Computers and Chemical Engineering 101 (2017) 167–192

Contents lists available at ScienceDirect

Computers and Chemical Engineering

journal homepage: www.elsevier.com/locate/compchemeng

Automatic generation of interlock designs using genetic algorithms

Yeremia Yehuda Lepar, Yu-Chih Wang, Chuei-Tin Chang*

Department of Chemical Engineering, National Cheng Kung University, Tainan 70101, Taiwan

ARTICLE INFO

Article history:
Received 20 January 2016
Received in revised form 20 February 2017
Accepted 22 February 2017
Available online 28 February 2017

Keywords:
Corrective maintenance
Preventive maintenance
Interlock
Cold-standby
Spare
Superstructure
Genetic algorithm

ABSTRACT

The hazardous units in a modern chemical plant are often equipped with safety interlocks to mitigate the detrimental effects of potential accidents. To achieve a desired level of reliability (or availability), not only the interlock configuration but also the maintenance policies of its components must be properly stipulated before actual installation. Although a number of deterministic programming models have already been developed for this purpose, their laborious formulation and solution steps are usually carried out on a case-by-case basis. To attain the essential qualities of conciseness, portability and maintainability for easy implementation, there is a definite need to develop a generic and modularized code according to an evolutionary algorithm.

The structural and maintenance specifications of an interlock can be represented with: (1) the number of measurement channels and the corresponding alarm logic, (2) the numbers of online and spare sensors in each channel and the corresponding voting gate, (3) the number of shutdown channels and the corresponding tripping configuration, (4) the numbers of online and standby actuators in each channel, and the corresponding activation mechanism, and (5) the inspection intervals of shutdown channels. All of them are encoded in this study with binary numbers for use as inputs to implement the genetic algorithm (GA). An interlock superstructure is also developed to facilitate the search for the best configuration and maintenance plan in any application. By minimizing the overall life-cycle expenditure, a generic MATLAB code has been developed for generating all aforementioned specifications in any application. Four examples are provided to demonstrate the benefits of the proposed optimization approach.

1. Introduction

In order to mitigate the detrimental outcomes of accidents, it is a common practice to install safety interlocks on the inherently hazardous units in a chemical plant. Since hardware failures are random events, it is imperative to keep these protective mechanisms operable at all time. In other words, each interlock should be properly configured and maintained so as to achieve a desired level of reliability (or availability).

Generally speaking, a safety interlock is designed to perform two basic functions: alarm and shutdown. The alarm is mainly facilitated with sensors. Based on their online measurements, a predetermined Boolean logic can be applied to determine whether an alarm should be set off. The shutdown function can be realized with actuators, for example, solenoid valves or power switches. In response to the alarm decision, these devices can be activated (or energized) to perform the required shutdown operation(s).

Since any hardware item may fail either safely (FS) or dangerously (FD), the probability of interlock malfunction can usually be lowered by introducing redundancy at the component level. The unsafe process state can be detected according to one or more critical variable (which is referred to as a "measurement channel" in this work), while each of them may be monitored with a set of identical sensors. Similarly, there may be more than one way to terminate a continuous manufacturing process and bring it to a safe state. For the purpose of ensuring successful shutdown, it may also be necessary to install repeated actuators. To facilitate illustration clarity, each of the aforementioned termination operations is called a "shutdown channel" throughout this paper.

* Corresponding author.
E-mail address: ctchang@mail.ncku.edu.tw (C.-T. Chang).

http://dx.doi.org/10.1016/j.compchemeng.2017.02.042
0098-1354/

The spare-supported corrective maintenance policy is adopted in the present study to upkeep the monitoring device(s) in the alarm subsystem. For each measurement channel, there may be more than one component installed online and also several spares stored offline. The failed online sensor is supposed to be immediately replaced with a functional spare and then repaired offline as quickly as possible. Lai et al. (2003) have carried out a preliminary study on the basis of this idea.

