

# Availability Modeling of Generalized k-out-of-n: G Warm Standby Systems with PEPA



# Availability Modeling of Generalized $k$-out-of-$n$: G Warm Standby Systems With PEPA

Xiaoyue Wu, Jane Hillston, Cheng Feng

***Abstract*—Developing analytical availability models for $k$-out-of-$n$: G warm standby repairable systems with many non-identical components is tedious and error-prone, requiring specification of the generator matrix of a high dimensional Markov chain. Using the performance evaluation process algebra (PEPA) as an intermediary, this paper gives a new modeling approach for availability evaluation of such systems with $r$ repair facilities. The components of the system are classified into $n$ different groups that consist of statistically identical components following exponential time-to-failure and repair time distributions. A library of PEPA components and their actions are defined for system component groups, repair facilities, repair queue and system dynamics. To capture the dependency of system states on components, a signaling mechanism is realized by actions with suitably high rates. A compilation tool is provided to automatically generate the PEPA model from a brief specification of the system, using the library components. This provides input for the PEPA analysis tool and is amenable to availability analysis. Examples are used to illustrate the proposed modeling method. Modeling with PEPA provides an efficient way to deal with availability evaluation of systems considered with many groups of repairable components.**

***Index Terms*—Reliability modeling, availability, process algebra, redundant systems, Markov processes.**

## ACRONYM

| | |
|---|---|
| PEPA | Performance evaluation process algebra |
| CTMC | Continuous-time Markov chain |
| BDD | Binary decision diagram |
| MMDD | Multi-state multi-valued decision diagram |
| SAN | Stochastic automata network |
| PH | Phase-type |
| DFT | Dynamic fault tree |
| $s$-identical | Statistically identical |

## NOTATIONS

| | |
|---|---|
| $n$ | number of component groups in the system |
| $N$ | set defined as $\{1, 2, \ldots, n\}$ |
| $M$ | total number of components in the system |
| $G_i$ | $i$th group of components |
| $N_i$ | number of components in $G_i$ |
| $k$ | integer, the system will fail if the number of active up components is less than $k$ |
| $r$ | number of repair facilities |
| $\lambda_i$ | failure rate in active up mode for components in $G_i$ (parameter of exponential distribution) |
| $\lambda_i'$ | failure rate in warm up mode for components in $G_i$ (parameter of exponential distribution) |
| $\mu_i$ | repair rate for components in $G_i$ (parameter of exponential distribution) |
| $a$ | active up state of component |
| $w$ | warm up state of component |
| $f$ | down state of component |
| $z$ | frozen state of component |
| $l_a^i$ | number of components in state $a$ for $G_i$ |
| $l_w^i$ | number of components in state $w$ for $G_i$ |
| $l_f^i$ | number of components in state $f$ for $G_i$ |
| $l_z^i$ | number of components in state $z$ for $G_i$ |
| $x_i$ | state of $i$th component group |
| $s$ | state of system. $s = (l_f^1, l_f^2, \cdots, l_f^n)$ |
| $m_i$ | number of failed components of $G_i$ in queue for repair |
| $m$ | state of queue for repair |
| $B^{i,u}_{l_a^i, l_w^i, l_f^i, l_z^i}$ | PEPA component for component of $G_i$ in state $(l_a^i, l_w^i, l_f^i, l_z^i)$, when the system is in up state. |
| $B^{i,d}_{l_a^i, l_w^i, l_f^i, l_z^i}$ | PEPA component for component of $G_i$ in state $(l_a^i, l_w^i, l_f^i, l_z^i)$, when the system is in down state. |
| $\epsilon$ | a very large activity rate for a PEPA component to send out its state change signal almost instantaneously after its state change |
| $fail_a^i, failL_a^i$ | action types representing failure of components of $G_i$ in active mode |
| $fail_w^i, failL_w^i$ | action types representing failure of components of $G_i$ in warm mode |
| $rep^i, repB^i$ | action types representing repair for components of $G_i$ |
| $acc^i$ | action type representing start of repairing component of $G_i$ |
| $hot^i$ | action type letting one of components of $G_i$ enter into state $a$ from state $w$ |
| $warm^i$ | action type letting one of components of $G_i$ enter into state $w$ from state $a$ |
| $freeze^i$ | action type that lets all up components of $G_i$ enter into state $z$ |

Manuscript received April 19, 2015; revised December 27, 2015; accepted April 4, 2016. Date of publication August XX, 20XX; date of current version September XX, 20XX. (*Corresponding author: Xiaoyue Wu.*)

Xiaoyue Wu is with the College of Information Systems and Management, National University of Defense Technology, Changsha, Hunan, 410073, China. e-mail: (xiaoyuewucn@nudt.edu.cn).

Jane Hillston is with the School of Informatics, the University of Edinburgh,Scotland, EH8 9AB, UK. (email: Jane.Hillston@ed.ac.uk)

Cheng Feng is with the School of Informatics, the University of Edinburgh,Scotland, EH8 9AB, UK.(email: s1109873@sms.ed.ac.uk)

Digital Object Identifier 00.0000/TSMC.0000.0000000

| | |
|---|---|
| $defreeze^i_j$ | action type that lets $j$ components of $G_i$ enter into state $a$ |
| $V_i, V_\emptyset$ | PEPA component representing that a repair facility is in the state of repairing a failed component of group $G_i$. $V_\emptyset$ denotes that the facility is in idle state |
| $G_s, G'_s$ | PEPA components corresponding to system behavior in state $s$ |
| $L_m$ | PEPA components corresponding to behavior of the repair queue in state $m$ |
| $\alpha(m)$ | function used to determine from which group to select a component to enter the repair process when the queue is in state $m$ |
| $\Lambda(m)$ | map for the resulting state of the queue after taking out a component for repair when the queue is in state $m$ |
| $I_d(s)$ | indicator function capturing whether the system in state $s$ is up or down |
| $s \equiv u$ | system state $s$ is an up state |
| $s \equiv d$ | system state $s$ is a down state |

## I. Introduction

RELIABILITY of a system refers to the probability that the system will perform its required function under given conditions for a stated time interval without failure. Availability is a broader term, but usually refers to the stationary availability or steady state availability [1], representing the long-term probability that the system is available, or the fraction of time that the system is in the operational state. Reliability and availability are closely related concepts, and jointly reflect the dependability of the system in delivering its service. To increase the dependability of critical systems, various kinds of standby redundancy techniques have been widely adopted in engineering practice. Examples include power plants with multiple generators, fault-tolerant computer systems and airplanes with multiple engines. According to the failure characteristics of the redundant components, standby designs are classified as cold, warm and hot standby [2]. For warm standby systems, the redundant components in the standby state are exposed to partial operational stresses and typically fail at a lower rate than the operating components. When an operating component fails, an available component in warm standby becomes active to replace it. Note that both hot and cold standby systems can be regarded as a special case of warm standby systems.

Because of its wide application in engineering and theoretical challenges, considerable effort has been dedicated to modeling and analysing the dependability of warm standby systems [3] [4]. Generally, the existing modeling and analysis methods can be classified into four categories [5]: state space-based methods, combinatorial methods, simulation methods, and recursive numerical methods. In our work we follow a state space-based approach, seeking to construct a continuous time Markov chain (CTMC) to model the system's dynamic behaviors. However, rather than construct the CTMC directly, we use the formal modeling language PEPA (Performance Evaluation Process Algebra), as an intermediary. PEPA is a well-established modeling language, supported by a rich suite of software tools [6], which uses compositional descriptions of interacting components to derive large-scale CTMC models that can be subjected to a variety of analyses. Using PEPA as an intermediary we are able to avoid the time-consuming and error-prone work of constructing a CTMC by hand to estimate availability. However, since many modelers will be unfamiliar with the formal notation used in PEPA, we provide the availability modeler with a library of predefined PEPA components and a high-level specification language which allows the PEPA model reflecting the system of interest to be constructed automatically.

