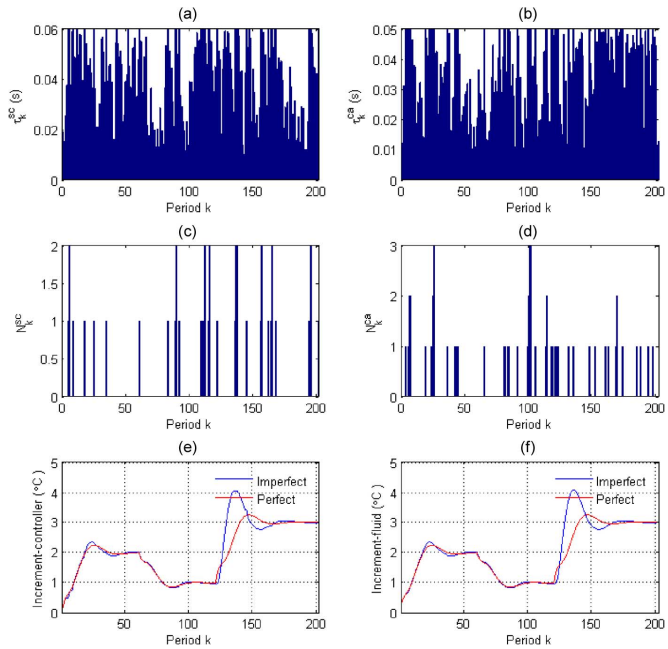


Fig. 7. Tracking performance of the industrial heat exchanger system.

The system performance can satisfy above operational requirements under perfect communication networks. And the operational performances of each control goal without considering networked degradations are $RT_1 = 7.2$ s, $PO_1 = 12.1\%$ and $ST_1 = 16.7$ s; $RT_2 = 7.6$ s, $PO_2 = 12.5\%$ and $ST_2 = 17.1$ s; $RT_3 = 7.6$ s, $PO_3 = 12.4\%$ and $ST_3 = 17.1$ s. Therefore, the predesign PID control strategy is capable to ensure the quality of the heating process with sequential-control goal.

When considering the networked degradations, the real-time performances will have significant performance degradations and the ability of the DNCSs to maintain expected performance will be affected. Fig. 7 shows the real-time performances of industrial heat exchanger system for one random simulation. The operational performances for three control goals are $RT_1 = 7.0$ s, $PO_1 = 17.5\%$ and $ST_1 = 21.3$ s; $RT_2 = 7.6$ s, $PO_2 = 16.6\%$ and $ST_2 = 16.2$ s; $RT_3 = 2.4$ s, $PO_3 = 55.3\%$ and $ST_3 = 21.1$. Base on (16), the heating process does not satisfy the maximal percentage overshoot and maximal settling time of the first control goal and maximal percentage overshoot of the third control goal. Therefore, the DNCSs in this simulation fail to deliver expected performance according to (17). In Fig. 7(e) and (f), an abrupt rise in the temperature increment exists because of the severe packet dropouts at the time domain of the third control goal. The continuous loss of the sample forces the controller to take the previous information to make decisions. Eventually, the real-time performance obviously exceeds the operational requirements of the third control goal.

Based on the event-based Monte Carlo simulation method, the system reliability and detailed information about the DNCSs subject to sequential-control goal are obtained. Table IV presents the reliability analysis of the industrial heat exchanger system as a tabulated function of different operational requirements with a precision interval ±2% and of simulations belonging to this interval.