On the other hand, since the actuators are not used during normal operations, a FD failure is only detectable upon demand. To suppress the possibility of these unobservable failures, a preventive maintenance strategy is often adopted to raise the availability of each shutdown channel. Vaurio (1995) suggested that the inspection intervals must be determined to minimize the cost rate or accident rate, and the same author (Vaurio, 1999) later integrated the age replacement policy into the preventive maintenance scheme. Under this policy, every component is replaced after a fixed number of inspections and/or repairs, even it is still functional. Badía et al. (2001) assumed only hidden failures may occur at the given system, and then proposed a computation procedure to determine the cost-optimal inspection interval. These authors (Badía et al., 2002) then extended this work to cases where both revealed and hidden failures are possible. Duarte et al. (2006) optimized the preventive maintenance strategy under assumption that the repair rate is constant, and both failure and hazard rates increase linearly over time. Wang and Pham (2011) formulated a multi-objective optimization problem to incorporate the imperfect maintenance strategies for a single-unit system subject to two competing risks. Kouedeu et al. (2011) proposed a two-level hierarchical decision-making approach to calculate the mean time to failure (MTTF) in the first level and to simultaneously optimize the production rate and the maintenance policies in the second level. Dohi and Nakagawa (2013) suggested using uniform inspection intervals for a simple repairable system with preventive repair to bring the system back to the state just as that in the beginning of working cycle. Finally, Wang and Zhang (2014) thoroughly reviewed the state of art in reliability and maintenance modeling, including models for repair, replacement and inspection policies for complex systems.

The aforementioned configurational and maintenance issues were traditionally addressed in the design stage with an ad hoc approach, which could be both long-winded and error prone. To circumvent this drawback, several mathematical programming models have been proposed in recent years to generate the interlock designs systematically. Liang and Chang (2008) developed an integer programming model to optimize the structures and maintenance policies of multilayer protective systems, while Liao and Chang (2010) later amended this model so as to extend its applications to the multichannel ones. Finally, Wibisono et al. (2014) further considered components with time-dependent failure rates in this model by incorporating the Weibull distribution.

Finding the feasible solution that yields the best value of a given objective function is the task to be performed in essentially every optimization problem. A suitable computation algorithm and the corresponding computer code are obviously needed for solving the problem efficiently. Liang and Chang (2008) and Liao and Chang (2010) produced the optimal interlock designs with the DICOPT solver in GAMS, while Wibisono et al. (2014) utilized BARON (Srivastava and Fahim, 2007). This solution tactic is unfortunately quite cumbersome in the *preparation stage* since both the mathematical model and the computer code have to be recreated each time a new application is being considered. Furthermore, the code maintainability is also a practical issue if it is necessary to incorporate dedicated models for new applications. A general-purpose code should therefore be developed to ensure modularity and conciseness.

Notice that the evolutionary solution methods have matured considerably in the recent years. Unlike the deterministic solvers, the required codes are easy to develop and maintain. Among various choices, the genetic algorithm (GA) is well-suited for solving a wide variety of optimization problems (Mitchell, 1998). In fact, implementing GA in the MATLAB environment can be very effective for the development of optimal maintenance policies. Okasha and Frangopol (2009) used the genetic algorithm to devise optimization strategies for scheduling maintenance actions and choosing structural components on the basis of system reliability, redundancy, and life-cycle cost. Azaron et al. (2009) developed a genetic procedure to solve a multi-objective discrete reliability optimization problem.

The present study is aimed to develop a generic GA-based search strategy for identifying, in any application, the optimal interlock design that minimizes the expected life-cycle expenditure. The system structure and maintenance program of an interlock can be uniquely stipulated with the following parameters: (1) the number of measurement channels and the corresponding alarm logic, (2) the numbers of online and spare sensors in each measurement channel and the corresponding voting gate, (3) the number of shutdown channels and the corresponding tripping configuration, (4) the numbers of online and standby actuators units in each shutdown channel, and the corresponding activation mechanism, and (5) the inspection intervals of shutdown channels. All of them are encoded with binary numbers for use as inputs to implement the genetic algorithm. With the given parameters mentioned above, one can calculate

- the availability and the expected numbers of repairs and replacements of each measurement channel,
- the purchase cost and the expected repair and replacement costs of each measurement channel,
- the availability and the expected numbers of repairs and inspections/replacements of each shutdown channel,
- the purchase cost and the expected repair and inspections/replacement costs of each shutdown channel, and
- the total expected loss due to FS and FD failures and the expected life-cycle expenditure.