### A. Related Work

State space-based methods, which are typically based on CTMCs, can effectively model the system's dynamic behaviors. Usually, the components are assumed to have exponential life time and repair time distributions. The reliability or availability is usually modeled by a CTMC and solved through Laplace transform. Many kinds of warm standby systems have been studied using this approach. Some important examples include: 1-out-of-2:G systems with common cause failures and human errors [7], with imperfect sensing and switching [8], 2-out-of-5:G systems with common cause failures and replacements [9], $k$-out-of-$n$:G warm standby system with $r$ repair facilities [10] [11], with balking and reneging components [12], with components with multiple failure modes [13], with unreliable repair facilities [14], warm standby systems with two non-identical components and failure of switching [15], warm standby subsystems with two non-identical components and in series connection with another subsystem [16]. In cases of nonexponential distributions, supplementary variable techniques [17]–[22] and phase-type (PH) distribution techniques [23] [24] can be used. Moreover, warm standby systems with $s$-identical components can be solved by developing iterative equations for state probabilities by event decomposition [25] [26]. However, the state-based approach suffers from the state space explosion problem and difficulty in generating the transition rate matrix when the number of components becomes moderately large. Sometimes, the expressions involving warm standby non-identical components can be so long that they occupy more than half a paper [16] [27], resulting in models that are complicated and hard to verify or solve.

Combinatorial methods are based on an algebra of event probabilities, and have been applied to many systems, including: systems with components having proportional hazard rates [28], two-unit parallel systems [29], $k$-out-of-$n$:G warm standby systems [2] [4], 1-out-of-$N$ : $G$ warm standby systems with special features [30] [31], $k$-out-of-$n$:G systems with a single warm standby component [32] and systems having two identical sets of components [33]. Besides, binary decision diagram (BDD) and multi-state multi-valued decision diagram (MMDD) have been applied for reliability evaluation of $k$-out-of-$n$:G systems [34]. In most cases, combinatorial methods are numerically very efficient, but are restricted to systems with non-repairable components.

Recursive numerical methods are proposed by Levitin, Xing and Dai [5], [35]–[38], which use algorithms based on

discretization approximation of component's distributions, and recursive formulas for reliability evaluation. They have been applied to many kinds of 1-out-of -$N$ standby systems with nonidentical warm standby components having general distributions, and special features, including imperfect switching mechanisms, state-dependent standby mode transfers, random replacement times, and dynamic uneven backups. However, in the existing literature on those methods, system components are assumed to be non-repairable during the mission.

Simulation methods place the least restrictions on the system, but require more computational time to ensure precise estimates. For example, Huang et al. obtained the reliability of a special warm standby system by simulation using Reliasoft's BlockSim software [33].

In most of the literature on warm standby systems with repairable components, components are assumed to be $s$-identical. Warm standby systems with more than two non-identical components have received less attention. Based on a CTMC model, Zhang et al. [27] studied the availability of a 3-out-of-4 repairable warm standby system with non-identical components divided into two groups. Later, Zhang et al. [39] extended the work to a $k$-out-of-$n$: G system with two types of components. Although theoretically this approach can be extended to systems with more than two groups of components, the construction of the state transition diagram and the associated transition rate matrix will become increasingly complicated and difficult to deal with directly.

Khatab et al. [40] noticed that the work by Zhang et al. [39] is limited to systems with only two categories of components, and studied $k$-out-of-$n$: G systems with more non-identical components. They gave algorithms for reducing the state space and constructing the state transition rate matrix. The availability is then obtained by a multidimensional Markov model, either built directly or via a stochastic automata network (SAN) model. However, the system that they study is assumed to be a hot standby system, and it is not readily apparent in the paper how the approach can be extended to the case of warm standby systems with non-identical components, either through direct construction of the global generator matrix or via the SAN descriptor, due to the complex synchronising events that need to be taken into account. Moreover, the details of modeling and evaluating availability with SAN are not presented.

From the above, we can see that the modeling of $k$-out-of-$n$: G warm standby systems with more than two non-identical repairable components and a limited number of repair facilities has not been sufficiently investigated, mainly due to the complex stochastic dependencies involved. However, in practice, due to different time and locations of installation, types or sources of manufacturers in order to reduce the risk of common cause failures, components of redundancy system may not be statistically identical [27] [36]. In addition, for availability evaluation of $k$-out-of-$n$: G repairable systems using the CTMC approach, specifying the infinitesimal generator directly can be time consuming, tedious and error prone. Therefore, in practice, it is necessary for the CTMC model to be generated automatically from a higher level modeling formalism.

PEPA is a high level stochastic modeling method with clear compositional structure and good quantitative analysis capability, and as such has found wide application [41]–[43]. For system dependability evaluation, Yan et al. evaluated the availability of a system with two servers in parallel connection [44]. Closest to our work is the recent paper by Kloul in which the author presents a mapping from dynamic fault trees (DFTs) to PEPA models [45]. As with our work, the motivation for using PEPA is to provide a bridge between a fault model and an underlying CTMC. In this paper, we will use PEPA for dependability modeling of $k$-out-of-$n$: G warm standby system with limited repair facilities.

### B. Contributions

This paper is intended to extend the work of [39] by providing a new availability modeling approach for $k$-out-of-$n$: G repairable systems with more than two component categories. By building on a set of predefined components developed in the performance evaluation process algebra (PEPA) [46], our approach can clearly describe the system's dynamic behavior in a compositional way, and avoid direct construction of the infinitesimal generator of the CTMC model. Moreover, for our model to be solved using existing PEPA tools, we provide a tool for compiling our model to a directly executable PEPA model by the existing PEPA analysis tool [6]. Our contributions are as follows:

1) We develop a library of PEPA components and composition templates to capture the behavior of $k$-out-of-$n$: G repairable systems with more than two component categories.
2) We establish a high-level specification format for a particular form of $k$-out-of-$n$: G repairable system, which can be mapped into an appropriate PEPA model using the library components. Once constructed, this PEPA model can be compiled using existing software to generate the underlying CTMC which is amenable to numerical analysis and from which the availability can be derived.
3) We present a software tool which automates this mapping, compiling the high-level specification into the corresponding PEPA model.

The rest of this paper is organized as follows. Section II provides a brief introduction to the PEPA modeling language. Section III presents the system description and main assumptions. Section IV develops the library of PEPA components for describing the groups of the system, repair facilities, queue for repair, and system behaviors. In Section V, we introduce our developed tool for generating the PEPA model automatically as the input file to the PEPA analysis tool for availability analysis. The proposed approach is verified and illustrated by numerical examples. Finally, Section VI concludes this paper and presents possible future research works along this direction.

## II. PEPA

PEPA is a stochastic process algebra used for modeling compositional stochastic systems [46]. From the perspective

of PEPA, a system consists of components cooperating with each other in their actions, each of which has an associated exponential time delay.

The syntax of PEPA is concise [46]. A PEPA component can be expressed using the language constructs defined in the following grammar:

$$P ::= (\alpha, \lambda).P \mid P + P \mid P \underset{L}{\bowtie} Q \mid A \tag{1}$$

The meanings of each of the combinators are given as follows.

- $(\alpha, \lambda).P$ *prefix:* the process completes an action of type $\alpha$, with an exponential time delay governed by rate $\lambda$, and then becomes process $P$.
- $P_1 + P_2$ *choice*, a process with alternative behaviors specified by the two distinct PEPA processes $P_1$ and $P_2$; a race condition determines which choice is selected and the other is discarded.
- $P \underset{L}{\bowtie} Q$ *cooperation*, the components $P$ and $Q$ must work simultaneously for action types in the set $L$; they proceed independently and concurrently on all other action types.
- $A \stackrel{\text{def}}{=} P$ *constant*, a name $A$ can be associated with a behavior $P$, allowing cyclic behaviour to be defined by mutually recursive definitions.

When components are working in cooperation they are governed by the principle of *bounded capacity* which enforces that the rate of the shared action is the minimum of the rates at which the action is offered in each of the cooperating components. When a component has no influence over the rate we say that it is *passive* and denote the rate by $\top$. In the library of PEPA components presented in this paper, we will also find it convenient to have some actions that occur (essentially) instantaneously. For this purpose, we introduce a very large rate $\epsilon$. This will be used to signal between components in the model when a state change has occurred.