TABLE IV
RELIABILITY ANALYSIS OF THE INDUSTRIAL HEAT EXCHANGER SYSTEM

Operational Requirements	[7.2s,12.1%,16.7s]; [7.6s,12.5%,17.1s]; [7.6s,12.4%,17.1s]	[8s,13%,18s]; [8s,16%,22s]; [8s,18%,24s]	[9s,15%,20s]; [9s,20%,25s]; [9s,25%,30s]	[10s,17%,22s]; [10s,24%,28s]; [10s,32%,36s]
RT_1	0.7822	0.9886	1	1
PO_1	0.1485	0.3568	0.6543	0.7351
ST_1	0.5545	0.7060	0.7766	0.9171
Goal 1	0.0693	0.3321	0.6273	0.7110
RT_2	0.7525	0.9467	0.9959	1
PO_2	0.1485	0.6584	0.7766	0.8072
ST_2	0.5842	0.8877	0.9841	0.9954
Goal 2	0.0396	0.5956	0.7719	0.8059
RT_3	0.7426	0.9600	1	1
PO_3	0.1683	0.7165	0.8213	0.8172
ST_3	0.4554	0.9762	0.9994	1
Goal 3	0.0198	0.6727	0.8213	0.8172
Reliability	0	0.1446	0.3986	0.4744

For example, [9 s, 15%, 20 s], [9 s, 20%, 25 s], and [9 s, 25%, 30 s] are the operational requirements of the three control goals, which have the same meanings illustrated by Table III. 0.6543 of this row indicates that the designed DNCSs have 65.43% probability to satisfy the requirement-maximal percentage overshoot of the first control goal. 0.7719 indicates that the DNCSs have 77.19% probability to fulfill all operational requirements of the second control. Thus, 0.3986 indicates that the ability of the DNCSs to make the system performances satisfy all operational requirements of the all three control goals is 39.86% out of 100%. Therefore, the system reliability is defined as 0.3986.

When taking into account the networked degradations, the predesign DNCSs have zero possibility to maintain the same performance which can all be obtained in the case of perfect communication networks, see the second row of Table IV. When setting less strict operational requirements, the ability of the DNCSs to maintain expected performances increases.

V. CONCLUSION

In this paper, stochastic model of the DNCSs is improved from two aspects. One is applying Markov process-reflected Wiener process to describe the continuous time delays and using independent homogenous Markov Chains to model the behaviors of packet dropouts. The other one is applying the difference equations to describe the stochastic model of the DNCSs. This novel model not only releases the assumption that the behaviors of faults in one period are independent from other periods, but also provides better evolution of the real-time system performance. The influence of the transmission delays and packet dropouts on the DNCSs can be clearly tracked.

The domain requirement analysis consists of operational requirements and nonfunctional requirements. The DNCSs conducting certain tasks are considered to be a failure if the dynamic performances do not satisfy all operational requirements. The nonfunctional requirement-reliability quantitatively defines the ability of the DNCSs to deliver expected operational performance at the presence of the degraded communication networks. A statistical approach is used to estimate such value which is derived from event-based Monte Carlo simulation method. The proposed reliability assessment method is applicable for general cases, regardless of the different structures of DNCSs.

The application example shows that the imperfect communication networks degrade the dynamic performance of the DNCSs. The reliability is dynamic and changing with the operational requirements. Future works could be aimed at the optimal parameter design of the control strategy to improve the reliability of the DNCSs subject to different operational requirements. Also, data-driven modeling methods can be applied here to get a better description of the networked degradations. The proposed framework has potential in solving the reliability problems related to more general systems, especially the nonlinear control systems.

ACKNOWLEDGMENT

The authors would like to thank the editor and the anonymous referees for their constructive comments and suggestions which led to substantial improvement of this paper.

REFERENCES

[1] J. Yao, X. Liu, G. Zhu, and L. Sha, "NetSimplex: Controller fault tolerance architecture in networked control systems," *IEEE Trans. Ind. Informat.*, vol. 9, no. 1, pp. 346–356, Feb. 2013.

[2] M. Das, R. Ghosh, B. Goswami, A. Gupta, A. Tiwari, and R. Balasubrmanian *et al.*, "Network control system applied to a large pressurized heavy water reactor," *IEEE Trans. Nucl. Sci.*, vol. 53, no. 5, pp. 2948–2956, Oct. 2006.

[3] J. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–162, Jan. 2007.

[4] I. Tejado, S. HosseinNia, B. Vinagre, and Y. Chen, "Efficient control of a smart wheel via Internet with compensation of variable delays," *Mechatronics*, vol. 23, no. 7, pp. 821–827, Oct. 2013.

[5] H. Fang, H. Ye, and M. Zhong, "Fault diagnosis of networked control systems," *Annu. Rev. Control*, vol. 31, no. 1, pp. 55–68, 2007.