To facilitate clear explanation, the remaining paper is organized as follow: the next section provides a theoretical foundation of the mathematical model, that is, the general structure of recursive multilayer protection mechanism and the superstructure of a single-layer safety interlock. The generalized versions of corrective and preventive maintenance strategies are explained in Section 3. After graphically modeling these maintenance programs with Markov diagrams, explicit formulas for computing the time-averaged availabilities and the expected numbers of repairs and replacements can then be derived accordingly. Section 4 explains the GA-based computation procedure, which is roughly divided into two parts: the chromosome encoding scheme and the fitness evaluation scheme. The former automatically translates an established superstructure and the corresponding maintenance programs into a binary string (i.e., the chromosome), while the latter evaluates the total life-cycle expenditure (i.e., the fitness measure) according to a given chromosome. Section 5 outlines the computation procedure of the genetic algorithm. Its implementation steps in practical applications are illustrated with a simple example in the same section, and additional case studies are reported in Section 6 to demonstrate the effectiveness the proposed approach. Finally, conclusions and possible future works are presented in Section 7.

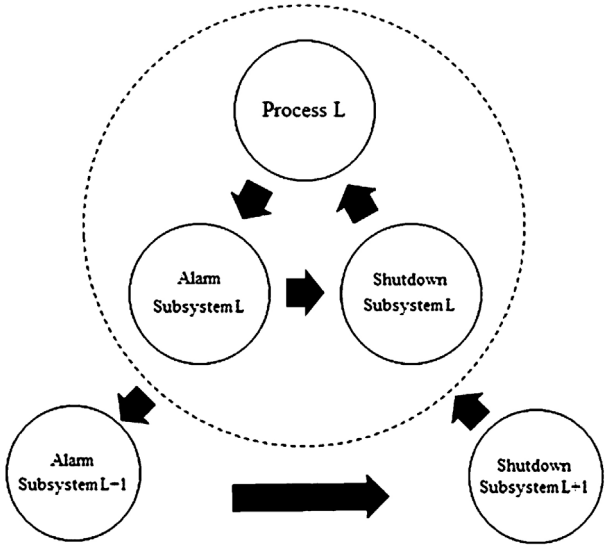

Fig. 1. The recursive structure of safety interlocks ($L = 1, 2, 3, \ldots$).

2. General structure of a protected system

The general structure of a multi-layer protected system is sketched in Fig. 1. The first L layers of this system are grouped together and enclosed within the dotted circle, while the first $L-1$ of them are viewed as "Process L". The alarm subsystem in layer L detects the unsafe state of Process L online and subsequently issues a control signal to activate the shutdown subsystem in the same layer. If all protective mechanisms embedded in the above-mentioned L layers fail, then Process $L+1$ is unprotected and the alarm and shutdown subsystems in layer $L+1$ may be triggered in the same way as those in the prior layer. Thus, a multi-layer interlocking structure can be viewed as a recursive operating procedure.

For illustration convenience, let us consider only the model formulation for describing a single layer. A binary variable is adopted here to denote the process condition under consideration, that is

$$\xi = \begin{cases} 1 & \text{if the process is in a specific unsafe state} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Since the unsafe process state may be revealed in several different process variables, such as the temperature, pressure, and flow rate, etc., a binary vector $\mathbf{x} = [\, x_1 \quad x_2 \quad \cdots \quad x_M \,]^T$ is used in this study to characterize their actual values, that is

$$x_i = \begin{cases} 1 & \text{if the } i\text{th process variable exceeds the specified safety limits} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