For convenience, we also introduce some derived syntax. When the set $L$ is empty, we write $P \underset{L}{\bowtie} Q$ as $P \parallel Q$. We will also use the concise notation $\prod_{j=1}^{n}(\alpha_j, \epsilon)$ to denote component undertaking a sequence of signaling actions $(\alpha_1, \epsilon), \cdots, (\alpha_n, \epsilon)$ i.e.,

$$\prod_{j=1}^{n}(\alpha_j, \epsilon).P = (\alpha_1, \epsilon).(\alpha_2, \epsilon).\cdots.(\alpha_n, \epsilon).P \tag{2}$$

For a PEPA component which has the behavior $A$ and also sometimes the behaviour $P$ depending on proposition $x$, we write $A + P|_x$, with the following meaning:

$$A + P|_x = \begin{cases} A + P & \text{if } x \text{ is true} \\ A & \text{otherwise} \end{cases} \tag{3}$$

This is useful to capture when the alternative behaviors offered by a component depend on the current state of the system.

As a simple example, consider a single component which may fail at exponential rate $r_f$, and be repaired by a single repair facility at exponential rate $r_r$. We may represent the component by the PEPA components:

$$\begin{aligned} Comp_{up} &\stackrel{\text{def}}{=} (fail, r_f).(failed, \epsilon).Comp_{down} \\ Comp_{down} &\stackrel{\text{def}}{=} (repair, \top).Comp_{up} \end{aligned}$$

whilst the repair facility can be represented as:

$$\begin{aligned} Rep_{idle} &\stackrel{\text{def}}{=} (failed, \top).Rep_{engaged} \\ Rep_{engaged} &\stackrel{\text{def}}{=} (repair, r_r).Rep_{idle} \end{aligned}$$

Here , the component $Comp_{up}$ uses a signal, *failed*, to engage the repair facility.

## III. System Description and Assumptions

Usually, a $k$-out-of-$n$: G warm standby system requires at least $k$ of its $n$ components to be up to keep the system in an operational state. Therefore, it can be seen as a generalization of a series and parallel system. In this paper, we assume that the system under study is a $k$-out-of-$n$: G warm standby system with $r$ repair facilities, where $n$ is the number of statistically identical groups of components. This is a generalization of the system studied in [39], as here $n$ can be greater than 2. As an illustration, a power plant with multiple groups of generators each with different failure and repair rates can be thought as an example of such a system [39].

We adopt a view that

1) The components of the system are divided into $n$ groups. Components of the same group are $s$-identical with regards to their failure and repair features.
2) For the system to be operational, at least $k$ components must be in an active up state.
3) The failure and repair times of all the components are mutually independent and follow non-identical exponential distributions. The rates are different for different groups but all components in the same group have the same rates.
4) Each group is associated with a priority index. The components in the same group have equal priority. The $i$th group has higher priority than the $j$th group if $i < j$.
5) A component with higher priority will be selected for repair before those with lower priority, but once a repair has started within a repair facility, it will not be preempted by the failure of a higher priority component.
6) Once a component with higher priority is repaired, if there is any component with lower priority in an active up state, it will be replaced by the newly repaired component and enter into its warm up state.
7) Once an active up component fails, a component with the same or nearest lower priority index in warm standby mode will enter into active up mode immediately, if it is available.
8) The repair facilities are all statistically identical. The repair is perfect, i.e., a repaired component is as good as new.
9) When all the repair facilities are occupied, the failed component must wait in a queue until a repair facility becomes idle. The size of the queue for waiting for repair is unlimited.
10) Switching is perfect (without failure) and instantaneous.
11) There are no common cause failures.
12) Once the system fails, no failure will occur for unfailed components (which will all enter into a frozen state), but repair work can still be conducted.

TABLE I
PAREMETERS OF COMPONENT GROUPS

| Group No | failure rate in active state | failure rate in warm state | repair rate | Number of Components |
|---|---|---|---|---|
| 1 | $\lambda_1$ | $\lambda'_1$ | $\mu_1$ | $N_1$ |
| 2 | $\lambda_2$ | $\lambda'_2$ | $\mu_2$ | $N_2$ |
| $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ | $\vdots$ |
| $n$ | $\lambda_n$ | $\lambda'_n$ | $\mu_n$ | $N_n$ |

13) Initially, all the system components are in the up state, and all the repair facilities are in the idle state.

In Table I, $\lambda_i, \lambda'_i$ denote the failure rate of components of group $G_i$ in active mode and warm mode respectively. $\mu_i$ is the repair rate of components in group $G_i$. $N_i$ is the number of components in group $G_i$. The total number of components of the system is $M = \sum_{i=1}^{n} N_i$.

Define the state space of a component as $\{a, f, w, z\}$, where $a, f, w, z$ are defined as follows.

- $a$ : component is in active mode and up.
- $f$ : component failed and is down.
- $w$ : component is in warm mode and up.
- $z$ : component is frozen in the up state because of system failure.

The state $z$ is called the frozen state, meaning that the component's current state is suspended in an up state (active up, or warm up), but it cannot currently fail because the system is in the down state. Once the system is restored to the up state, the component will immediately enter the up state.

### A. System States

For group $G_i$, since all the components within the group are $s$-identical, its state can be expressed as

$$x_i = (l_a^i, l_w^i, l_f^i, l_z^i) \tag{4}$$

where $l_a^i, l_w^i, l_f^i, l_z^i$ denote the number of its components in state $a, w, f, z$ respectively.

Generally speaking, we can specify the system state in terms of all $x_i, i \in N$ as defined by (4) . Thus, we can denote a system state as

$$x = (x_1, x_2, \cdots, x_n) \tag{5}$$

Let $X$ denote the set of all possible $x$.

First, it can be shown that the state of the system can be determined by the numbers of failed components of all groups [39]. So, a system state can also be denoted as

$$s = (l_f^1, l_f^2, \cdots, l_f^n) \tag{6}$$

To understand this, we just need to show that the state of each group can be uniquely determined from knowing $s$.

Let $S$ denote the set of all $s$. In Tables II and III, we give the group state patterns when the system is up and down, respectively.

As shown in Table II, if the system is in the up state, it means that there is no component in state $z$, and all the components not in the failed state must be in either state $a$ or $w$. Since the number of active up components must be $k$, we must have

$$M - \sum_{i=1}^{n} l_f^i = \sum_{i=1}^{n} l_a^i + \sum_{i=1}^{n} l_w^i = k + \sum_{i=1}^{n} l_w^i \geq k \tag{7}$$

TABLE II
GROUP STATES WHEN THE SYSTEM IS UP

| $G_1$ | $\cdots$ | $G_{q-1}$ | $G_q$ | $G_{q+1}$ | $\cdots$ | $G_n$ |
|---|---|---|---|---|---|---|
| $l_a^1$ | $\cdots$ | $l_a^{q-1}$ | $l_a^q$ | 0 | $\cdots$ | 0 |
| 0 | 0 | 0 | $l_w^q$ | $l_w^{q+1}$ | $\cdots$ | $l_w^n$ |
| $l_f^1$ | $\cdots$ | $l_f^{q-1}$ | $l_f^q$ | $l_f^{q+1}$ | $\cdots$ | $l_f^n$ |
| 0 | $\cdots$ | 0 | 0 | 0 | $\cdots$ | 0 |

TABLE III
GROUP STATES WHEN THE SYSTEM IS DOWN

| $G_1$ | $\cdots$ | $G_{q-1}$ | $G_q$ | $G_{q+1}$ | $\cdots$ | $G_n$ |
|---|---|---|---|---|---|---|
| 0 | $\cdots$ | 0 | 0 | 0 | $\cdots$ | 0 |
| 0 | $\cdots$ | 0 | 0 | 0 | $\cdots$ | 0 |
| $l_f^1$ | $\cdots$ | $l_f^{q-1}$ | $l_f^q$ | $l_f^{q+1}$ | $\cdots$ | $l_f^n$ |
| $l_z^1$ | $\cdots$ | $l_z^{q-1}$ | $l_z^q$ | $l_z^{q+1}$ | $\cdots$ | $l_z^n$ |

As shown in Table III, if the system is in the failure state, it means that all the components not in the down state must be in state $z$. So, it must be

$$M - \sum_{i=1}^{n} l_f^i = \sum_{i=1}^{n} l_z^i < k \tag{8}$$

The last inequality is true because otherwise the system would be in the up state with enough active up components.