[6] C. Aubrun, D. Sauter, and J. Yame, "Fault diagnosis of networked control systems," *Int. J. Ap. Mat. Com-Pol.*, vol. 18, no. 4, pp. 525–537, Dec. 2008.

[7] H. Kang and T. Sung, "An analysis of safety-critical digital systems for risk-informed design," *Reliab. Eng. Syst. Safe.*, vol. 78, no. 3, pp. 307–314, Dec. 2002.

[8] S. Authen and J. E. Holmberg, "Reliability analysis of digital systems in a probabilistic risk analysis for nuclear power plants," *Nucl. Eng. Technol.*, vol. 44, no. 5, pp. 471–482, Jun. 2012.

[9] A. Ahmadi, F. Salmasi, M. Noori-Manzar, and T. Najafabadi, "Speed sensorless and sensor-fault tolerant optimal PI regulator for networked DC motor system with unknown time-delay and packet dropout," *IEEE Trans. Ind. Electron.*, vol. 61, no. 2, pp. 708–717, Feb. 2014.

[10] S. Chai, G. Liu, D. Rees, and Y. Xia, "Design and practical implementation of internet-based predictive control of a servo system," *IEEE Trans. Control Syst. Technol.*, vol. 16, no. 1, pp. 158–168, Jan. 2008.

[11] Y. Kang, Z. Li, X. Cao, and D. Zhai, "Robust control of motion/force for robotic manipulators with random time delays," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1708–1718, Sep. 2013.

[12] H. Zhang, Y. Shi, and A. Mehr, "Robust static output feedback control and remote PID design for networked motor systems," *IEEE Trans. Ind. Electron.*, vol. 58, no. 12, pp. 5396–5405, Dec. 2011.

[13] N. Kottenstette, J. Hall, X. Koutsoukos, J. Sztipanovits, and P. Antsaklis, "Design of networked control systems using passivity," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 3, pp. 649–665, May 2013.

[14] K. Kim and P. Kumar, "Real-time middleware for networked control systems and application to an unstable system," *IEEE Trans. Control Syst. Technol.*, vol. 21, no. 5, pp. 1898–1906, Sep. 2013.

[15] J. Wu and T. Chen, "Design of networked control systems with packet dropouts," *IEEE Trans. Autom. Control*, vol. 52, no. 7, pp. 1314–1319, Jul. 2007.

[16] A. Al-Dabbagh and L. X. Lu, "Reliability modeling of networked control systems using dynamic flowgraph methodology," *Reliab. Eng. Syst. Safe.*, vol. 95, no. 11, pp. 1202–1209, Nov. 2010.

[17] F. Lian, J. Moyne, and D. Tilbury, "Network design consideration for distributed control systems," *IEEE Trans. Control Syst. Technol.*, vol. 10, no. 2, pp. 297–307, Mar. 2002.

[18] W. Kim, K. Ji, and A. Ambike, "Real-time operating environment for networked control systems," *IEEE Trans. Autom. Sci. Eng.*, vol. 3, no. 3, pp. 287–296, Jul. 2006.

[19] D. Zhang, Q. Wang, L. Yu, and Q. Shao, "H-infinity filtering for networked systems with multiple time-varying transmissions and random packet dropouts," *IEEE Trans. Ind. Informat.*, vol. 9, no. 3, pp. 1705–1716, Aug. 2013.

[20] H. Li and Y. Shi, "Networked min-max model predictive control of constrained nonlinear systems with delays and packet dropouts," *Int. J. Control*, vol. 86, no. 4, pp. 610–624, Apr. 2013.

[21] L. Schenato, "Optimal estimation in networked control systems subject to random delay and packet drop," *IEEE Trans. Autom. Control*, vol. 53, no. 5, pp. 1311–1317, Jun. 2008.

[22] N. Chaudhuri, D. Chakraborty, and B. Chaudhuri, "Damping control in power systems under constrained communication bandwidth: A predictor corrector strategy," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 1, pp. 223–231, Jan. 2012.