where $i = 1, 2, \ldots, M$. For the purpose of monitoring x_i, it is assumed that there may be one or more identical sensor configured in the same measurement channel. The channel output also form a binary vector $\mathbf{y} = [\, y_1 \quad y_2 \quad \cdots \quad y_M \,]^T$ and each element is used to reflect whether the unsafe state is confirmed in the corresponding channel, that is

$$y_i = \begin{cases} 1 & \text{if the } i\text{th channel detects an unsafe state} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

where $i = 1, 2, \ldots, M$. The alarm logic, which can be expressed with a binary function $f(\mathbf{y})$, is then applied to these channel outputs, and this logic can be expressed as

$$f(\mathbf{y}) = \begin{cases} 1 & \text{if the alarm system sets off alarm} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

If a decision is made to set off the alarm, i.e., $f(\mathbf{y}) = 1$, one or more shutdown operation may be required and each is represented with a binary variable as follows:

$$u_j = \begin{cases} 1 & \text{if the } j\text{th shutdown operation is called for} \\ 0 & \text{otherwise} \end{cases} \tag{5}$$

where $j = 1, 2, \ldots, K$. Note that every operation should be facilitated with more than one identical actuator and its outcome is expressed with still another binary variable, i.e.

$$v_j = \begin{cases} 1 & \text{if the } j\text{th shutdown operation is completed} \\ 0 & \text{otherwise} \end{cases} \tag{6}$$

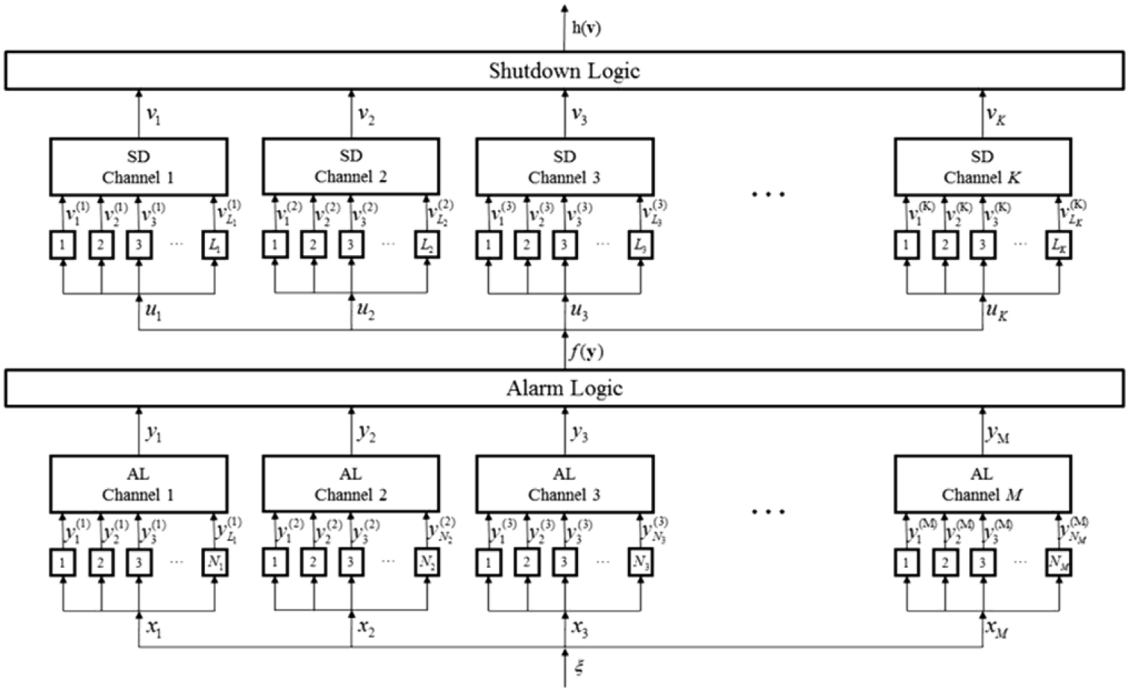

Fig. 2. Superstructure of a single-layer safety interlock.

where $j = 1, 2, \ldots, K$. An additional binary function of the vector $\mathbf{v} = [\, v_1 \quad v_2 \quad \cdots \quad v_K \,]^T$ can be defined to characterize the outcomes of all possible combinations of these shutdown operations, that is:

$$h(\mathbf{v}) = \begin{cases} 1 & \text{if the system is brought to a safe shutdown state} \\ 0 & \text{otherwise} \end{cases} \tag{7}$$

The corresponding interlock superstructure can be found in Fig. 2.