As a result, we can use function $I_d(s)$ to indicate whether system state $s$ is a down state, which is defined as

$$I_d(s) = \begin{cases} 1 & M - \sum_{i=1}^{n} l_f^i < k \\ 0 & \text{otherwise} \end{cases} \tag{9}$$

Define $q(s)$ as the integer $q \in N$ that satisfies

$$\sum_{j=1}^{q-1} (N_j - l_f^j) < k \leq \sum_{j=1}^{q} (N_j - l_f^j) \tag{10}$$

when the system is up, and $q(s) = 0$ when the system is down.

Now we can detail how to uniquely determine a group state when the system is up or down.

*1) Group state when the system is up:* If $I_d(s) = 0$, then $s$ is an up state, denoted as $s \equiv u$, and from Table II we can calculate the state of group $G_i$ in the following way.

$$l_a^i = \begin{cases} N_i - l_f^i & i < q(s) \\ k - \sum_{j=1}^{q-1} l_a^j & i = q(s) \\ 0 & i > q(s) \end{cases} \tag{11}$$

$$l_w^i = \begin{cases} 0 & i < q(s) \\ N_q - l_f^q - (k - \sum_{j=1}^{q-1} l_a^j) & i = q(s) \\ N_i - l_f^i & i > q(s) \end{cases} \tag{12}$$

$$l_z^i = 0 \tag{13}$$

*2) Group state when the system is down:* If $I_d(s) = 1$, then $s$ is a down state, denoted as $s \equiv d$, and from Table III we can find the state of group $G_i$ as

$$l_a^i = 0 \tag{14}$$
$$l_w^i = 0 \tag{15}$$
$$l_z^i = N_i - l_f^i \tag{16}$$

Thus, given any system state $s$ in the form of (6), we can uniquely determine the corresponding state $x$ in the form of (5) for all groups. Hence, we can define a map $\chi : S \to X$:

$$x = (x_1, x_2, \cdots, x_n) = \chi(s) = \chi(l_f^1, l_f^2, \cdots, l_f^n) \tag{17}$$

From the previous discussion, the total number of system states in $X$ is at most $\prod_{j=1}^{n}(N_j + 1)$. If $N_i = 2, n = 2$, this number will be 9. Here, we say "at most" because the state space can be further reduced if we consider that state $s$ must satisfy

$$\sum_{i=1}^{n} l_f^i \leq M - k + 1 \tag{18}$$

This is because, by our assumptions, no further failure can occur once the system has failed.

## IV. Availability Modeling with PEPA

### A. Groups of System Components

In this paper, we provide the following PEPA components to represent the behavior of group $G_i$ in state $x_i$.

$$\begin{aligned} B^{i,u}_{l_a^i,l_w^i,l_f^i,0} \stackrel{\text{def}}{=} & (fail_a^i, l_a^i \cdot \lambda_i).(failL_a^i, \epsilon).B^{i,u}_{l_a^i-1,l_w^i,l_f^i+1,0}|_{l_a^i>0} \\ & + (fail_w^i, l_w^i \cdot \lambda_i').(failL_w^i, \epsilon).B^{i,u}_{l_a^i,l_w^i-1,l_f^i+1,0}|_{l_w^i>0} \\ & + (repB^i, \top).B^{i,u}_{l_a^i,l_w^i+1,l_f^i-1,0}|_{l_f^i>0} \\ & + (warm^i, \top).B^{i,u}_{l_a^i-1,l_w^i+1,l_f^i,0}|_{l_a^i>0} \\ & + (hot^i, \top).B^{i,u}_{l_a^i+1,l_w^i-1,l_f^i,0}|_{l_w^i>0} \\ & + (freeze^i, \top).B^{i,d}_{0,0,l_f^i,l_a^i+l_w^i} \end{aligned} \tag{19}$$

$$\begin{aligned} B^{i,d}_{0,0,l_f^i,l_z^i} \stackrel{\text{def}}{=} & (repB^i, \top).B^{i,d}_{0,0,l_f^i-1,l_z^i+1}|_{l_f^i>0} \\ & + \sum_{j=0}^{l_z^i} (defreeze_j^i, \top).B^{i,u}_{j,l_z^i-j,l_f^i,0} \end{aligned} \tag{20}$$

In the above component models, for each component group $G_i$, we use two kinds of PEPA components to represent system states: $B^{i,u}_{l_a^i,l_w^i,l_f^i,0}$ when the system is up and $B^{i,d}_{0,0,l_f^i,l_z^i}$ when the system is down.

*1)* $B^{i,u}_{l_a^i,l_w^i,l_f^i,0}$*:* Since the system is in the up state, so the components of this group will fail at rate $l_a^i \cdot \lambda_i$ from active up states and at rate $l_w^i \cdot \lambda_i'$ from warm up states. The action type $fail_a^i$ is used to send signals to other PEPA components defined later to capture system behaviors, and and $failL_a^i$ is used to synchronize with other PEPA components defined later to capture repair queue behaviors.

When a group component is repaired by a repair facility, action $repB^i$ will occur in passive cooperation, the number of failed components will decrease by 1, and the number of warm standby components of this group will increase by 1. Whether the repaired component needs to further enter into the active up state will be left to be determined by PEPA components representing system behaviors as will be introduced later in this section.

If the group receives signal $warm^i$, one of its active up components will immediately enter into the warm up state. In contrast, if it receives signal $hot^i$, one of its components in the warm up state will immediately enter into the active up state.

If the group receives the signal $freeze^i$, indicating that the system is down, it will immediately force all of its up components (in both active and warm states) to enter into state $z$.

*2)* $B^{i,d}_{0,0,l_f^i,l_z^i}$*:* This is the PEPA component used to capture the group behavior when the system is in the down state.

When a group component is repaired by a repair facility, action $repB^i$ will occur in passive cooperation, and the number of failed components will decrease by 1, and the number of frozen components of this group will increase by 1. Whether it needs to enter into the active up state or the warm up state will be left to be determined by PEPA components representing system behaviors as will be introduced later in this section.

If it receives a signal $defreeze_j^i$, which means that the system is entering an up state, this component will immediately let $j$ components in state $z$ enter into the active up state and the remaining $l_z^i - j$ components in state $z$ enter into the warm up state.

We can estimate the maximum number of PEPA components thus defined needed in a model. By combinatorial mathematics [47], for integer equation

$$\sum_{i=1}^{q} x_i = N \tag{21}$$

the number of all possible solutions is $C_{q-1+N}^{q-1}$

Since group $G_i$ has $N_i$ components, we have

$$l_a^i + l_w^i + l_f^i + l_z^i = N_i \tag{22}$$

Recall that operational components may be in any of the states *active*, *warm* or *frozen*. Notice that according to our definition of the frozen state, for each group $G_i$, $l_a^i + l_w^i$ and $l_z^i$ cannot be greater than 0 at the same time, i.e., for system state $s$

$$(s = u) \Rightarrow (l_z^i = 0) \tag{23}$$
$$(s = d) \Rightarrow (l_a^i + l_w^i = 0) \tag{24}$$

So we only need to consider the cases

$$l_a^i + l_w^i + l_f^i = N_i, \quad s = u \tag{25}$$

and

$$l_f^i + l_z^i = N_i, \quad s = d \tag{26}$$

By the preceding conclusion, the numbers of possible solutions for (25) and (26) are $C_{N_i+2}^2$, $C_{N_i+1}^1$ respectively, so

the maximum number of PEPA components that need to be considered for (19) and (20) is

$$N_g^p = \sum_{i=1}^{n} \left[ C_{N_i+2}^2 + C_{N_i+1}^1 \right] \tag{27}$$

For instance, if $n = 2, N_i = 2, \forall i$, then $N_g^p = 18$.

### B. Repair Facilities

Since all the repair facilities are treated as $s$-identical, for each of the $r$ repair facilities, we provide the following PEPA components

$$V_\emptyset \stackrel{\text{def}}{=} \sum_{i \in N} (acc^i, \epsilon).V_i \tag{28}$$

$$V_i \stackrel{\text{def}}{=} (rep^i, \mu_i).(repB^i, \epsilon).V_\emptyset \qquad \forall i \in N \tag{29}$$

where $V_\emptyset$ denotes that repair facility $V$ is idle. $V_i$ denotes that the repair facility is in the process of repairing a failed component of group $G_i$.

When a repair facility is in the idle state, it can accept a failed component by sending out action signal $acc^i$ to all component groups when there is one or more system components waiting for repair in the queue.