[23] M. Yau, S. Guarro, and G. Apostolakis, "Demonstration of the dynamic flowgraph methodology using the Titan-II space launch vehicle digital flight control-system," *Reliab. Eng. Syst. Safe.*, vol. 49, no. 3, pp. 335–353, 1995.

[24] K. Bjorkman, "Solving dynamic flowgraph methodology models using binary decision diagrams," *Reliab. Eng. Syst. Safe.*, vol. 111, pp. 206–216, Mar. 2013.

[25] R. Ghostine, J. Thiriet, and J. Aubry, "Variable delays and message losses: Influence on the reliability of a control loop," *Reliab. Eng. Syst. Safe.*, vol. 96, no. 1, pp. 160–171, Jan. 2011.

[26] H. Zhang, Y. Shi, and J. Wang, "Observer-based tracking controller design for networked predictive control systems with uncertain Markov delays," *Int. J. Control*, vol. 86, no. 10, pp. 1824–1836, Oct. 2013.

[27] M. Yu, L. Wang, T. Chu, and F. Hao, "Stabilization of networked control systems with data packet dropout and transmission delays: Continuous-time case," *Eur. J. Control*, vol. 11, no. 1, pp. 40–49, 2005.

[28] Y. Zhang and H. Fang, "Stabilization of nonlinear networked systems with sensor random packet dropout and time-varying delay," *Appl. Math. Model*, vol. 35, no. 5, pp. 2253–2264, May 2011.

[29] Y. Guo and T. Pan, "Robust stability of uncertain systems over network with bounded packet loss," *J. Appl. Math.*, 2012.

[30] P. Seiler and R. Sengupta, "An H (infinity) approach to networked control," *IEEE Trans. Autom. Control*, vol. 50, no. 3, pp. 356–364, Mar. 2005.

[31] R. Yang, G. Liu, P. Shi, C. Thomas, and M. Basin, "Predictive output feedback control for networked control systems," *IEEE Trans. Ind. Electron.*, vol. 61, no. 1, pp. 512–520, Jan. 2014.

[32] B. Zhang and W. Zheng, "H-infinity filter design for nonlinear networked control systems with uncertain packet-loss probability," *Signal Process.*, vol. 92, no. 6, pp. 1499–1507, Jun. 2012.

[33] F. Yang and Q. Han, "H-infinity control for networked systems with multiple packet dropouts," *Inf. Sci.*, vol. 252, pp. 106–117, Dec. 2013.

[34] P. Chen and S. Gao, "Observer-based feedback stabilization of networked control systems with random packet dropouts," *Math. Probl. Eng.*, vol. 2013, Article ID 218682, 7 pages, 2013.

[35] Y. Zhao, G. Liu, and D. Rees, "Design of a packet-based control framework for networked control systems," *IEEE Trans. Control Syst. Technol.*, vol. 17, no. 4, pp. 859–865, Jul. 2009.

[36] L. Cauffriez, J. Ciccotelli, B. Conrard, and M. Bayart Ciame, "Design of intelligent distributed control systems: A dependability point of view," *Reliab. Eng. Syst. Safe.*, vol. 84, no. 1, pp. 19–32, Apr. 2004.

[37] J. Clarhaut, B. Conrard, S. Hayat, and V. Cocquempot, "Optimal design of dependable control system architectures using temporal sequences of failures," *IEEE Trans. Reliab.*, vol. 58, no. 3, pp. 511–522, Sep. 2009.

[38] L. Cauffriez, V. Benard, and D. Renaux, "A new formalism for designing and specifying RAMS parameters for complex distributed control systems: The safe-SADT formalism," *IEEE Trans. Reliab.*, vol. 55, no. 3, pp. 397–410, Sep. 2006.

[39] H. Karimi, N. Duffie, and S. Dashkovskiy, "Local capacity H infinity control for production networks of autonomous work systems with time-varying delays," *IEEE Trans. Autom. Sci. Eng.*, vol. 7, no. 4, pp. 849–857, Oct. 2010.