3. Maintenance programs of critical components

In principle, the corrective and preventive maintenance policies can be used to raise the availability levels of critical components in the alarm and shutdown subsystems respectively. The generalized versions of these two strategies are presented in the sequel.

3.1. Corrective maintenance policy

It is assumed in this study that only online sensors may fail and these failures are observable. A spare-supported corrective maintenance program can be tailored especially for these revealed failures in a measurement channel (Liao and Chang, 2010). Although a rigorous model has already been developed, its essential formulations are still outlined below for the sake of illustration clarity.

To be specific, let us assume that there are m sensors purchased for a particular channel, and n of them are placed online while the rest are stored offline as spares. Initially all sensors are assumed to be normal. If at any instance an online sensor fails and at least one spare is functional, then replace the former with the latter immediately. The failed sensor is taken offline and then placed in queue for repair. The offline repair process is in effect only when all online sensor(s) are working, while repairing the failed online sensor(s) can take place only if none of the spares are functional. Finally, it is assumed that the failed sensor(s) can be repaired only one at a time in sequence. The corresponding Markov diagram can be found in Fig. 3, in which every node denotes a distinct channel state and node 1 is associated with the initial condition. The transition rates between states can be divided into three types, i.e., the failure rate (λ), the repair rate (μ), and the replacement rate (ε), and all of them are constants. Due to these different transitions, each node can be uniquely characterized by two nonnegative integers, i.e., the numbers of failed online and offline sensors. For examples, let us consider node 2 and node $n+2$ in Fig. 2. The aforementioned numbers in the former case should be 1 and 0, while they are 0 and 1 in the latter. Note also that all channel states can be divided into 8 separate blocks according to the connections surrounding each node (Liao and Chang, 2010) (see Fig. 4).

To reduce computation load, let us consider only the asymptotic probability of every state in the Markov diagram. By assuming that the operation horizon is long enough so that the steady-state probabilities of all the aforementioned states can be reached within a relatively short time period, the state probabilities of the first 7 blocks can be approximated according to the following asymptotic state equations:

- Block 1:

$$P_{j+2} = \frac{j\lambda}{\mu} P_1; \quad j = 1, 2, \ldots, n. \tag{8}$$

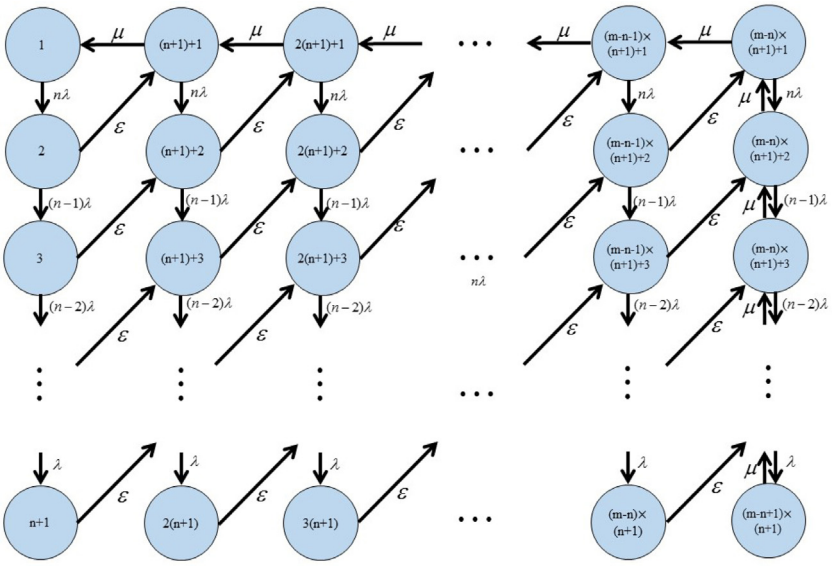

Fig. 3. Markov diagram of a measurement channel under corrective maintenance policy with n online sensors and $m-n$ offline spares.

