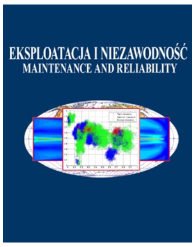


Eksploatacja i Niezawodnosc – Maintenance and Reliability

Volume 24 (2022), Issue 2

journal homepage: http://www.ein.org.pl

Article citation info:
Zhao J, Zhang Z, Xu T, Cao X, Wang Q, Cai Z. Defensive strategy optimization of consecutive-k-out-of-n systems under deterministic external risks. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2022; 24 (2): 306–316, http://doi.org/10.17531/ein.2022.2.12.

Defensive strategy optimization of consecutive-k-out-of-n systems under deterministic external risks

Indexed by:
Web of Science Group

Jiangbin Zhao[a], Zaoyan Zhang[a], Tianbo Xu[a], Xiangang Cao[a,*], Qiyu Wang[b], Zhiqiang Cai[b]

[a]Xi'an University of Science and Technology, Department of Intelligence Manufacturing, School of Mechanical Engineering, No. 58 Yanta Road, Beilin District, Xi'an Shaanxi, 710054, China
[b]Northwestern Polytechnical University, Department of Industrial Engineering, School of Mechanical Engineering, No. 127 West Youyi Road, Beilin District, Xi'an Shaanxi, 710072, P.R.China

Highlights

- A defensive capability based on real-time reliability is developed for Con/k/n systems.
- Defensive importance measure is constructed to optimize component redundancy locally.
- The effectiveness of DIMGA is verified by comparing it with CGA under 36 scenarios.
- Con/k/5 systems' redundancy distribution rule under spacing/continuous risk is analyzed.

Abstract

Consecutive-k-out-of-n (Con/k/n) system, a reconfigurable system, can improve the system performance by adjusting the redundancy and assignment of components. This paper aims to determine the optimal defensive strategy of Con/k/n systems under external risks. The defensive capability of Con/k/n systems is evaluated based on real-time system reliability, and a defensive importance measure (DIM) is constructed to optimize components' redundancy locally. To solve the proposed optimization model effectively, a DIM-based genetic algorithm (DIGA) is developed by integrating the advantages of DIM's local search with the global search ability of the classical genetic algorithm (CGA). The numerical experiment under 36 scenarios illustrates that DIGA is more effective than CGA verified by average defensive capability, robustness, and convergence generations. Moreover, the redundancy distribution analysis of Con/k/5 systems in the optimal defensive strategy shows that the redundancy of F(G) systems is in a spaced (continuous) way under spacing *k*-1 risk or continuous *k* risk.

Keywords

consecutive-k-out-of-n system, external risks, defensive capability, strategy optimization, redundancy distribution.

1. Introduction

Defensive strategies (redundancy and assignment of components) are essential to prevent severe catastrophic events, decreasing economic losses from many other disasters. Some scholars have studied the negative effect of risk on the system performance, and the reported research work verified that effective defensive strategy can resist the degradation of system performance [8, 9, 33, 37]. So, risk events may cause enormous losses for the government when the defensive strategy is not appropriate. For example, the fires in New South Wales burned for 210 days before being wholly extinguished on July 18, 2019, burning 400 hectares, killing 33 people and more than 1 billion animals, and destroying 2,500 homes. Consecutive-k-out-of-n (Con/k/n) system is arranged in a line consisting of *n* ordered components, involving the F system and G system, and the F(G) system fails(works) if and only if at least consecutive *k* components fail (work). Con/k/n system is widely used in quality control systems[21], flow transfer systems[40], sensor detection systems [16], production monitoring systems (PMS) [36], communication systems[17], performance-sharing heating systems [38], and other applications[29]. Moreover, Con/k/n systems are reconfigurable systems whose performance can be improved by changing components' positions, adding redundant components, or replacing components, which gives Con/k/n systems a more flexible way to protect against external risks. Therefore, it is necessary to evaluate the defensive capability of Con/k/n systems considering defensive strategies.

System resilience is an important indicator to evaluate the system's ability to resist degradation or recover to its normal state[35]. The resilience assessment methods can be divided into three types: time-based resilience, performance-based resilience, and data-based resilience. Time-based resilience indexes consider the habitable time, travel time, or recovery time. The length of time that a building can remain habitable after a prolonged power outage during extended periods of extreme weather is regarded as passive survivability to evaluate the thermal resilience of buildings [28]. By integrating and assessing the effect of recovery controls, time-based resilience is proposed to identify the impact of the evolution of recovery overtime on the critical

(*) Corresponding author.

E-mail addresses: J. Zhao (ORCID: 0000-0002-3034-6710): zhaojiangbin@xust.edu.cn, Z. Zhang (ORCID: 0000-0002-0003-3393): zhangzaoyan@stu.xust.edu.cn, T. Xu (ORCID: 0000-0002-5393-9252): xutianbo@xust.edu.cn, X. Cao (ORCID: 0000-0002-4799-9654): xgcao_xust@163.com, Q. Wang (ORCID: 0000-0002-4385-8176): wangqiyu@mail.nwpu.edu.cn, Z. Cai (ORCID: 0000-0002-7380-8110): caizhiqiang@nwpu.edu.cn

path [31]. A new time-based resilience measure is defined as the ratio of the integral of the normalized system performance within its maximum allowable recovery time after the disruption to the integral of the performance in the normal state [18]. The resilience of rail transit network under incidents is defined as the speed of rail transit network recover from the worst network performance under incidents to its original state by considering the waiting time, in-vehicle travel time, and transfer time [24]. Performance-based resilience is evaluated by considering the system states or functionality loss. A performance-based resilience assessment method is proposed for engineered systems through functionality loss and associated monetary costs [26]. A combined probabilistic framework is established by analyzing limit states associated with performance levels [3]. A quantitative framework for assessing system resilience is proposed by focusing on absorption, recovery, and adaptation to disruptions [34]. Data-based resilience is evaluated by utilizing the raw data to simulate the uncertainty of risk events. A data envelopment analysis framework for dynamic networks is developed by combining quality function deployment with a decision-making trial and evaluation laboratory to assess the system resilience [30]. A data-based uncertainty set is built to randomly generate the historical or forecast information of extreme weather events to measure system resilience [22]. Apriori-based disruption generator is established to simulate the disruption and its propagation based on real-life data, which can assess the system resilience accurately [13]. With the consideration of Con/k/n systems' characteristics, the real-time system reliability of Con/k/n systems considering the component redundancy and component assignment is available for evaluating the system resilience. So, the defensive capability of Con/k/n systems is a system ability to resist system performance degradation, which is the system resilience in preparation and responsive phases.

Increasing or enhancing the system resilience is one of the most heated topics under destructive disasters. The resilience of the transportation network under a disaster is measured, and the resilience optimization model under configuration cost and crossing time constraints is constructed [20]. An adaptive robust optimization-based framework is developed to enhance the resilience of the interdependent critical infrastructure systems, which can evaluate the potential impacts of natural hazards on an infrastructure [11]. A tri-level protection-interdiction-restoration problem for interdependent networks is proposed to optimize system resilience [12]. A model is constructed to analyze and optimize the network resilience by machine learning to improve customer experiences at lower operational expenses [14]. System resilience can be increased by reinforcing the weakest components to maximize the system resilience under a cost constraint [1]. An integrated method is established to get the resilience enhancement strategies of interdependent critical infrastructures by combining the hierarchical model with a predictive control-based dynamic model [23]. A two-stage stochastic mixed-integer linear programming method is developed to optimize the preparation and resource configuration to enhance the resilience of power distribution systems [43]. The quantitative measures of the cyber-physical power system resilience applied in the existing literature are summarized, and the optimization of system resilience focused on the optimal recovery sequence of components, identification and protection of critical nodes, and the enhancement of the coupling patterns between physical and cyber networks [39]. A comprehensive review of transmission networks focuses on the optimization models and methodologies to enhance the grid resilience by reconfiguration methods [4].

Importance theory is an effective tool to identify the weak links of system design, maintenance, and resource allocation, which can help reliability engineers quickly make the best decisions [32]. Importance measure (IM) can improve the solving efficiency of complex optimization problems in maintenance strategy[7, 42], and many scholars are utilizing IMs to enhance system resilience. Two IMs are proposed to enhance the system resilience by allocating resources to reduce their vulnerability or expedite their recovery [2]. The importance ranking of nodes in interdependent infrastructure networks is used in a heuristic algorithm to rank and prioritize infrastructure links, which can support decision-making for designing and managing the system resilience [6]. The resilience-based component importance for multi-state networks qualifies the impact of a component's capacity improvement and recovery time on network resilience. The importance ranking of components determines the minimal recovery path based on a stochastic ranking method [41]. Resilience-based component importance is introduced to optimize the infrastructure resilience under budgetary constraints [27]. The residual resilience-based IM is used to evaluate the importance of ports and routes by the Copeland method, and the restoration priority based on IM is developed to minimize the residual resilience [10]. The recovery priority of failed components after a disaster in the power grid system is determined by the IM, which is the influence of the failed components on the power grid resilience [5]. A series of component resilience IMs, evaluated by the Monte Carlo-based method, is used in a transportation network to reasonably allocate limited resources[19].