[40] L. Zhang, Y. Shi, T. Chen, and B. Huang, "A new method for stabilization of networked control systems with random delays," *IEEE Trans. Autom. Control*, vol. 50, no. 8, pp. 1177–1181, Aug. 2005.

[41] A. Vidal and A. Banos, "Reset compensation for temperature control: Experimental application on heat exchangers," *Chem. Eng. J.*, vol. 159, no. 1–3, pp. 170–181, May 2010.

[42] C. Sharma, S. Gupta, and V. Kumar, "Modeling and simulation of heat exchanger used in soda recovery," in *Proc. WCE*, London, U.K., Jul. 6–8, 2011, vol. II.

[43] H. Xiao, L. Lee, and K. Ng, "Optimal computing budget allocation for complete ranking," *IEEE Trans. Autom. Sci. Eng.*, vol. 11, no. 2, pp. 516–524, Apr. 2014.

[44] J. Yuan, S. Ng, and K. Tsui, "Calibration of stochastic computer models using stochastic approximation methods," *IEEE Trans. Autom. Sci. Eng.*, vol. 10, no. 1, pp. 171–186, Jan. 2012.

[45] X. Si and D. Zhou, "A generalized result for degradation model-based reliability estimation," *IEEE Trans. Autom. Sci. Eng.*, vol. 11, no. 2, pp. 632–637, Apr. 2012.

[46] J. Kamat and W. Riley, "Determination of reliability using event-based Monte Carlo simulation," *IEEE Trans. Reliab.*, vol. 24, no. 1, pp. 73–75, Apr. 1975.

[47] W. Yeh, Y. Li, Y. Chung, and M. Chih, "A particle swarm optimization approach based on Monte Carlo simulation for solving the complex network reliability problem," *IEEE Trans. Reliab.*, vol. 59, no. 1, pp. 212–221, Mar. 1975.

[48] L. Li and L. Zhong, "Generalised nonlinear $l_2 - l_\infty$ filtering of discrete-time Markov jump descriptor systems," *Int. J. Control*, vol. 87, no. 3, pp. 653–664, Mar. 4, 2014.

[49] A. Goncalves, A. Fioravanti, and J. Geromel, "Filtering of discrete-time Markov jump linear systems with uncertain transition probabilities," *Int. J. Robust Nonlin. Control*, vol. 21, no. 6, pp. 613–624, Apr. 2011.

[50] J. Nilsson, "Real-time control systems with delays," Ph.D. dissertation, Dept. Autom. Control, Lund Inst. Technol., Lund, Sweden, Jan. 1998.

[51] O. Aalen, "Nonparametric estimation of partial transition probabilities in multiple decrement models," *Ann. Stat.*, vol. 6, no. 3, pp. 534–545, 1978.

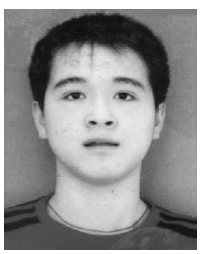
[52] J. Zhang and J. Chen, "Neural PID control strategy for networked process control," *Math. Probl. Eng.*, vol. 2013, 2013.

[53] H. Baik, H. S, and D. Abraham, "Estimating transition probabilities in Markov chain-based deterioration models for management of wastewater systems," *J. Water Res. PL-ASCE.*, vol. 132, no. 1, pp. 15–24, Jan. 2006.

[54] R. Yang, P. Shi, and G. Liu, "Filtering for discrete-time networked nonlinear systems with mixed random delays and packet dropouts," *IEEE Trans. Autom. Control*, vol. 56, no. 11, pp. 2655–2660, Nov. 2011.

[55] W. Zhang and L. Yu, "Output feedback stabilization of networked control systems with packet dropouts," *IEEE Trans. Autom. Control*, vol. 52, no. 9, pp. 1705–1710, Sep. 2007.