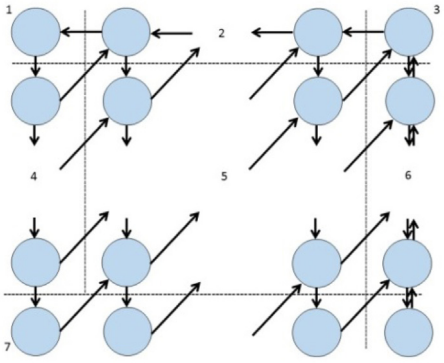

Fig. 4. Classification of channel states in a generalized Markov diagram for the measurement channel.

- Block 2:

$$P_{(j+1)[m-(i-2)]+1} = \frac{\mu + j\lambda}{\mu} P_{(j+1)[m-(i-1)]+1} - \frac{\varepsilon}{\mu} P_{(j+1)(m-i)+2}; \quad j = 1, 2, \ldots, n; \quad i = j+2, j+3, \ldots, m. \tag{9}$$

- Block 3:

$$P_{(j+1)(m-j)+2} = \frac{\mu + \lambda}{\mu} P_{(j+1)(m-j)+1} - \frac{\varepsilon}{\mu} P_{(j+1)[m-(j+1)]+2}; \quad j = 1, 2, \ldots, n. \tag{10}$$

- Block 4:

$$P_{i+1} = P_1 \lambda^i \prod_{k=1}^{i} \frac{j+1-k}{\varepsilon + (j-k)\lambda}; \quad j = 1, 2, \ldots, n; \quad i = 1, 2, \ldots, j-1. \tag{11}$$

- Block 5:

$$P_{(j+1)[m-(i-1)]+j} = \frac{2\lambda}{\varepsilon + \lambda} P_{(j+1)[m-(i-1)]+j-1} - \frac{\varepsilon}{\varepsilon + \lambda} P_{(j+1)(m-i)+j+1}; \quad j = 1, 2, \ldots, n; \quad i = j+2, j+3, \ldots, m. \tag{12}$$

- Block 6:

$$P_{(j+1)(m-j)+j+1} = \frac{\mu + \lambda}{\mu} P_{(j+1)(m-j)+j} - \frac{2\lambda}{\mu} P_{(j+1)(m-j)+j-1} - \frac{\varepsilon}{\mu} P_{(j+1)[m-(j+1)]+j+1}; \quad j = 1, 2, \ldots, n \tag{13}$$

- Block 7:

$$P_{(j+1)(m-i)+n+1} = \frac{\lambda}{\varepsilon} P_{(j+1)(m-i)+j}; \quad j = 1, 2, \ldots, n; \quad i = j+1, j+2, \ldots, m. \tag{14}$$

In addition, note that the sum of all state probabilities should equal unity, i.e.

$$\sum_{j=1}^{(m-n+1)(n+1)} P_j = 1 \tag{15}$$

Since Eqs. (8)–(15) are linear and the coefficients of variables can be determined in advance, the generalized solution procedure can be coded in a straightforward fashion. To illustrate this point, let us consider a simple example of 2 online and 2 spare sensors, i.e., $m = 4$ and $n = 2$. The corresponding linear system can be written as $\mathbf{Ax} = \mathbf{b}$, where