As illustrated by the existing literature, many studies have focused on evaluating resilience for networks and enhancing system resilience. However, the existing system resilience assessment cannot evaluate the resilience of Con/k/n systems. In recent years, the research on resilience importance measures has been increasingly used in various strategies of enhancing system resilience. In this paper, Con/k/n system is a kind of reconfigurable system having many flexible ways to improve the system reliability, so the defensive capability analysis of Con/k/n systems based on the real-time system reliability is important to remain the system at a better performance level. The defensive strategy optimization model facing external risks under limited cost constraints is then presented. The proposed model's decision variables (component redundancy and component assignment) are too tedious or difficult to achieve. The defensive importance measure is introduced to find the best redundancy adjustment using its advanced local search ability. The defensive importance measure-based optimization algorithm is developed by integrating the advantages of defensive importance measure (local search ability) and genetic algorithms (global search ability).

The remainder of this paper is organized as follows. Section 2 introduces the defensive strategy optimization under external risks. Section 3 describes the detailed process of defensive IM-based genetic algorithm (DIMGA). Section 4 compares the performance of DIMGA and classical genetic algorithm (CGA). In Section 5, numerical experiments of Con/k/n systems are implemented to analyze the redundancy distribution of the optimal defensive strategy under the continuous or spacing risks. Finally, the research results and future research are summarized in Section 6.

2. Defensive strategy optimization under external risks

In order to clearly explain the calculation process of the defensive capability of Con/k/n systems, some assumptions are summarized as follows.

(1) The system and all components have two states, working or failure.
(2) Components are independent of each other, and their lifetimes obey the Weibull distribution.
(3) The external risk mainly affects the shape parameters and scale parameters of components' lifetime distributions.
(4) The impact degree on different positions depends on the external risks' direction, intensity, and occurrence time.
(5) The defensive strategy involves the redundancy and assignment of the component module.

2.1. Defensive capability of Con/k/n systems

The system defensive capability is a function related to the assignment and redundancy of components, the lifetime of components, and environmental information. The defensive capability in $[0,t_d]$ of

Con/k/n systems is the ratio of the area enclosed by the actual system reliability and time axis to the area enclosed by the ideal system reliability and time axis. In order to describe the defensive capability clearly, Figure 1 depicts that the actual real-time system reliability $R_1(t)$ decreases over time, and the area between the actual system reliability curve and the ideal system reliability represents the performance loss. Moreover, the ideal system reliability $R_0(t)=1$. Therefore, the defensive capability of Con/k/n systems is calculated by Equation (1):

Therefore, the defensive capability of Con/k/n systems is calculated by Equation (1):

$$f^R(t)=\frac{\int_0^t R_1(t)dt}{\int_0^t R_0(t)dt}=\frac{\int_0^t R_1(t)dt}{t}\approx\frac{\Delta t\cdot\sum_{l=1}^{N_0}R_1(l\Delta t)}{N_0\Delta t}\approx\frac{\sum_{l=1}^{N_0}R_1(l\Delta t)}{N_0},(0\le t\le t_d) \tag{1}$$

where $f^R(t)$ is the defensive capability of the Con/k/n system at time *t*; N_0 is the number of strips with the same width in the interval [0, *t*], and the time length of each strip is $\Delta t\approx t/N_0$, so $\int_0^t R_1(t)dt\approx\Delta t\cdot\sum_{l=1}^{N_0}R_1(l\Delta t)$.

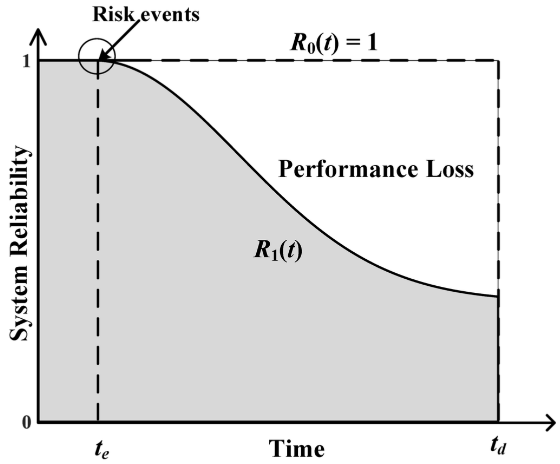


Fig. 1. Actual and ideal real-time system reliability over time

The real-time reliability of the Con/k/n: F system with redundant components can be calculated by Equation (2) [15]:

$$R_1^F(t)=R_l^F(t,n,k,x_{ij},n_i,t_i)=R_l^F(t,n-1,k,x_{ij},n_i,t_i)$$
$$-R_l^F(t,n-k-1,k,x_{ij},n_i,t_i)p_{n-k}^s(t)(\prod_{i=n-k+1}^n q_i^s(t)) \tag{2}$$

where n is the number of component modules; n_i is the number of redundant components in module *i*; x_{ij} represents component module *i* is placed in position *j*; $p_j^s(t)=\sum_{i=1}^n x_{ij}\left(1-\left(1-p_i\left(t\right)\right)\left(1-p_i\left(\max(t-t_i,0)\right)\right)^{n_i}\right)$ is the reliability of component module *i* placed in position *j* at time *t*; $p_i(t)$ is the reliability of component *i* at time *t*, and t_i is the occurrence time of risk, which is regarded as the activation time of redundant components in component module *i*; $R_l^F(t,n,k,x_{ij},n_i)$ is the system's reliability at time *t* for Con/k/n: F system when component redundancy n_i and assignment of component module x_{ij} are known. Particularly, $R_1^F(t)$=1 when $n<k$.

Similarly, the real-time reliability of the Con/k/n: G system with component modules can be calculated by Equation (3) [15]:

$$R_1^G(t)=R_l^G(t,n,k,x_{ij},n_i,t_i)=R_l^G(t,n-1,k,x_{ij},n_i,t_i)$$
$$+Q_l^G(t,n-k-1,k,x_{ij},n_i,t_i)q_{n-k}^s(t)(\prod_{i=n-k+1}^n p_i^s(t)) \tag{3}$$

where $q_j^s(t)=1-p_j^s(t)$; $R_l^G(t,n,k,x_{ij},n_i)$ is the system's reliability at time *t* for Con/k/n: G system; $R_1^G(t)$=0 when $n<k$.

2.2. Detailed description of external risks

The detailed risk information is shown in Figure 2. Three types of external risks include continuous risks, equal spacing risks, and non-equal spacing risks. The continuous risk means all the affected positions are continuous; equal spacing risk means the distance between two adjacent affected positions is the same, while the non-equal spacing risk is different. The risk pattern defines the travel direction and risk effects: Pattern I means risks occur simultaneously with the same intensity; Pattern II means risks transits from left to right, and the position at the left side occurs earlier with stronger intensity; Pattern III is the opposite of Pattern II. So, the external risk mainly affects the components' lifetime distribution parameters in different positions. The impact degree depends on the occurrence time and intensity of risks, which is related to the risk pattern.