When a repair facility is in the state of repairing a failed component from group $G_i$, it will complete the action $rep^i$ at rate $\mu_i$, and share this with the PEPA component representing system behavior. It will send signal $repB^i$ to the corresponding PEPA group component immediately after the repair completion.

It can be easily seen that there are totally $N_r^p = n + 1$ PEPA component equations to describe repair facilities. For $n = 2$, $N_r^p = 3$.

### C. Queue for Repair

Since the number of repair facilities is finite, so the incoming components must wait in a queue when all the repair facilities are busy. Since we set priority for all groups in accordance with their group index, for two components $D^i \in G_i, D^j \in G_j$ waiting for repair, if $i < j$, then $D^i$ will enter the repair process ahead of $D^j$ when there is an idle facility.

We use the following index to denote the state of the queue

$$m = (m_1, m_2, \ldots, m_n) \tag{30}$$

where $m_i$ is the number of failed components of group $G_i$.

Thus, we provide a PEPA component for the queue in state $m$ as below

$$\begin{aligned} L_{m_1,m_2,\ldots,m_n} \stackrel{\text{def}}{=} & \sum_{s \in \{a,w\}} (failL_s^1, \top).L_{m_1+1,m_2,\ldots,m_n} \\ & + \sum_{s \in \{a,w\}} (failL_s^2, \top).L_{m_1,m_2+1,\ldots,m_n} \\ & \cdots \\ & + \sum_{s \in \{a,w\}} (failL_s^n, \top).L_{m_1,m_2,\ldots,m_n+1} \\ & + (acc^{\alpha(m)}, \top).L_{\Lambda(m)}|_{\alpha(m)>0} \end{aligned} \tag{31}$$

By the above PEPA expression, when a system component of group $G_i$ fails, the queue component will receive a signal $failL_s^i$, and so the queue will change the number of its corresponding elements. When a repair facility becomes idle, it will send signal $acc^{\alpha(m)}$ to the queue, and select a failed component for repair according to the priorities of all the components waiting in queue; subsequently the queue will decrease the number of its elements associated with the group.

In (31), $\alpha(m)$ is an index function of the queue state $m$, which is used to determine from which group to select a group component to enter the repair process

$$\begin{aligned} \alpha(m) &= \alpha(m_1, m_2, \ldots, m_n) \\ &= \begin{cases} 1 & m_1 > 0 \\ 2 & m_1 = 0, m_2 > 0 \\ \cdots & \cdots \\ n & m_1 = \cdots = m_{n-1} = 0, m_n > 0 \\ 0 & m_1 = m_2 = \cdots = m_n = 0 \end{cases} \end{aligned} \tag{32}$$

Notice that $\alpha(m)$ is defined in the way of (32) because a component can enter the repair process only when there is no component from a higher priority group waiting in the queue.

$\Lambda(m)$ in (31) is a map from $m$ to the resulting state of the queue after taking out a component for repair when the state of the queue is $m$.

$$\begin{aligned} \Lambda(m) &= \Lambda(m_1, m_2, \ldots, m_n) \\ &= (0, \cdots, 0, m_{\alpha(m)} - 1, m_{\alpha(m)+1}, \cdots, m_n) \end{aligned} \tag{33}$$

In a more compact form, (31) can be written as

$$\begin{aligned} L_m \stackrel{\text{def}}{=} & \sum_{\substack{i \in N \\ s \in \{a,w\}}} (failL_s^i, \top).L_{m_1,\cdots,m_{i-1},m_i+1,m_{i+1},\cdots,m_n} \\ & + (acc^{\alpha(m)}, \top).L_{\Lambda(m)}|_{\alpha(m)>0} \end{aligned} \tag{34}$$

From the above, we know that there are in total $N_q^p = \prod_{i=1}^{n}(N_i + 1)$ PEPA component equations to describe the queue. For $n = 2, N_i = 2, i = 1, 2$, we have $N_q^p = 9$.

### D. System Behavior

*1) Components for Sending Signals:* To facilitate cooperation between PEPA components for availability evaluation, we need to send signals when the system state changes. Such signals should be sent out immediately after the system enters into a new state, so we assign a sufficiently large activity rate, $\epsilon$, to associated activities. This large rate means that the probability that these activities do not win in the race condition is negligibly small.

For generating PEPA component definitions for the system states, we can first generate $S$ by enumeration, and then reduce the space by deleting all those equations that do not satisfying the constraint (18). In the sequel, we will refer to $S$ as the reduced state space.

Thus, for each $s \in S$, we define a PEPA component

$$G_s \stackrel{\text{def}}{=} (G : I_d(s), \epsilon).G_s' \tag{35}$$

where $G : I_d(s)$ is the action type used to send out the message about whether the system is in the down state. For example, $G : 1$ means that the system enters into a down state, while $G : 0$ means that the system enters into an up state.

Obviously, the number of PEPA components in (35) is equal to the number of states in $S$, which is at most $\prod_{j=1}^{n}(N_j+1)$.

*2) Components for Interaction with Groups:* To describe the dependence of system states on the states of its groups, for each $s = (l_f^1, \cdots, l_f^{i-1}, l_f^i, l_f^{i+1}, \cdots, l_f^n) \in S$, we define maps $\xi_i(s)$ and $\gamma_i(s)$ as follows:

$$\xi_i(s) = (l_f^1, \cdots, l_f^{i-1}, l_f^i + 1, l_f^{i+1}, \cdots, l_f^n)$$
$$\gamma_i(s) = (l_f^1, \cdots, l_f^{i-1}, l_f^i - 1, l_f^{i+1}, \cdots, l_f^n)$$

For notational brevity, let

$$s' = \xi_i(s) \qquad s'' = \gamma_i(s)$$
$$q' = q(s') \qquad q'' = q(s'')$$

where $q(s)$ is the integer defined by (10), i.e. the integer that identifies the active group with the lowest priority.

Then, the PEPA component associated with system state $s$ can be written as

$$\begin{aligned} G'_s \stackrel{\text{def}}{=} \sum_{i\in N} \Big[ & (fail_a^i, \top).(hot^{q'}, \epsilon).G_{s'}|_{s'\equiv u} \\ & + (fail_a^i, \top).\prod_{j=1}^{n}(freeze^j, \epsilon).G_{s'}|_{s'\equiv d} \\ & + (fail_w^i, \top).G_{s'} \\ & + (rep^i, \top).(hot^i, \epsilon).(warm^{q''}, \epsilon).G_{s''}|_{s\equiv u, s''\equiv u, i<q''} \\ & + (rep^i, \top).G_{s''}|_{s\equiv u, s''\equiv u, i\geq q''} \\ & + (rep^i, \top).\prod_{j=1}^{n}(defreeze_t^j, \epsilon).G_{s''}|_{s\equiv d, s''\equiv u} \Big] \end{aligned} \tag{36}$$

where $t$ is the number of frozen components that need to be put into the active state, which can be calculated as follows

$$t = \begin{cases} N_j - l_f^j & j < q'' \\ k - \sum_{r=1}^{q''-1}(N_r - l_f^r) & j = q'' \\ 0 & j > q'' \end{cases}$$

The terms in (36) are justified by the following explanations.

1) 1st term: when a system component of $G_i$ fails from the active up state, and the system is up before and after the failure, another component of group $G_{q'}$ should enter the active up state from the warm state. The index $q'$ is determined by relation (10). This term exists only if the resulting system state is up.
2) 2nd term: when a system component of $G_i$ fails from the active up state, and the system is down after the failure, components in the up state of all groups should enter the frozen state. This term exists only if the resulting system state is down.
3) 3rd term: when a system component of $G_i$ fails from the warm up state, there will be no influence on the states of other groups.
4) 4th term: when a system component of $G_i$ finishes repair, it will send a signal $rep^i$. If the system is in the up state before and after the event occurs, and the component has higher priority than a currently active up component, then it should enter into the active up state; thus a signal $hot^i$ is sent to group $G_i$, the replaced component (with the lowest priority among the currently active up components) is forced to enter the warm up state by the signal $warm^q$. This term exists only if the repaired component has higher priority than a currently active up component.
5) 5th term: when a system component of $G_i$ finishes repair, if the system is in the up state before and after the event occurs, and the component does not have higher priority than any currently active up component, then nothing needs to be done other than the number of failed components decreases by 1.
6) 6th term: when a system component of $G_i$ finishes repair, if the system then becomes up from the down state, then the first $k$ frozen components with highest priorities will enter the active up state; this is realized by sending out the signal $defreeze_t^j$ to group $G_j$ to let $t$ of its components enter the active up state, and the remaining components enter the warm up state.