$$\mathbf{A} = \begin{bmatrix} \frac{2\lambda}{\mu} & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \frac{-\varepsilon}{\mu} & 0 & \frac{2\lambda+\mu}{\mu} & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{-\varepsilon}{\mu} & 0 & \frac{2\lambda+\mu}{\mu} & -1 & 0 \\ \frac{2\lambda}{\lambda+\varepsilon} & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{\varepsilon}{\lambda+\varepsilon} & \frac{2\lambda}{\lambda+\varepsilon} & 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \frac{-\varepsilon}{\mu} & \frac{-2\lambda}{\mu} & \frac{\lambda+\mu}{\mu} & -1 \\ 0 & \frac{\lambda}{\varepsilon} & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \frac{\lambda}{\varepsilon} & -1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}; \quad \mathbf{b} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}; \quad \mathbf{x} = \begin{bmatrix} P_1 \\ P_2 \\ P_3 \\ P_4 \\ P_5 \\ P_6 \\ P_7 \\ P_8 \\ P_9 \end{bmatrix}$$

If $\lambda = 1.8\ \text{month}^{-1}$, $\mu = 3.5\ \text{month}^{-1}$ and $\varepsilon = 365\ \text{month}^{-1}$, one can then produce the following results

$$\mathbf{x} = \mathbf{A}^{-1}\mathbf{b} = \begin{bmatrix} -0.521 & -0.302 & -0.148 & -0.303 & -0.149 & -0.059 & -0.150 & -0.059 & 0.209 \\ -0.005 & -0.005 & -0.001 & -0.002 & -0.001 & -0.001 & -0.001 & -0.001 & 0.002 \\ 0 & 0 & -0.002 & 0 & 0 & 0 & 0 & 0 & 0 \\ -0.250 & -0.310 & -0.153 & -0.312 & -0.153 & -0.060 & -0.154 & -0.061 & 0.216 \\ -0.002 & -0.003 & -0.004 & -0.003 & -0.004 & -0.001 & -0.001 & -0.001 & 0.002 \\ 0 & 0 & 0 & -1.517 & 0 & -0.002 & 0 & 0 & 0 \\ 0.024 & -0.036 & -0.158 & -0.036 & -0.158 & -0.062 & -0.159 & -0.063 & 0.223 \\ 0.310 & 0.246 & 0.120 & 0.246 & 0.120 & -0.065 & 0.120 & -0.065 & 0.230 \\ 0.445 & 0.412 & 0.347 & 0.412 & 0.347 & 0.252 & 0.347 & 0.251 & 0.118 \end{bmatrix} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 0.209 \\ 0.002 \\ 0 \\ 0.216 \\ 0.002 \\ 0 \\ 0.223 \\ 0.230 \\ 0.118 \end{bmatrix}$$

If a k-out-of-n voting gate is incorporated in the measurement channel, the time-averaged availability of this channel can be estimated as follows

$$\overline{Av}^{Corr} = \sum_{j=0}^{m-n} \sum_{i=0}^{n-k} P_{i+(n+1)j+1} \tag{16}$$

This is essentially the sum of all asymptotic probabilities corresponding to the channel states with at least k working sensors online. In the above example, the average availability associated with 1-out-of-2 voting gate in the above example can be computed as follows

$$\overline{Av}^{Corr} = \sum_{j=0}^{2} \sum_{i=0}^{1} P_{i+(2+1)j+1} = P_1 + P_2 + P_4 + P_5 + P_7 + P_8 = 0.882 \tag{17}$$

On the other hand, the expected numbers of repairs and replacements per unit time period can be approximated with the following equations (Liang and Chang, 2008).

$$ENRr^{Corr}(m, n) = \mu \left[\sum_{j=1}^{m-n} P_{j(n+1)+1} + \sum_{i=1}^{n} P_{(m-n)(n+1)+i+1} \right] \tag{18}$$

$$ENRpl^{Corr}(m, n) = \varepsilon \left[\sum_{j=0}^{m-n-1} \sum_{i=1}^{n} P_{j(n+1)+i+1} \right] \tag{19}$$