2.3. Defensive strategy optimization under external risks

When the external risk information (occurrence time, risk types, risk patterns, and risk effects) is known, the defensive strategy optimization model can be constructed by considering the objective function, decision variables, and constraints. The objective is to maximize the defensive capability of Con/k/n systems, which can be calculated by Equation (1). The decision variable is the defensive strategy, including the redundancy and assignment of components. The constraints mainly come from the position restriction of components, the reliability limitations of components, the defensive cost, etc. Therefore, the mathematical model of defensive strategy optimization under external risks is listed as follows.

$$\max: f^R(x_{ij},n_i\,|\,t_i,t,n,k,\alpha_i,\beta_i) \tag{4}$$

$$\text{s.t. } \sum_{j=1}^n x_{ij}=1,(i=1,2,\cdots,n) \tag{5}$$

$$\sum_{i=1}^n x_{ij}=1\,,(i=1,2,\cdots,n) \tag{6}$$

$$p_j^s(t)=\sum_{i=1}^n x_{ij}\left(1-\left(1-p_i\left(t\right)\right)\left(1-p_i\left(\max(t-t_i,0)\right)\right)^{n_i}\right) \tag{7}$$

$$p_i\left(t\right)=\begin{cases} e^{-(t/\alpha_i)^{\beta_i}} & t\le t_i \\ e^{-((t\text{-}t_i)/a_i\alpha_i)^{b_i\beta_i}} & t>t_i \end{cases} \tag{8}$$

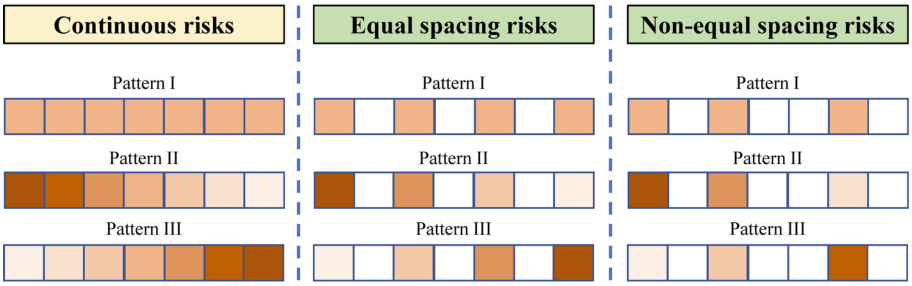


Fig. 2. The types and patterns of external risks

$$\sum_{i=1}^{n} c_i(n_i+1) \le C_0 \tag{9}$$

Equation (4) points out the decision variables (assignment of component module x_{ij} and component redundancy n_i) and the evaluation method of the system defensive capability; Equation (5) states that component module *i* can only select one position and Equation (6) means that position *j* can only accept one component module, and these two constraints are used to determine the unique assignment of components; Equation (7) defines the reliability of component modules at the position *j* at time *t*; Equation (8) evaluates the component reliability at time *t* in component module *i*; Equation (9) represents the constraints of defensive cost for achieving the specific defensive strategy. Where c_i is the unit price of component *i* and its redundant components; C_0 is the maximum cost of defensive configuration; n_i is the redundant level of component *i,* so the defensive cost of component module *i* is equal to $c_i(n_i+1)$.

3. Defensive IM-based genetic algorithm

To better obtain the optimal defensive strategy, a DIMGA is developed by combining the advantages of genetic algorithm and DIM.

3.1. The definition of DIM

DIM is defined as the change in system defensive capability after adding a redundant component, and the calculation method is shown as follows:

$$I_R^D(i\,|\,n_i,t) = f^R(n_i+1,t) - f^R(n_i,t) \tag{10}$$

where $I_R^D(i|n_i,t)$ is the DIM of component *i* at time *t* when its redundancy level is n_i; $f^R(n_i+1,t)$ is the system defensive capability after adding a redundant component for component *i* at time *t*.

3.2. DIM-based genetic algorithm

CGA is a general and famous algorithm with the standard process to solve various optimization problems. Therefore, the flow chart of DIMGA is developed based on the CGA, shown in Figure 3, and some key subprocesses of DIMGA are introduced in detail as follows.

(1) Real-number encoding method

A $2\times n$ matrix with real-number elements can represent a possible defensive strategy. The first row represents the arrangement of component modules, and the second row is the redundancy level of component modules.

(2) Crossover operations

The algorithm uses the single-point crossover to recombine genes of two individuals. If the recombinant genes are not adjusted, duplicate genes may appear in an individual, which is not allowed in a component arrangement. The detailed adjustment method to eliminate the duplicate genes is listed as follows. The missing genes in the component arrangement are identified at first, and then the selected genes with the larger serial number are randomly assigned to the available positions.

(3) Mutation operation

Mutation operation is to adjust the gene of an individual according to the mutation probability p_m. If the generated random number in [0, 1] is larger than p_m, the individual does not perform the mutation. Otherwise, select a mutation point from two rows in an individual: if the mutation point is in the first row, exchanging the component at the mutation point with other components; if the mutation point is in the second row, randomly selecting a component and reducing its redundancy by one.

(4) DIM-based local search method.

The DIM-based local search method is used to adjust the redundancy of components, which is a two-step adjustment method. The first step is to find the component module with the least reduction of system defensive capability when reducing a redundant component of this module; the second step is to add a redundant component for a component module with the largest DIM under the condition of cost constraints.

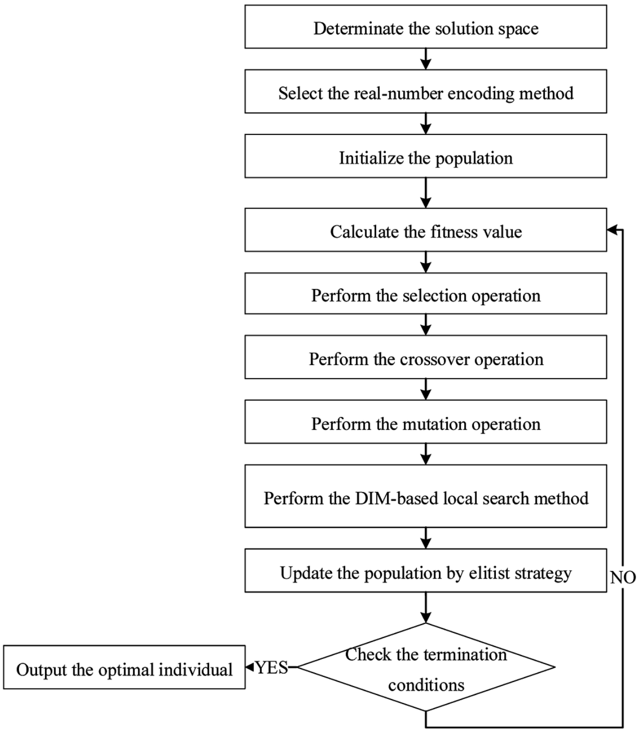

Determinate the solution space
Select the real-number encoding method
Initialize the population
Calculate the fitness value
Perform the selection operation
Perform the crossover operation
Perform the mutation operation
Perform the DIM-based local search method
Update the population by elitist strategy
NO
Check the termination conditions
YES
Output the optimal individual

Fig. 3 The flowchart of DIMGA

- For each individual in the population, perform the following operations, which is the detailed process of the DIM-based local search method.
- Randomly generate a number in the interval [0, 1]. If it is greater than the specified local search probability p_l, go to the next step; otherwise, output the initial individual.
- Select the component module by $i^* = \arg\max\{i\,|-I_R^D(i\,|\,n_i-1,t), i=1,2,\cdots,n\}$, and reduce one redundant component in module *i*.
- Under the cost constraint, select the component module j^* with the largest DIM by $j^* = \arg\max\{j\,|-I_R^D(j\,|\,n_j, n_{i^*}-1,t), c_j \le c_{i^*}, j=1,2,\cdots,n\}$, and add one redundant component for the component module j^*.

(5) Termination conditions. One is the maximum running generations, and the other is the maximum continuous generations in which the solution is unchanged. The algorithm stops if either of the two termination conditions is met.

4. Performance comparison of DIMGA and CGA

In order to illustrate the advantages of DIM, the simulation experiments under different risks are implemented by comparing the performance of DIMGA and CGA. The difference between CGA and DIMGA is that CGA does not perform the DIM-based local search method, and other steps are the same as DIMGA.

4.1. Experimental design

The simulation experiments use MATLAB to perform related programs and obtain simulation results. The software version and hardware configuration are summarized as follows.

- Software version: MATLAB 2016b.
- Hardware configuration: Intel(R) Core (TM) i7-9750H CPU @ 2.60 GHz, 2.59 GHz; 16 GB.

(1) System parameters

In the simulation experiment, six systems (n = 5, k = 3; n = 10, k = 3; n = 15, k = 6; n = 20, k = 6; n = 25, k = 8; n = 30, k = 10) with different scales are selected respectively for Con/k/n: F(G) systems. Each system is set with two different amounts of tasks and three types of risk modes. So there are 36 different scenarios (six 6 different system sizes, two risk events, and three risk modes) of F systems or G systems, whose symbols are shown in Table 1.

The occurrence time of risks in Pattern I is set as 3.5. The moment of risk occurrence in Pattern II is randomly generated in the interval [2, 7] in ascending order, but Pattern III is generated in descending order. The scale parameters α from component 1 to component n are randomly generated in the interval [1,3] in descending order, and the shape parameters are randomly generated in the same way. Similarly, the impact factors a (for scale parameters) and b (for shape parameters) are randomly generated in the interval [0.3,1] by the descending order and ascending order, respectively. The evaluation time of the system defensive capability is 10. c_i is randomly generated in the interval [3, 10], and C_0 is equal to $2\sum_{i=1}^{n} c_i$; $\Delta t = 0.1$.