Since each $s \in S$ is associated with a PEPA component definition, the total number PEPA components here is also at most $\prod_{j=1}^{n}(N_j+1)$.

### *E. Cooperations Between Components*

The complete PEPA model describes the dynamic behaviour of the system by integrating all the components via cooperations between them.

First, we define the following PEPA component to integrate all the group components. This is a parallel composition of components, one for each group as defined in (19).

$$\begin{aligned} BS \stackrel{\text{def}}{=} B^{1,u}_{N_1,0,0,0}|| \cdots ||B^{q-1,u}_{N_{q-1},0,0,0}||B^{q,u}_{N_q-h,h,0,0} \\ ||B^{q+1,u}_{0,N_{q+1},0,0}|| \cdots ||B^{n,u}_{0,N_n,0,0} \end{aligned} \tag{37}$$

where $q$ is given by

$$\sum_{j=1}^{q-1} N_j < k \leq \sum_{j=1}^{q} N_j \tag{38}$$

and $h = \left(\sum_{j=1}^{q} N_j\right) - k$. The definition reflects that all components are initially assumed to be in the up state and the first $k$ components are active whilst the remainder are initially warm and up.

Next, we define a PEPA component to integrate $BS$ with the system behavior component by using cooperative actions between them as defined below.

$$CoBS \stackrel{\text{def}}{=} BS \underset{L}{\bowtie} G_y \tag{39}$$

where the set of synchronising action types $L$ are defined to be

$$\begin{aligned} L = \{ & fail_a^i, fail_w^i, warm^i, hot^i, freeze^i, \\ & defreeze_j^i \mid i \in N, j \leq N_i\} \end{aligned} \tag{40}$$

and

$$y = \underbrace{(0, \cdots, 0)}_{n} \tag{41}$$

Finally, we need to define a PEPA component which combines $CoBS$ with the repair queue component and all the repair facility components. This is a cooperation between the various components which enforces synchronization on appropriate activities.

$$CoBQR \stackrel{\text{def}}{=} \left( CoBS \underset{\substack{i \in N \\ failL_s^i, failL_w^i}}{\bowtie} L_{\underbrace{(0,0,\cdots,0)}_{n}} \right) \underset{\substack{i \in N \\ acc^i, rep^i, repB^i}}{\bowtie} \left( \underbrace{V_\emptyset || \cdots || V_\emptyset}_{r} \right) \tag{42}$$

### F. Availability Evaluation

For availability evaluation, we introduce the following PEPA components

$$\begin{aligned} GSys_0 &\stackrel{\text{def}}{=} (G:1, \top).GSys_1 \\ GSys_1 &\stackrel{\text{def}}{=} (G:0, \top).GSys_0 \end{aligned}$$

where $GSys_0$ represents that the system is in the up state, and $GSys_1$ denotes that the system is in the down state.

For evaluating system availability, we define a PEPA component that reflects the system state changes depending on the dynamics of all the other components as follows:

$$CopGSys \stackrel{\text{def}}{=} GSys_0 \underset{\{G:0,G:1\}}{\bowtie} CoBQR \tag{43}$$

The availability of the system can then be calculated as the steady state probability of PEPA component $GSys_0$.

## V. Model Generation and Examples

### A. Tool for Generating PEPA model

We have implemented a tool which can automatically generate a PEPA model for a given generalized $k$-out-of-$n$: G warm standby system by following the generation rules introduced in this paper. Specifically, to describe a generalized $k$-out-of-$n$: G warm standby system, one only needs to write a fairly simple file which describes the value of $k$, the number of repair facilities $r$, and the active mode failure rate $\lambda_i$, warm mode failure rate $\lambda_i'$, repair rate $\mu_i$, number of components $N_i$ for each group in the following text format:

$k$
$r$
$\lambda_1, \lambda_1', \mu_1, N_1$
$\cdots$
$\lambda_n, \lambda_n', \mu_n, N_n$

This software tool is available for download at http://groups.inf.ed.ac.uk/paloma/k-out-of-n.jar. It is written in Java and can be run on any machine if JDK 6 or a higher version of Java is installed. The default value of $\epsilon$ is set to be 100 in the tool, but it can be easily replaced with another appropriate value in the generated PEPA file by using any text editor. The rule is that $\epsilon$ needs to be significantly larger than all the failure rates and repair rates of system components in applications.

The associated PEPA model can be generated by our tool using the following command:

java -jar k-out-of-n.jar filename

where filename is the directory of the description file for the generalized $k$-out-of-$n$: G warm standby system. The generated PEPA file can be directly parsed and analysed in the Eclipse environment once the PEPA analysis tool PEPA plugin (http://www.dcs.ed.ac.uk/pepa/documentation/ [6]) is installed.

The current PEPA plugin tool can provide the steady state probability of each PEPA component. Therefore, by using the generated PEPA model, we can readily also obtain other performance measures of the system. For example, if we are interested in the average idle probability of the repair facility, we can simply evaluate it as the steady state probability of $V_\emptyset$ in (28).

### B. Numerical Examples

To verify our modeling approach, we use the example presented in [39] by Zhang et al. The example is a 3-out-of-(2+2): G warm standby system with 2 repair facilities. The components are partitioned into two groups, each of which has two $s$-identical components. For components of the first group, the failure rate in either the active state or the warm standby state is 0.0007. For components of the second group, the failure rates in active state and warm standby state are 0.001 and 0.0005 respectively. The repair rates for components of the first and second group are 0.05, 0.03 respectively.

To build the PEPA model automatically, we write a text file as follows.

3
2
$0.0007, 0.0007, 0.05, 2$
$0.001, 0.0005, 0.03, 2$

Using our compiler, we transform this description into the input file for the PEPA plugin tool. By analyzing the model with the PEPA plugin tool, the system's stationary availability is calculated as 0.997579, which matches well with the result 0.9976 reported in [39]. Note that this result is obtained by numerical solution of the underlying CTMC, not by simulation.

For further verification, in addition to the above example, we consider a special case of $k$-out-of-$n$: G warm standby systems. Suppose the system is a 1-out-of-$n$ warm standby system with identical components, with failure rate in the active up state and warm standby state denoted as $\lambda$ and $\lambda'$ respectively, and the repair rate is $\mu$, then the availability of the system $A_s$ and the idle probability of repair facility $I_r$ can be solved by using the analytical method provided by Cao and Cheng in [48].

TABLE IV
PARAMETERS OF EXAMPLE SYSTEM

| Group No | failure rate in active state | failure rate in warm state | repair rate | Number of Components |
|---|---|---|---|---|
| 1 | 0.02 | 0.01 | 0.02 | 2 |
| 2 | 0.04 | 0.02 | 0.03 | 2 |
| 3 | 0.05 | 0.01 | 0.05 | 2 |
| 4 | 0.06 | 0.01 | 0.05 | 2 |
| 5 | 0.07 | 0.01 | 0.05 | 2 |

TABLE V
AVAILABILITIES RESULTS IN DIFFERENT CASES

| $r$ | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2 grps | 0.4178 | 0.4178 | 0.4178 | | | |
| 3 grps | 0.5235 | 0.6726 | 0.7360 | 0.7360 | 0.7360 | |
| 4 grps | 0.5401 | 0.7266 | 0.8322 | 0.8823 | 0.9013 | 0.9013 |
| 5 grps | 0.5440 | 0.7423 | 0.8631 | 0.9238 | 0.9517 | 0.9640 |

$$I_r = \{1 + \sum_{j=1}^{n} \frac{1}{\mu^j} \prod_{q=0}^{j-1} [\lambda + (n-q-1)\lambda']\}^{-1} \tag{44}$$

$$A_s = 1 - \frac{I_r}{\mu^n} \prod_{q=0}^{n-1} [\lambda + (n-q-1)\lambda'] \tag{45}$$

Assuming that $n = 1$, $N_1 = 5, k = 1$, and $r = 1$, then the system will become a 1-out-of-5 warm standby repairable system with only one component group, which has $s$-identical components. Letting $\lambda = 0.05$, $\lambda' = 0.02$, $\mu = 0.08$, and using (44), (45), we can obtain $A_s = 0.87443$, $I_r = 0.09135$. By our generated PEPA model and the PEPA plugin tool, setting $\epsilon = 100$ in the generated model (recall that $\epsilon$ is the rate of an activity which is effectively instantaneous; 100 was chosen as a suitable rate here as it is significantly larger than the other rates in the model), we obtain $A_s = 0.87439$, $I_r = 0.09172$. The difference between the results is mainly due to the approximation in the PEPA model since $\epsilon$ has a finite value. If $\epsilon = 1000$ in the generated model, we get $A_s = 0.87442$, $I_r = 0.09139$, which is closer to the previous analytical results derived by (44), (45).