[56] Z. Wang, Y. Liu, and X. Liu, "Exponential stabilization of a class of stochastic system with Markovian jump parameters and mode-dependent mixed time-delays," *IEEE Trans. Autom. Control*, vol. 55, no. 7, pp. 1656–1662, Jul. 2010.
[57] D. Yue, E. Tian, Y. Zhang, and C. Peng, "Delay-distribution-dependent stability and stabilization of t-s fuzzy systems with probabilistic interval delay," *IEEE Trans. Syst. Man Cybern. B Cybern.*, vol. 39, no. 2, pp. 503–515, Apr. 2009.
[58] D. Kim, Y. Lee, W. Kwon, and H. Park, "Maximum allowable delay bounds of networked control systems," *Control Eng. Pract.*, vol. 11, no. 11, pp. 1301–1313, Nov. 2003.
[59] D. Yue and Q. Han, "Delayed feedback control of uncertain systems with time-varying input delay," *Automatica*, vol. 41, no. 2, pp. 233–240, Feb. 2005.
[60] K. Jacobs, *Stochastic Processes for Physicists*. Cambridge, U.K.: Cambridge Univ. Press, 2010, pp. 57–59.
[61] G. Meyer, R. Su, and L. Hunt, "Application of nonlinear transformations to automatic flight control," *Automatica*, vol. 20, no. 1, pp. 103–107, 1984.
[62] J. Hauser, S. Sastry, and P. Kokotovic, "Nonlinear control via approximate input-output linearization: The ball and beam example," *IEEE Trans. Autom. Control*, vol. 37, no. 3, pp. 392–398, Mar. 2005.
[63] A. Krener, "On the equivalence of control systems and the linearization of nonlinear systems," *SIAM J. Control*, vol. 11, no. 4, pp. 670–676, Nov. 1973.
[64] W. Lin and C. Byrnes, "Remarks on linearization of discrete-time autonomous systems and nonlinear observer design," *Syst. Control Lett.*, vol. 25, no. 1, pp. 31–40, May 1995.
[65] A. Karimi, H. Khatibi, and R. Longchamp, "Robust control of polytopic systems by convex optimization," *Automatica*, vol. 43, no. 8, pp. 1395–1402, Aug. 2007.



Huadong Mo (S'14) received the B.S. degree from the Department of Automation, University of Science and Technology of China, Hefei, China, in 2012. He is currently working toward the Ph.D. degree at the Department of Systems Engineering and Engineering Management, City University of Hong Kong, Hong Kong.

His research interests include reliability modeling and optimization of complex systems, such as smart grid system, power plant and control system.

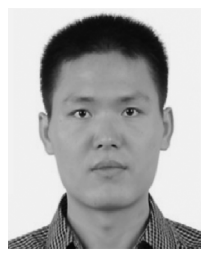
Wei Wang received the B.S. degree from the Department of Automation, University of Science and Technology of China, Hefei, China, in 2011. He is currently working toward the Ph.D. degree at the Department of Automation, University of Science and Technology of China, Hefei, China.

His research interests include reliability modeling and interval analysis.

Min Xie (M'91–SM'94–F'06) received the Ph.D. degree in quality technology from Linkoping University, Linkoping, Sweden, in 1987.

Currently, he is a Chair Professor at City University of Hong Kong. He has authored or coauthored numerous refereed journal papers, and some books on quality and reliability engineering, including *Software Reliability Modeling* (World Scientific), *Weibull Models* (Wiley), *Computing Systems Reliability* (Kluwer), and *Advanced QFD Applications* (ASQ Quality Press).

Prof. Xie was awarded the prestigious LKY Research Fellowship in 1991. He is an Editor of the *International Journal of Reliability, Quality and Safety Engineering*, Department Editor of IIE TRANSACTIONS, Associate Editor of the IEEE TRANSACTIONS ON RELIABILITY AND RELIABILITY ENGINEERING AND SYSTEM SAFETY, and is on the editorial board of a number other international journals.



Junlin Xiong (M'11) received the B.Eng. and M.Sci. degrees from Northeastern University, Shenyang, China, and the Ph.D. degree from the University of Hong Kong, Hong Kong, in 2000, 2003, and 2007, respectively.

From 2007 to 2010, he was a Research Associate at the University of New South Wales, Australian Defence Force Academy, Australia. In 2010, he joined the University of Science and Technology of China where he is currently a Professor with the Department of Automation. His current research interests are in the fields of Markovian jump systems, networked control systems, and negative imaginary.