Note: ‘Sym.’ represents ‘Symbol’.

(2) Algorithm parameters

The algorithm parameters of DIMGA and CGA are listed as follows. The population size is 100, the maximum generation $G_{\max} = 100$, the crossover probability $p_c = 0.9$, the mutation probability p_m=0.1, the local search probability $p_l = 0.1$, and the convergence limitation is 50.

(3) Indicators of algorithm performance

For F systems and G systems, DIMGA and CGA are executed 50 times for 36 scenarios separately, and three indicators analyze the simulation results: the average defensive capability, the robustness of the algorithm based on the coefficient of variation (CV), and the convergence of algorithm measured by the mean of running generations.

4.2. Analysis of experimental results

The optimization results show the performance of these two algorithms (GA and DIMGA) based on the three mentioned indexes, and each algorithm runs 50 times.

(1) System defensive capability of DIMGA and CGA

The mean system defensive capabilities of 36 typical systems running 50 times for F and G systems are shown in Figures 4 and 5, respectively.

For F systems, all the mean defensive capability of DIMGA is larger than that of CGA because we can see the red section in each bar from Figure 4. The results of mean capability for some small-scale systems (F2, F3, F4, and F6) obtained by two algorithms are close, and the results of DIMGA are a bit higher than that of CGA. The maximum difference of defensive capability is 0.0723 in F30, and the minimum difference of defensive capability is 0.0051 in F4. The average improvement of the mean defensive capability obtained by DIMGA is 0.0372 higher than that of CGA, which is 5.97% higher than CGA.

For G systems, all the mean defensive capability of DIMGA is larger than that of CGA because we can see the red section in each bar from Figure 5. The mean capability of some small-scale systems (G1, G2, G5, and G6) obtained by two algorithms is close, and the results of DIMGA are a bit higher than that of CGA. The maximum difference of defensive capability is 0.0769 in G12, and the minimum difference of defensive capability is 0.0039 in G2. The average improvement of the mean defensive capability obtained by DIMGA is 0.0329 higher than that of CGA, which is 11.39% higher than CGA.

Table 1 The symbols of Con/k/n: F(G) systems under 36 scenarios

Sym.	n	k	Risk num	Risk Pattern	Sym.	n	k	Risk num	Risk Pattern	Sym.	n	k	Risk num	Risk Pattern
F1	5	3	2	I	**F25**	25	8	8	1	**F13**	15	6	5	I
F2	5	3	2	II	**F26**	25	8	8	2	**F14**	15	6	5	II
F3	5	3	2	III	**F27**	25	8	8	3	**F15**	15	6	5	III
F4	5	3	4	I	**F28**	25	8	16	1	**F16**	15	6	10	I
F5	5	3	4	II	**F29**	25	8	16	2	**F17**	15	6	10	II
F6	5	3	4	III	**F30**	25	8	16	3	**F18**	15	6	10	III
F7	10	3	3	I	**F31**	30	10	10	1	**F19**	20	6	6	I
F8	10	3	3	II	**F32**	30	10	10	2	**F20**	20	6	6	II
F9	10	3	3	III	**F33**	30	10	10	3	**F21**	20	6	6	III
F10	10	3	6	I	**F34**	30	10	20	1	**F22**	20	6	12	I
F11	10	3	6	II	**F35**	30	10	20	2	**F23**	20	6	12	II
F12	10	3	6	III	**F36**	30	10	20	3	**F24**	20	6	12	III
F13	15	6	5	I	**G1**	5	3	2	1	**G25**	25	8	8	I
F14	15	6	5	II	**G2**	5	3	2	2	**G26**	25	8	8	II
F15	15	6	5	III	**G3**	5	3	2	3	**G27**	25	8	8	III
F16	15	6	10	I	**G4**	5	3	4	1	**G28**	25	8	16	I
F17	15	6	10	II	**G5**	5	3	4	2	**G29**	25	8	16	II
F18	15	6	10	III	**G6**	5	3	4	3	**G30**	25	8	16	III
F19	20	6	6	I	**G7**	10	3	3	1	**G31**	30	10	10	I
F20	20	6	6	II	**G8**	10	3	3	2	**G32**	30	10	10	II
F21	20	6	6	III	**G9**	10	3	3	3	**G33**	30	10	10	III
F22	20	6	12	I	**G10**	10	3	6	1	**G34**	30	10	20	I
F23	20	6	12	II	**G11**	10	3	6	2	**G35**	30	10	20	II
F24	20	6	12	III	**G12**	10	3	6	3	**G36**	30	10	20	III

(2) Robustness analysis of DIMGA and CGA

The coefficient of variation is a ratio of standard variance to the mean value, which is used to evaluate the robustness of the algorithms. The smaller the CV, the more robust the algorithm is. From Figure 6, the results obtained by CIMGA in almost all of the F systems are smaller than that of CGA, except for F5 and F6. The results of 36 typical F systems illustrate that CIMGA has better robustness than CGA. For G systems, the CVs of CIMGA in almost all cases are smaller than that of CGA in G1~G28, but the CVs of CIMGA are larger than that of CGA in the large-scale systems in G29~G36 in Figure 7. In the G systems, although the CVs of DIMGA are somewhat larger than that of CGA, the differences between them are not significant, so the robustness of the two algorithms is close. CIMGA also keeps better robustness in F systems and most G systems, so CIMGA is suitable for solving defensive optimization problems, especially for F systems.

(3) Convergence generations of DIMGA and CGA

The convergence generation represents the speed of the algorithm reaching the optimal solution. The smaller the convergence generation, the faster the convergence speed of the algorithm. For F systems, about 75% of typical systems have lower average convergence generations performing the DIMGA, shown in Figure 8. However, in G systems, with the increase of system scale, the mean convergence generations of DIMGA are slightly larger than that of CGA, which accounts for 41.67%, shown in Figure 9.

Therefore, DIMGA performs well in terms of mean system defensive capability in all typical F and G systems, and robustness in most typical F and G systems. Although the average running generations of DIMGA are a bit larger than that of CGA in some typical systems, all the mean convergence generations of these two algorithms are similar. Furthermore, DIMGA can still be used effectively to solve