To show the capability of our model in dealing with $k$-out-of-$n$: G warm standby systems with more component groups, we add 3 groups of components to the previous system discussed by Zhang et al. in [39] ; the parameters of the first two groups are changed but $k$ remains as 3. Table IV gives the parameters of the considered system.

To study the influence of the number of groups and repair facilities, we calculate the system availability with different numbers of repair facilities $r$ and increasing numbers of groups. The results of system availability are shown in Table V, where $i$ grps ($i = 2, 3, 4, 5$) means the system consisting of the first $i$ groups in Table IV,

From the results in Table V, we can see that the availability of the system will no longer increase when the number of repair facilities exceeds some value. This means that the repair is no longer the bottleneck in the system. For example, for the system consisting of the first three groups, after $r$ becomes 4, availability remains the same. This means that if the repair capability is sufficient, the availability will be mainly determined by the failure rates of the components. Moreover, we can observe that with a fixed number of repair facilities, the system availability will increase gradually with the number of groups, but not as significantly as by increasing $r$ when it is relatively small. In summary, we can see that for $k$-out-of-$n$: G warm standby systems, both the number of groups and the number of repair facillities are useful for improving the system availability, but after they are sufficiently large, increasing only one of them will have no obvious effect when the other remains the same. Table VI shows the total time cost to generate and solve the PEPA models for the different cases. All the experiments were run on a MacBook Pro laptop with 8 GB memory size and 2 GHz Intel Core i7.

TABLE VI
TIME COST IN DIFFERENT CASES (IN SECONDS)

| $r$ | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| 2 grps | 0.001 | 0.001 | 0.001 | | | |
| 3 grps | 0.01 | 0.01 | 0.01 | 0.01 | 0.01 | |
| 4 grps | 0.22 | 0.24 | 0.30 | 0.35 | 0.36 | 0.37 |
| 5 grps | 7.89 | 8.73 | 9.97 | 10.27 | 11.48 | 13.01 |

## VI. CONCLUSION

Availability modeling of warm standby repairable systems with non-identical components is a challenging topic due to strong interdependencies and system dynamics. In contrast to the conventional Markov chain modeling approach in existing literature, our PEPA-based modeling approach can avoid the difficulty in directly establishing the high dimensional generator matrix of the Markov chain, whose elements depend on the state dynamics of the components. In essence, direct construction of the generator matrix is a flat modeling approach, whereas PEPA is a compositional modeling approach, which can describe the whole system by integrating models of its subsystems with different levels of action cooperations. This makes the modeling process relatively clear, in a logical way. In addition, as the resulting PEPA model has compositional structure, we can also obtain other performance measures like idle probability of the repair facility using the PEPA modeling and analysis tools.

However, there are also some limitations of our approach. Firstly, our research in this paper does not consider more complex cases with imperfect coverage, switching and sensing failures, common cause failures, components with different repair rates for failures from active up states and warm up states. Secondly, due to the current limitations of the PEPA tool, we are unable to provide reliability evaluation results. Thirdly, although our approach avoids the direct construction of the high dimensional infinitesimal generator of the CTMC, and hands this job over to the PEPA tool, the state explosion problem of the CTMC model still exists in solving the model using the PEPA tool. The scale of the model that can be solved will depend on the capability of specific computer running

the software. More efficient algorithms for solving large scale CTMCs are still needed. Therefore, with respect to availability and reliability modeling of warm standby systems using PEPA, much interesting and meaningful research is anticipated.

## ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their helpful comments and suggestions.

## REFERENCES

[1] A. Birolini, *Reliability engineering: Theory and Practice*, 5th ed. Berlin Heidelberg: Springer, 2007.

[2] S. Amari, H. Pham, and R. Misra, "Reliability characteristics of k-out-of-n warm standby systems," *IEEE Transactions on Reliability*, vol. 61, no. 4, pp. 1007–1018, 2012.

[3] R. D. Yearout, P. Reddy, and D. L. Grosh, "Standby redundancy in reliability - a review," *IEEE Transactions on Reliability*, vol. 35, no. 3, pp. 285–292, 1986.

[4] J. She and M. Pecht, "Reliability of a k-out-of-n warm-standby system," *IEEE Transactions on Reliability*, vol. 41, no. 1, pp. 72–75, 1992.

[5] G. Levitin, L. Xing, and Y. Dai, "Reliability of non-coherent warm standby systems with reworking," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 444–453, 2015.

[6] M. Tribastone, A. Duguid, and S. Gilmore, "The PEPA Eclipse plugin," *ACM SIGMETRICS Performance Evaluation Review*, vol. 36, no. 4, pp. 28–33, 2009.

[7] B. Dhillon and N. Yang, "Reliability and availability analysis of warm standby systems with common-cause failures and human errors," *Microelectronics Reliability*, vol. 32, no. 4, pp. 561–575, 1992.

[8] D. Kececioglu and S. Jiang, "Reliability of a repairable standby system with imperfect sensing and switching," in *Proceedings of Annual Reliability and Maintainability Symposium*, 1990, pp. 260–267.

[9] I. Yusuf and B. Gimba, "Modeling and evaluation of MTSF of 2-out-of-5 warm standby repairable system with replacement at common cause failure," *Applied Mathematical Sciences*, vol. 7, no. 129, pp. 6403–6415, 2013.

[10] G. Arulmozhi, "M out of N reliability system with s warm standby spares," in *Proceedings of the National Conference on Mathematical and Computationa Models*, R. Nadarajan and P. Kandasamy, Eds., PSG College of Technology. Coimbatore, INDIA: Allied Publishers Ltd., 2001, pp. 108–115.

[11] Y. Pang, H.-Z. Huang, Y. Liu, and M. Xie, "A systematic approach to the reliability analysis of an n-unit warm standby system with k-repair facility," in *ASME 2009 International Design Engineering Technical Conferences and Computers and Information in Engineering Conference*. American Society of Mechanical Engineers, 2009, pp. 679–684.

[12] J.-C. Ke and K.-H. Wang, "The reliability analysis of balking and reneging in a repairable system with warm standbys," *Quality and Reliability Engineering International*, vol. 18, no. 6, pp. 467–478, 2002.

[13] M. Jain and G. Sharma, "Reliability analysis of k-out-of n: G machining systems with mixed spares and multiple modes of failure (technical note)," *International Journal of Engineering-Transactions A: Basics*, vol. 20, no. 3, pp. 243–250, 2007.

[14] K.-H. Wang, J.-B. Ke, and W.-C. Lee, "Reliability and sensitivity analysis of a repairable system with warm standbys and r unreliable service stations," *The International Journal of Advanced Manufacturing Technology*, vol. 31, no. 11-12, pp. 1223–1232, 2007.

[15] L. Yuan and X.-Y. Meng, "Reliability analysis of a warm standby repairable system with priority in use," *Applied Mathematical Modelling*, vol. 35, no. 9, pp. 4295–4303, 2011.

[16] L. Bulama, I. Yusuf, and S. I. Bala, "Stochastic modeling and analysis of some reliability characteristics of a repairable warm standby system," *Applied Mathematical Sciences*, vol. 7, no. 118, pp. 5847–5862, 2013.

[17] B. Dhillon, "Reliability and availability analysis of a system with warm standby and common cause failures," *Microelectronics Reliability*, vol. 33, no. 9, pp. 1343–1349, 1993.

[18] E. J. Vanderperre, "Long-run availability of a warm standby system," *Mathematical Notes*, vol. 84, no. 5-6, pp. 623–630, 2008.