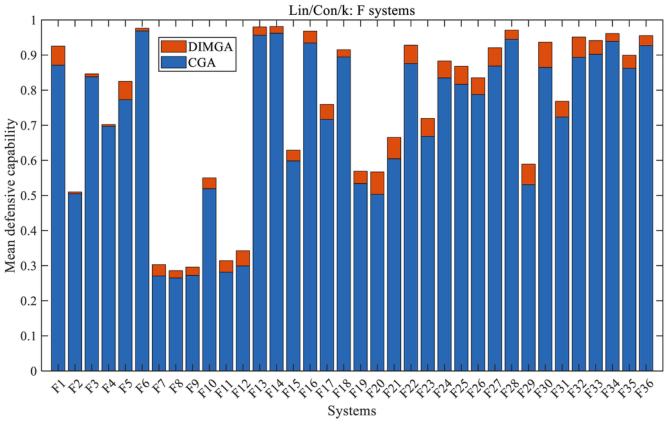


Fig. 4. Mean defensive capability of DIMGA and CGA for 36 typical F systems

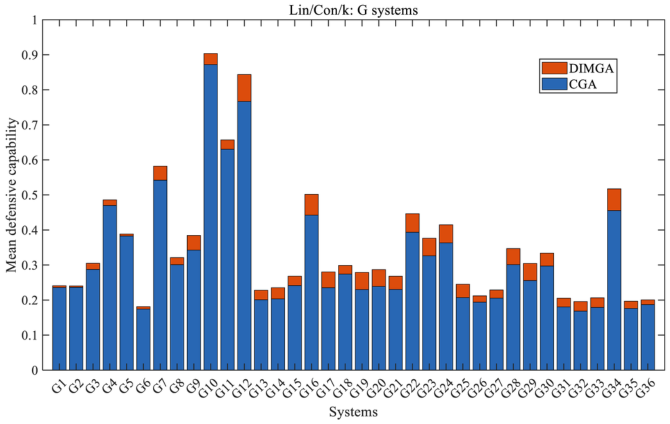


Fig. 5. Mean defensive capability of DIMGA and CGA for 36 typical G systems

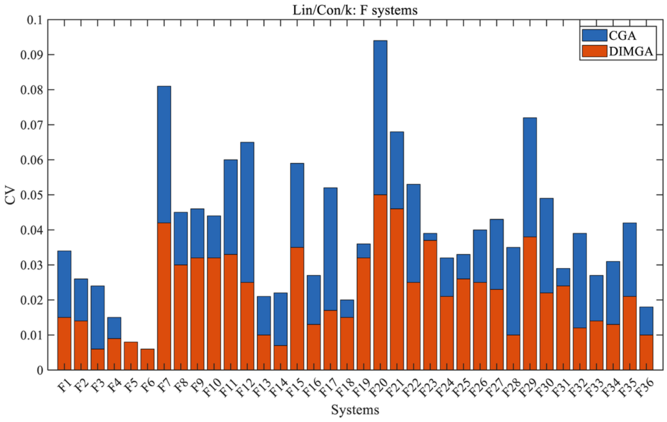


Fig. 6. CVs of DIMGA and CGA for 36 typical F systems

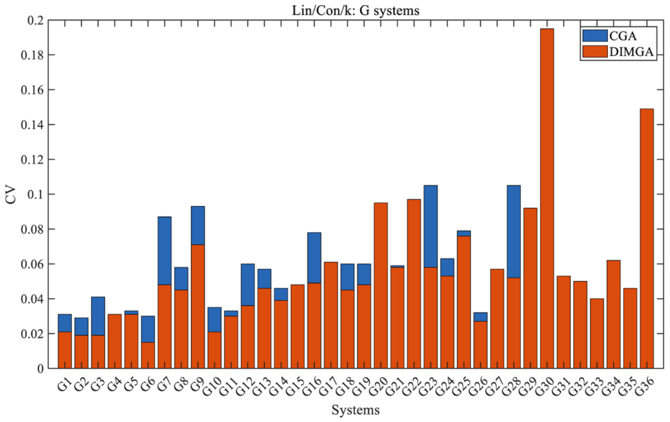


Fig. 7. CVs of DIMGA and CGA for 36 typical G systems

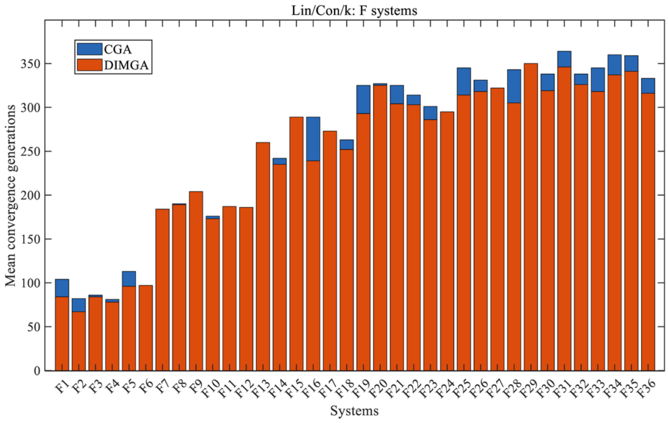


Fig. 8. Mean convergence generations of DIMGA and CGA for 36 typical F systems

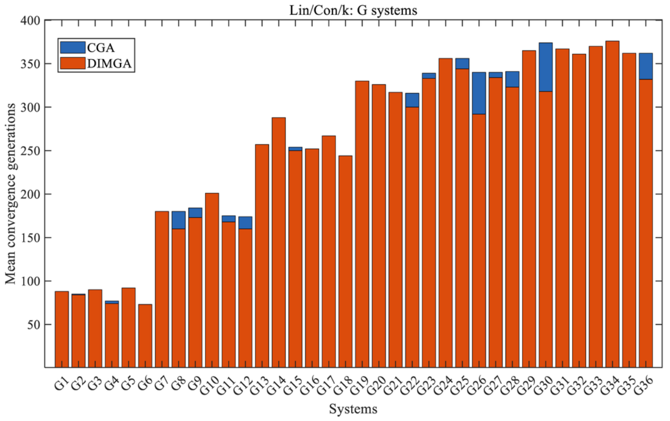


Fig. 9. Mean convergence generations of DIMGA and CGA for 36 typical G systems

the defensive optimization problem of G and F systems, although the performance difference between DIMGA and CGA in some systems is narrow. Therefore, DIMGA is more suitable for solving the defensive capability optimization problem of F systems.

5. Numerical examples

To analyze the relationship between component redundancy and assignment of a component module, the batch sampling-based quality control systems are taken as numerical examples to consider the optimal defensive strategy. Generally, continuous k risks have a great influence on the reliability of Con/k/n: F systems, while equal spacing k-1 risks have a greater influence on the reliability of G systems. Therefore, two types of risks (continuous k & equal spacing k-1) are taken as examples to analyze the changes in components' redundancy of the optimal assignment under different risks for F systems and G systems with n = 5.

5.1. Cases design under continuous and equal spacing risks

Combining three risk patterns with two risk types (continuous *k* & equal spacing *k*-1), the optimal defensive strategies under three system scales (*n* = 5, *k* = 2; *n* = 5, *k* = 3; *n* = 5, *k* = 4) are analyzed. So, there are 30 cases for Con/k/5 systems under continuous *k* risks, listed in Table 2, while there are 21 cases for Con/k/5 systems under equal spacing k-1 risks in Table 3.

Table 2 All cases under continuous k risks for Con/k/5 systems

Symbol	k	Risk distribution	Patterns	Symbol	k	Risk distribution	Patterns
C1	2	[1 1 0 1 1]	I	C16	3	[1 1 1 0 0]	I
C2	2	[1 1 0 1 1]	II	C17	3	[1 1 1 0 0]	II
C3	2	[1 1 0 1 1]	III	C18	3	[1 1 1 0 0]	III
C4	2	[1 1 0 0 0]	I	C19	3	[0 1 1 1 0]	I
C5	2	[1 1 0 0 0]	II	C20	3	[0 1 1 1 0]	II
C6	2	[1 1 0 0 0]	III	C21	3	[0 1 1 1 0]	III
C7	2	[0 1 1 0 0]	I	C22	3	[0 0 1 1 1]	I
C8	2	[0 1 1 0 0]	II	C23	3	[0 0 1 1 1]	II
C9	2	[0 1 1 0 0]	III	C24	3	[0 0 1 1 1]	III
C10	2	[0 0 1 1 0]	I	C25	4	[1 1 1 1 0]	I
C11	2	[0 0 1 1 0]	II	C26	4	[1 1 1 1 0]	II
C12	2	[0 0 1 1 0]	III	C27	4	[1 1 1 1 0]	III
C13	2	[0 0 0 1 1]	I	C28	4	[0 1 1 1 1]	I
C14	2	[0 0 0 1 1]	II	C29	4	[0 1 1 1 1]	II
C15	2	[0 0 0 1 1]	III	C30	4	[0 1 1 1 1]	III

Table 3 All cases under interval k-1 risks for Con/k/5 systems

Symbol	k	Risk distribution	Pattern	Symbol	k	Risk distribution	Pattern
S1	2	[1 0 1 0 1]	I	S12	2	[0 0 1 0 1]	III
S2	2	[1 0 1 0 1]	II	S13	2	[1 0 0 1 0]	I
S3	2	[1 0 1 0 1]	III	S14	2	[1 0 0 1 0]	II
S4	2	[1 0 1 0 0]	I	S15	3	[1 0 0 1 0]	III
S5	2	[1 0 1 0 0]	II	S16	3	[0 1 0 0 1]	I
S6	2	[1 0 1 0 0]	III	S17	3	[0 1 0 0 1]	II
S7	2	[0 1 0 1 0]	I	S18	3	[0 1 0 0 1]	III
S8	2	[0 1 0 1 0]	II	S19	3	[1 0 0 0 1]	I
S9	2	[0 1 0 1 0]	III	S20	3	[1 0 0 0 1]	II
S10	2	[0 0 1 0 1]	I	S21	3	[1 0 0 0 1]	III
S11	2	[0 0 1 0 1]	II				

To guarantee the effectiveness of the final defensive strategy, the optimal defensive strategy is obtained by performing DIMGA 5 times and selecting the maximum one.

5.2. Result discussion

To illustrate the redundancy and assignment of component module in the optimal defensive strategy clearly, a new representation of defensive strategy is developed based on a box with two numbers, and an example is shown in Figure 10. The number at the upper left green box represents the component index in the corresponding position, and the number in the center is the number of redundant components in the corresponding position. In this example, the assignment of a component module from position 1 to position 5 is 3, 2, 4, 1, 5, respectively, and the component redundancy from position 1 to position 5 is 0, 2, 3, 2, 0, respectively. The shade of the background color represents the intensity of the risk. The darker the color, the greater the risk intensity and the earlier the risk occurs.

The relationship between the redundancy position and risk distribution in Con/k/5: F systems under continuous *k* risks for 30 cases is shown in Figure 11. When *k* = 2, the F system mainly considers adding redundant components in positions 2 and 4 because the number of redundant components in these two positions are non-zero positive integers from C1 to C15. Moreover, redundant components should be added at least in one risk position. When *k* = 3, the F system mainly adds redundant components in positions 1 and 3. When *k* = 4, C25, C26, and C27 add redundant s components in positions 1 and 4, while C28, C29, and C30 add redundant components in positions 4 and 5. For F systems under continuous *k* risks, the redundant components should be distributed in the spaced way, and the position *k* must add the redundant components.

The relationship between the redundancy position and risk distribution in Con/k/5: G systems under continuous *k* risks for 30 cases is shown in Figure 12. In G systems, when *k* = 2, C1, C2, and C3 have two continuous two risks, and the redundant components are added in positions 4 and 5. From C4 to C15, there are two continuous risks, and all the redundant components are added in the position where the risk occurs. The ways of adding redundant components for cases when *k* = 3 and 4 are similar to when *k* = 2, and all the redundant components are added to the position where risks occur. Therefore, redundant components in G systems under the continuous *k* risks are added in a continuous way, and the distribution of redundant components is consistent with the affected positions.

The relationship between the redundancy position and risk distribution in Con/k/5: G systems under continuous *k* risks for 30 cases is shown in Figure 12. In G systems, when *k* = 2, C1, C2, and C3 have two continuous two risks, and the redundant components are added in positions 4 and 5. From C4 to C15, there are two continuous risks, and all the redundant components are added in the position where the risk occurs. The ways of adding redundant components for cases when *k* = 3 and 4 are similar to when *k* = 2, and all the redundant components are added to the position where risks occur. Therefore, redundant components in G systems under the continuous *k* risks are added in a continuous way, and the distribution of redundant components is consistent with the affected positions.

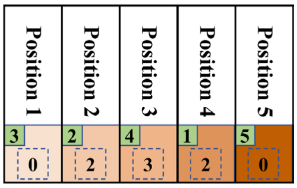


Fig. 10. An example of the new representation for the defensive strategy

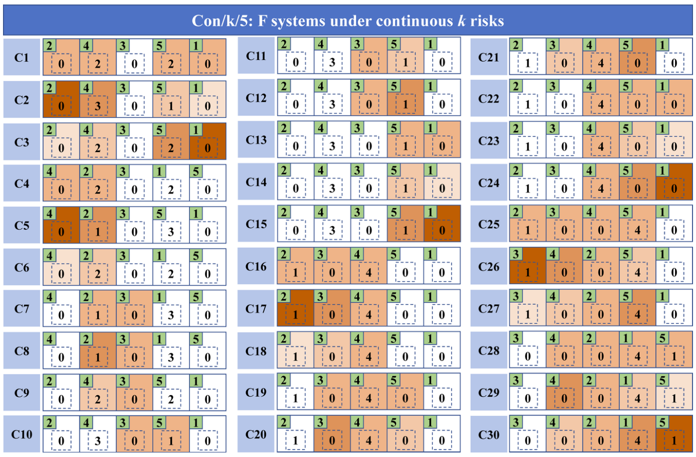


Fig. 11. The redundancy distribution of Con/k/5: F systems under continuous k risks

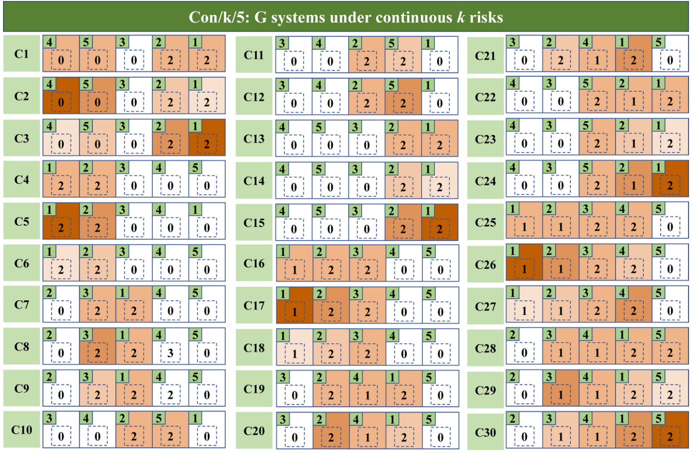


Fig. 12. The redundancy distribution of Con/k/5: G systems under continuous k risks

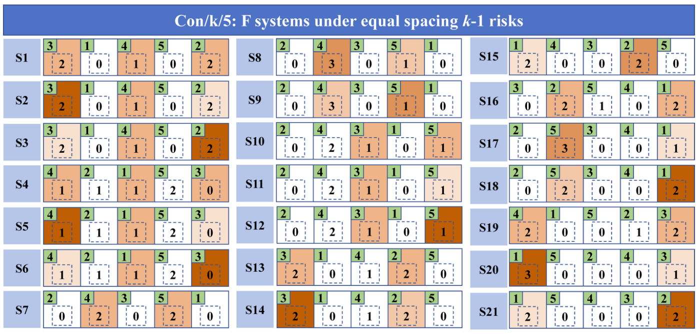


Fig. 13. The redundancy distribution of Con/k/5: F systems under equal spacing k-1 risks

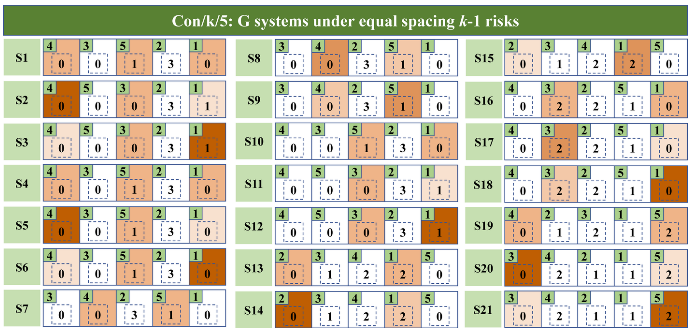


Fig. 14. The redundancy distribution of Con/k/5: G systems under equal spacing k-1 risks

The relationship between the redundancy position and risk distribution in Con/*k*/5: F systems under equal spacing *k*-1 risks for 21 cases is shown in Figure 13. When *k* = 2, the risk interval is 1; if the risk in the first position occurs, there will be three risk events from S1 to S6; and when there is no risk event in the first position, there will be two risk events from S7 to S12. When three risk events occur, the redundant components are added to the affected positions in S1, S2, and S3; while the redundant components are added in the first four positions in S4, S5, S6. When two risk events occur, the redundant components are added to the affected positions in S7, S8, and S9, while the redundant components are added to the affected positions and their adjacent positions in S10, S11, and S12 in a spaced way. In summary, in the cases of spacing *k* risks, the redundancy in F systems should be distributed in a spaced way, and redundant components should be added to the affected positions as a priority.

The relationship between the redundancy position and risk distribution in Con/*k*/5: G systems under equal spacing *k*-1 risks for 21 cases is shown in Figure 14. When *k* = 2, the risk spaced distance is 1, and the redundant components are allocated to two consecutive positions, one is the affected position, and the other is its adjacent unaffected positions. When *k* = 3, the spaced distance is 2, and the redundant components are allocated to three continuous positions, and one of them is the affected positions. When *k* = 4, the spaced distance is 3, adding redundancy to the components in four continuous positions, and one of the components is in affected positions. In conclusion, G systems in 21 cases show that redundancy is added continuously. Priority is given to adding redundancy to the affected positions and their adjacent positions, and the number of positions to add redundancy is equal to *k*.

5.3. An example of PMS

PMS is a typical con/*k*/*n*: F system, which consists of *n* monitors arranging parallel with the same distance, and the PMS fails once at least consecutive *k* monitors fail at the same time because of the appearance of the blind area [25]. Considering the monitoring distance of each monitor is k_0 unit distance, all the distance between two adjacent monitors in Con/*k*/*n* system is $k_0/2k$ unit distance. To better understand the structure of PMS, an example of PMS (Con/3/10: F system) is shown in Figure 15. In this example, the monitoring distance of each monitor k_0 is 30 meters, so the distance between two monitors on the same side is $k_0/2k$ = 5 meters.