[19] A. Mishra and M. Jain, "Availability of k-out-of-n: F secondary subsystem with general repair time distribution," *International Journal of Engineering-Transactions A: Basics*, vol. 26, no. 7, pp. 743–752, 2013.

[20] E. J. Vanderperre, "Point availabilty of a warm standby system," *International Journal of Pure and Applied Mathematics*, vol. 74, no. 2, pp. 235–249, 2012.

[21] M. El-Damcese and N. El-Sodany, "Availability analysis of the k-out-of-n: G system using markov model and supplementary variable technique," *International Journal of Scientific & Engineering Research*, vol. 5, no. 12, pp. 653–663, 2014.

[22] E. J. Vanderperre and S. S. Makhanov, "On the availability of a warm standby system: a numerical approach," *Top*, vol. 22, no. 2, pp. 644–657, 2014.

[23] J. E. Ruiz-Castro and G. Fernández-Villodre, "A complex discrete warm standby system with loss of units," *European Journal of Operational Research*, vol. 218, no. 2, pp. 456–469, 2012.

[24] C. E. Wells, "Reliability analysis of a single warm-standby system subject to repairable and nonrepairable failures," *European Journal of Operational Research*, vol. 235, no. 1, pp. 180–186, 2014.

[25] S. Srinivasan and R. Subramanian, "Reliability analysis of a three unit warm standby redundant system with repair," *Annals of Operations Research*, vol. 143, no. 1, pp. 227–235, 2006.

[26] K. Soni, U. Singh, and R. Jha, "Mathematical analysis of reliability of M out of N warm stand by system with repair facilities," *International Journal of Advance Research and Innovation*, vol. 2, no. 4, pp. 745–749, 2014.

[27] T. Zhang and M. Horigome, "Availability of 3-out-of-4: G warm standby system," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 83, no. 5, pp. 857–862, 2000.

[28] X. Li, R. Yan, and M. J. Zuo, "Evaluating a warm standby system with components having proportional hazard rates," *Operations Research Letters*, vol. 37, no. 1, pp. 56–60, 2009.

[29] E. Papageorgiou and G. Kokolakis, "Reliability analysis of a two-unit general parallel system with (n-2) warm standbys," *European Journal of Operational Research*, vol. 201, no. 3, pp. 821–827, 2010.

[30] Q. Zhai, R. Peng, L. Xing, and J. Yang, "Binary decision diagram-based reliability evaluation of k-out-of-(n+ k) warm standby systems subject to fault-level coverage," *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, vol. 227, no. 5, pp. 540–548, 2013.

[31] R. Peng, Q. Zhai, L. Xing, and J. Yang, "Reliability of 1-out-of-(n+ 1) warm standby systems subject to fault level coverage," *International Journal of Performability Engineering*, vol. 9, no. 1, pp. 117–120, 2013.

[32] S. Eryilmaz, "Reliability of a k-out-of-N system equipped with a single warm standby component," *IEEE Transactions on Reliability*, vol. 62, no. 2, pp. 499–503, 2013.

[33] W. Huang, J. Loman, and T. Song, "A reliability model of a warm standby configuration with two identical sets of units," *Reliability Engineering & System Safety*, vol. 133, pp. 237–245, 2015.

[34] S. Li, S. Sun, S. Si, S. Zhang, and H. Dui, "Decision diagram based methods and reliability analysis for k-out-of-n: G systems," *Journal of Mechanical Science and Technology*, vol. 28, no. 10, pp. 3917–3923, 2014. [Online]. Available: http://dx.doi.org/10.1007/s12206-014-0902-z

[35] G. Levitin, L. Xing, and Y. Dai, "Mission cost and reliability of 1-out-of-N:G warm standby systems with imperfect switching mechanisms," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 44, no. 9, pp. 1262–1271, 2014.

[36] ——, "Non-homogeneous 1-out-of-N warm standby systems with random replacement times," *IEEE Transactions on Reliability*, 2015, early Access.

[37] ——, "Heterogeneous 1-out-of-N warm standby systems with dynamic uneven backups," *IEEE Transactions on Reliability*, no. 99, pp. 1–15, 2015, early Access.

[38] ——, "Reliability and mission cost of 1-out-of-N:G systems with state-dependent standby mode transfers," *IEEE Transactions on Reliability*, vol. 64, no. 1, pp. 454–462, 2015.

[39] T. Zhang, M. Xie, and M. Horigome, "Availability and reliability of k-out-of-(M+N): G warm standby systems," *Reliability Engineering & System Safety*, vol. 91, no. 4, pp. 381–387, 2006.

[40] A. Khatab, N. Nahas, and M. Nourelfath, "Availability of K-out-of-N: G systems with non-identical components subject to repair priorities," *Reliability Engineering & System Safety*, vol. 94, no. 2, pp. 142–151, 2009.

[41] W. Jian, H. Wang, and G. Zhao, "Formal modeling and quantitative evaluation for information system survivability based on PEPA," *The Journal of China Universities of Posts and Telecommunications*, vol. 15, no. 2, pp. 88–113, 2008.

[42] X. Yang, R. Han, Y. Guo, J. Bradley, B. Cox, R. Dickinson, and R. Kitney, "Modelling and performance analysis of clinical pathways using

the stochastic process algebra PEPA," *BMC bioinformatics*, vol. 13, no. Suppl 14, p. S4, 2012.
[43] J.-M. Fourneau, L. Kloul, and F. Valois, "Performance modelling of hierarchical cellular networks using PEPA," *Performance Evaluation*, vol. 50, no. 2, pp. 83–99, 2002.
[44] B. Yan, X. Wu, and Y. Fu, "Reliability prediction for network systems using stochastic process algebra," *Journal of Xi'an Jiaotong University*, vol. 6, p. 008, 2011 (in Chinese).
[45] L. Kloul, "From DFTs to PEPA: A model-to-model transformation," in *Proceedings of the 6th European Performance Engineering Workshop on Computer Performance Engineering*. Berlin, Heidelberg: Springer-Verlag, 2009, pp. 94–109.
[46] J. Hillston, *A Compositional Approach to Performance Modelling*. Cambridge University Press, 2005, vol. 12.
[47] K. Rosen, *Discrete Mathematics and Its Applications 7th edition*. McGraw-Hill, 2011.
[48] J. Cao and K. Cheng, *Introduction to Reliability Mathematics*, 1st ed. Beijing: Science Press, 1986 (in Chinese).

**Xiaoyue Wu** Xiaoyue Wu received the B.S. degree in 1984, and the M.S. degree in 1987 in Water Resource Engineering from Tsinghua University, Beijing, China. He received the Ph.D. degree in Management Science and Engineering from National University of Defense Technology, Changsha, China, in 2000. He was a visiting scholar at the Department of Mechanical and Industrial Engineering (MIE) , the University of Toronto, Canada, from December 2002 to December 2003, and an academic visitor at the Laboratory for Foundations of Computer Science (LFCS) from May 2014 to May 2015, at the University of Edinburgh, UK. He is currently a Professor at the College of Information Systems and Management, National University of Defense Technology, China. His main research interests include reliability modeling and evaluation of complex systems, decision analysis under uncertainty.

Prof. Wu is the president of the Reliability Committee of the Operations Research Society of China (RORSC).

**Jane Hillston** Jane Hillston received a B.A. degree in Mathematics from the University of York, England in 1985, and a M.S. degree in Mathematics from Lehigh University, U.S.A., in 1987. She received the Ph.D. degree in computer science in 1994 from the University of Edinburgh, where she is currently working as Professor of Quantitative Modelling. Her principal research interests are in the use of stochastic process algebras to model and analyze dynamic systems.

Prof. Hillston was awarded the first Roger Needham Award in 2004 by the British Computer Society in recognition of her work on PEPA. She was elected to fellowship of the Royal Society of Edinburgh in 2007.

**Cheng Feng** Cheng Feng received a B.Eng. degree in Computer Science and Technology from Beijing Language and Culture University, China, in 2011, and a M.S. degree in Computer Science from the University of Edinburgh, UK, in 2012. He is currently a Ph.D. student supervised by Professor Jane Hillston and Professor Gordon Plotkin in the School of Informatics at the University of Edinburgh, UK. His research interests are in the use of stochastic process algebras to describe large-scale spatial population models and scalable techniques for analysing such models.