In order to verify the results of numerical experiments, the defensive strategy of Con/3/10: F system under different risk types and risk patterns is analyzed in this example of PMS. Assuming that the external disturbs can affect the parameters of *a* and b for the components under the risks. Considering the monitors are electronic products and their lifetime is about 20000 ~ 50000 hours, so the lifetime follows the exponential distribution under the normal work condition with parameters $\alpha_i = 2 \sim 5 \times 10^4$ hours and $\beta_i = 1$. But the external disturbs may affect the impact factors *a* (for scale parameters) and *b* (for shape parameters). To analyze the optimization of defensive strategy, the external risk begins at the moment corresponding to the 10000th hours and lasts for 1200 hours, and the risks include continuous k risks under Patterns I and II & equal spacing *k*-1 risks under Patterns I and II. The parameters of the system, algorithm, and risk information are listed in Table 4.

By implementing the DIMGA, the optimal defensive strategy and redundancy distribution are listed in Table 5. Under continuous *k* risks, the optimal system resilience of Pattern I and II are both 0.9990, and the cost consumption is 6988 yuan and 6972 yuan, respectively. We can find that all the redundant components in PMS under continuous risks are distributed in a spaced way and position k has been added the redundant components. Under the equal spacing k-1 risks, the optimal system resilience of Pattern I is 0.9986 while the cost consumption is 6994, and the optimal system resilience of Pattern II is 0.9984 while the cost is 6947. The redundancy distribution of two patterns is arranged in a spaced way, and most of the affected positions have been added the redundant components. Therefore, the results of

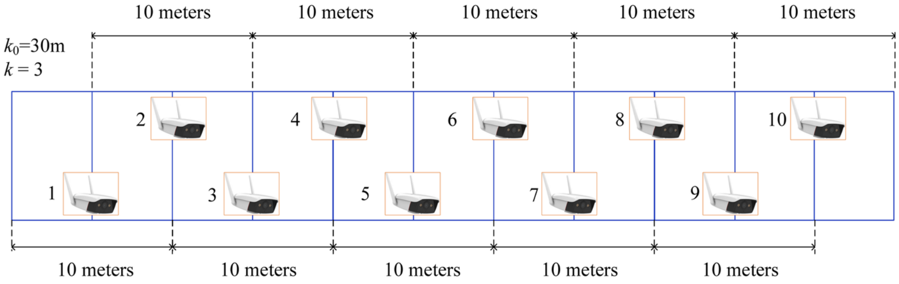
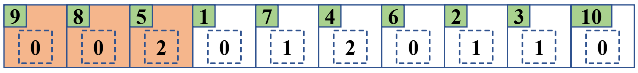
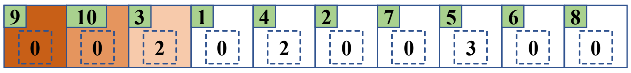
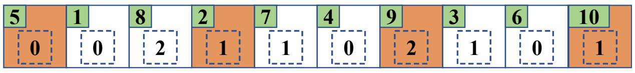
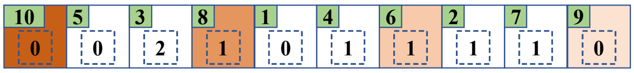


Fig. 15. The structure of PMS example (Con/3/10: F system)

Table 4. Parameters in the example of PMS (Con/3/10: F system)

Parameters	Values
System parameters	α =[42400, 39700, 37800, 35600, 32500, 31600, 31500, 28600, 24700, 22700] hours, β =[1, 1, 1, 1, 1, 1, 1, 1, 1, 1], n = 10, k = 3, C_0 = 7000 yuan, cc =[500, 473, 453, 431, 399, 390, 389, 360, 320, 300] yuan, k_0 = 30 meters.
Algorithm Parameters	Population size: 200, $G_{\max} = 400$, $p_l = 0.1$, $p_m = 0.1$, p_c=0.9, convergence limitation: 100.
Continuous k risk under Pattern I	risk start time: t_1=t_2=t_3=10000 hours, t = 11200 hours, a =[0.7, 0.7, 0.7, 1, 1, 1, 1, 1, 1, 1], b =[0.9, 0.9, 0.9, 1, 1, 1, 1, 1, 1, 1]
Continuous k risk under Pattern II	risk start time: t_1=t_2=t_3=10000 hours, t = 11200 hours, a =[0.5, 0.7, 0.9, 1, 1, 1, 1, 1, 1, 1], b =[0.6, 0.8, 0.95, 1, 1, 1, 1, 1, 1, 1]
Equal spacing k-1 risk under Pattern I	risk start time: t_1=t_4=t_7=t_{10}=10000 hours, t = 11200 hours, a =[0.7, 1, 1, 0.7, 1, 1, 0.7, 1, 1, 0.7], b =[0.9, 1, 1, 0.9, 1, 1, 0.9, 1, 1, 0.9]
Equal spacing k-1 risk under Pattern II	risk start time: t_1=t_4=t_7=t_{10}=10000 hours, t = 11200 hours, a =[0.6, 1, 1, 0.7, 1, 1, 0.8, 1, 1, 0.9], b =[0.5, 1, 1, 0.6, 1, 1, 0.7, 1, 1, 0.8]

Table 5. Optimal defensive strategy under different risk patterns

Risk information	Index	Results
Continuous k risks under Pattern I	System resilience	0.9990
	Cost	6988
	Redundancy distribution	 9 8 5 1 7 4 6 2 3 10 0 0 2 0 1 2 0 1 1 0
Continuous k risks under Pattern II	System resilience	0.9990
	Cost	6972
	Redundancy distribution	 9 10 3 1 4 2 7 5 6 8 0 0 2 0 2 0 0 3 0 0
Equal spacing k-1 risks under Pattern I	System resilience	0.9986
	Cost	6994
	Redundancy distribution	 5 1 8 2 7 4 9 3 6 10 0 0 2 1 1 0 2 1 0 1
Equal spacing k-1 risks under Pattern II	System resilience	0.9984
	Cost	6947
	Redundancy distribution	 10 5 3 8 1 4 6 2 7 9 0 0 2 1 0 1 1 1 1 0

this PMS example also verified the distribution rules of F systems in Section 5.2.

6. Conclusions

In this paper, the DIMGA is developed to get the optimal defensive strategy by integrating the advantages of DIM and GA under different external risks (three risk types & three risk patterns). The redundancy distribution rules can be summarized as follows. Under continuous *k* risks or spacing *k*-1 risks, the redundancy distribution of F systems under continuous risks should be in the spaced way, while G systems should be in a continuous way. This distribution rule can be applied to the redundancy allocation for large-scale systems when the associated complex algorithm is not considered. In the future, we also need to consider the uncertainty of the external risks to extend the application fields of the proposed method.

Acknowledgment

This research work was supported by the National Natural Science Foundation of China (Nos. 72101202, 51875451, 51834006).

References

1. Ahmadian N, Lim G J, Cho J, Bora S. A quantitative approach for assessment and improvement of network resilience. Reliability Engineering & System Safety 2020; 200: 106977, https://doi.org/10.1016/j.ress.2020.106977.
2. Almoghathawi Y, Barker K. Component importance measures for interdependent infrastructure network resilience. Computers and Industrial Engineering 2019; 133: 153-164, https://doi.org/10.1016/j.cie.2019.05.001.
3. Anwar G A, Dong Y, Zhai C. Performance-based probabilistic framework for seismic risk, resilience, and sustainability assessment of reinforced concrete structures. Advances in Structural Engineering 2020; 23(7): 1454-1472, https://doi.org/10.1177/1369433219895363.
4. Aziz T, Lin Z, Waseem M, Liu S. Review on optimization methodologies in transmission network reconfiguration of power systems for grid resilience. International Transactions on Electrical Energy Systems 2021; 31(3): e12704, https://doi.org/10.1002/2050-7038.12704.
5. Bai G, Wang H, Zheng X et al. Improved resilience measure for component recovery priority in power grids. Frontiers of Engineering Management 2021; 8(4): 545-556, https://doi.org/10.1007/s42524-021-0161-5.
6. Balakrishnan S, Zhang Z. Criticality and Susceptibility Indexes for Resilience-Based Ranking and Prioritization of Components in Interdependent Infrastructure Networks. Journal of Management in Engineering 2020; 36(4): 04020022, https://doi.org/10.1061/(ASCE)ME.1943-5479.0000769.
7. Bukowski L, Werbińska-Wojciechowska S. Using fuzzy logic to support maintenance decisions according to resilience-based maintenance concept. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2021; 23 (2): 294-307, https://doi.org/10.17531/ein.2021.2.9.
8. Che H, Zeng S, Guo J. A reliability model for load-sharing k -out-of- n systems subject to soft and hard failures with dependent workload and shock effects. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2020; 22(2): 253-264, https://doi.org/10.17531/ein.2020.2.8.
9. Che H, Zeng S, You Q et al. A fault tree-based approach for aviation risk analysis considering mental workload overload. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2021; 23(4): 646-658, https://doi.org/10.17531/ein.2021.4.7.
10. Dui H, Zheng X, Wu S. Resilience analysis of maritime transportation systems based on importance measures. Reliability Engineering and System Safety 2021; 209: 107461, https://doi.org/10.1016/j.ress.2021.107461.
11. Fang Y P, Zio E. An adaptive robust framework for the optimization of the resilience of interdependent infrastructures under natural hazards. European Journal of Operational Research 2019; 276(3): 1119-1136, https://doi.org/10.1016/j.ejor.2019.01.052.
12. Ghorbani-Renani N, González A D, Barker K, Morshedlou N. Protection-interdiction-restoration: Tri-level optimization for enhancing interdependent network resilience. Reliability Engineering and System Safety 2020; 199: 106907, https://doi.org/10.1016/j.ress.2020.106907.
13. Jaiswal D P, Anand H, Srinivasan S M, Darayi M. A Data-Driven Model to Generate Disruptive Scenarios for Infrastructure Resilience Studies. Procedia Computer Science 2021; 185: 248-255, https://doi.org/10.1016/j.procs.2021.05.026.
14. Kakadia D, Ramirez-Marquez J E. Quantitative approaches for optimization of user experience based on network resilience for wireless service provider networks. Reliability Engineering & System Safety 2020; 193: 106606, https://doi.org/10.1016/j.ress.2019.106606.
15. Kuo W, Zhang W, Zuo M. Consecutive-k-out-of-n:G system: The mirror image of a consecutive-k-out-of-n:F system. IEEE Transactions on Reliability 1990; 39(2): 244-253, https://doi.org/10.1109/24.55888.
16. Levitin G, Xing L, Dai Y. Linear multistate consecutively-connected systems subject to a constrained number of gaps. Reliability Engineering & System Safety 2015; 133: 246-252, https://doi.org/10.1016/j.ress.2014.09.004.
17. Li M, Hu L, Peng R, Bai Z. Reliability modeling for repairable circular consecutive-k-out-of-n: F systems with retrial feature. Reliability Engineering & System Safety 2021; 216: 107957, https://doi.org/10.1016/j.ress.2021.107957.
18. Li R, Dong Q, Jin C, Kang R. A new resilience measure for supply chain networks. Sustainability 2017; 9(1): 144, https://doi.org/10.3390/su9010144.
19. Li R, Gao Y. On the component resilience importance measures for infrastructure systems. International Journal of Critical Infrastructure Protection 2021: 100481, https://doi.org/10.1016/j.ijcip.2021.100481.
20. Liao T Y, Hu T Y, Ko Y N. A resilience optimization model for transportation networks under disasters. Natural Hazards 2018; 93(1): 469-489, https://doi.org/10.1007/s11069-018-3310-3.
21. Lin Y-K, Huang C-F. Assessment of spare reliability for multi-state computer networks within tolerable packet unreliability. International Journal of Systems Science 2015; 46(6): 1020-1035, https://doi.org/10.1080/00207721.2013.807383.
22. Liu R-P, Lei S, Peng C et al. Data-based resilience enhancement strategies for electric-gas systems against sequential extreme weather events. IEEE Transactions on Smart Grid 2020; 11(6): 5383-5395, https://doi.org/10.1109/TSG.2020.3007479.
23. Liu X, Fang Y-P, Zio E. A hierarchical resilience enhancement framework for interdependent critical infrastructures. Reliability Engineering & System Safety 2021; 215: 107868, https://doi.org/10.1016/j.ress.2021.107868.
24. Lu Q-C. Modeling network resilience of rail transit under operational incidents. Transportation Research Part A: Policy and Practice 2018; 117: 227-237, https://doi.org/10.1016/j.tra.2018.08.015.
25. Ma C, Wang Q, Cai Z et al. Component reassignment for reliability optimization of reconfigurable systems considering component degradation. Reliability Engineering and System Safety 2021; 215: 107867, https://doi.org/10.1016/j.ress.2021.107867.
26. Moslehi S, Reddy T A. Sustainability of integrated energy systems: A performance-based resilience assessment methodology. Applied

Energy 2018; 228: 487-498, https://doi.org/10.1016/j.apenergy.2018.06.075.

27. Najarian M, Lim G J. Optimizing infrastructure resilience under budgetary constraint. Reliability Engineering and System Safety 2020; 198: 106801, https://doi.org/10.1016/j.ress.2020.106801.
28. Ozkan A, Kesik T, Yilmaz A Z, O'Brien W. Development and visualization of time-based building energy performance metrics. Building Research & Information 2019; 47(5): 493-517, https://doi.org/10.1080/09613218.2018.1451959.
29. Qu L, Han C, Li Y et al. Recent Advances in the Reliability Evaluation and Optimization of Linear Multistate Consecutively-connected Systems. Recent Patents on Engineering 2021; 15(3): 314-325, https://doi.org/10.2174/1872212114999200517123155.
30. Ramezankhani M J, Torabi S A, Vahidi F. Supply chain performance measurement and evaluation: A mixed sustainability and resilience approach. Computers and Industrial Engineering 2018; 126: 531-548, https://doi.org/10.1016/j.cie.2018.09.054.
31. Rosato V, Di Pietro A, Kotzanikolaou P et al. Integrating resilience in time-based dependency analysis: a large-scale case study for urban critical infrastructures. Issues on Risk Analysis for Critical Infrastructure Protection, IntechOpen: 2021, 91-110, https://doi.org/10.5772/intechopen.97809.
32. Si S, Zhao J, Cai Z, Dui H. Recent advances in system reliability optimization driven by importance measures. Frontiers of Engineering Management 2020; 7(3): 335-358, https://doi.org/10.1007/s42524-020-0112-6.
33. Szaciłło L, Jacyna M, Szczepański E, Izdebski M. Risk assessment for rail freight transport operations. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2021; 23(3): 476-488, https://doi.org/10.17531/ein.2021.3.8.
34. Tran H T, Balchanos M, Domerçant J C, Mavris D N. A framework for the quantitative assessment of performance-based system resilience. Reliability Engineering and System Safety 2017; 158(February 2016): 73-84, https://doi.org/10.1016/j.ress.2016.10.014.
35. Vintr Z, Malach J. Selected aspects of physical structures vulnerability-state-of-the-art. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2012; 14 (3): 189-194.
36. Wang D, Si S, Cai Z, Zhao J. Reliability optimization of linear consecutive-k-out-of-n: F systems driven by reconfigurable importance. Reliability Engineering & System Safety 2021; 216: 107994, https://doi.org/10.1016/j.ress.2021.107994.
37. Wang Y, Guo L, Wen M, Yang Y. Availability analysis for a multi-component system with different k-out-of-n: G warm standby subsystems subject to suspended animation. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2019; 21(2): 289-300, https://doi.org/10.17531/ein.2019.2.14.
38. Wu C, Pan R, Zhao X, Cao S. Reliability evaluation of consecutive-k-out-of-n: F systems with two performance sharing groups. Computers and Industrial Engineering 2021; 153: 107092, https://doi.org/10.1016/j.cie.2020.107092.
39. Wu G, Li Z S. Cyber Physical Power System (CPPS): A review on measures and optimization methods of system resilience. Frontiers of Engineering Management 2021; 8: 503-518, https://doi.org/10.1007/s42524-021-0163-3.
40. Xiang Y, Levitin G, Dai Y. Linear multistate consecutively-connected systems with gap constraints. IEEE Transactions on Reliability 2012; 61(1): 208-214, https://doi.org/10.1109/TR.2011.2182393.
41. Xu Z, Ramirez-Marquez J E, Liu Y, Xiahou T. A new resilience-based component importance measure for multi-state networks. Reliability Engineering and System Safety 2020; 193: 106591, https://doi.org/10.1016/j.ress.2019.106591.
42. Zhang C, Zhang Y, Dui H et al. Importance measure-based maintenance strategy considering maintenance costs. Eksploatacja i Niezawodnosc - Maintenance and Reliability 2022; 24 (1): 15-24, https://doi.org/10.17531/ein.2022.1.3.
43. Zhang Q, Wang Z, Ma S, Arif A. Stochastic pre-event preparation for enhancing resilience of distribution systems. Renewable and Sustainable Energy Reviews 2021; 152: 111636, https://doi.org/10.1016/j.rser.2021.111636.