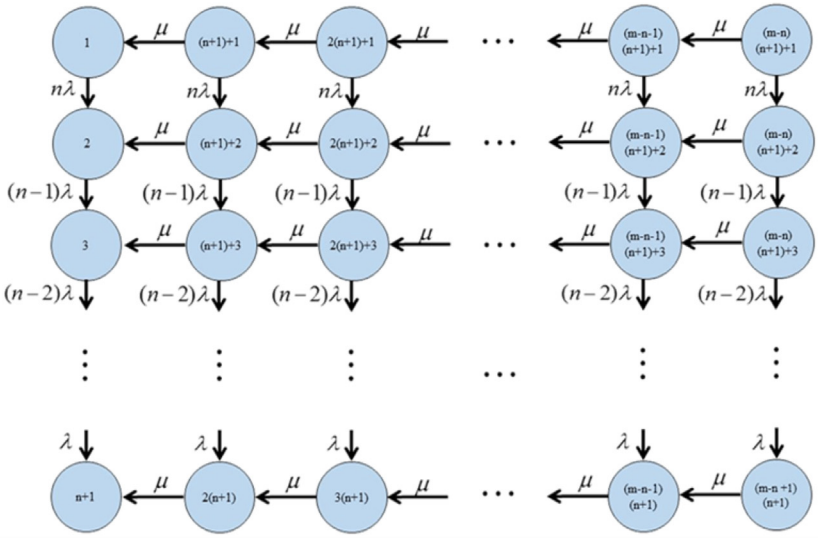

Fig. 5. Markov diagram of a shutdown channel under preventive maintenance program with n online units and $m-n$ spares.

Thus, these numbers in the above example can be calculated accordingly as:

$$ENRr^{Corr}(4,2) = \mu\left[\sum_{j=1}^{2} P_{j(2+1)+1} + \sum_{i=1}^{2} P_{(4-2)(2+1)+i+1}\right] = \mu(P_4 + P_7 + P_8 + P_9) = 2.75\,(\text{month}^{-1}) \tag{20}$$

$$ENRpl^{Corr}(4,2) = \varepsilon\left[\sum_{j=0}^{4-2-1}\sum_{i=1}^{2} P_{j(2+1)+i+1}\right] = \varepsilon(P_2 + P_3 + P_5 + P_6) = 1.46\,(\text{month}^{-1}) \tag{21}$$

3.2. Preventive maintenance policy

The preventive maintenance policy has been used primarily to reduce the probability of hidden or unrevealed failures associated with an actuator, e.g., a solenoid valve, a safety valve, or a rupture discs, etc. Any such unit is operated only after the unsafe process state is detected, while under the normal conditions it should be left idle. A proper preventive maintenance program must be put in place to keep the availability of the shutdown subsystem above an acceptable level. Let us assume that, for a shutdown channel, a total of m identical actuators are purchased and n of them are placed online while the rest are treated as cold standbys. All online actuators in a shutdown channel are inspected regularly at constant intervals. After inspection, the functional unit should be left online and the failed one immediately replaced with a working cold standby (if available). The broken units can only be repaired offline. It is assumed that all failure and repair rates are constants and the aforementioned successive actions for inspection and replacement (which together are referred to as a *switch* in this paper) are always successful, i.e., a "perfect" switch.

Since the aforementioned policy has never been modeled rigorously before, a generalized formulation is presented in the sequel. Let us first consider the Markov diagram in Fig. 5, which is adopted in this work to describe the state transition patterns under the proposed maintenance program between two successive inspections. Within each inspection interval, a transition can be triggered either by failure or repair, and the corresponding failure and repair rates are also denoted as λ and μ, respectively. Note that all channel states can be divided into 9 blocks as shown in Fig. 6.

Since the channel states are renewed after each inspection and the corresponding steady-state probabilities cannot be reached asymptotically before the next inspection, the following *dynamic* models should be adopted to describe the system behavior (Hoyland and Rausand, 1994):

- Block 1

$$\frac{dP_1}{dt} = \mu P_{n+2} - n\lambda P_1 \tag{22}$$

- Block 2

$$\frac{dP_{j(n+1)+1}}{dt} = -(\mu + n\lambda)P_{j(n+1)+1} + \mu P_{(j+1)(n+1)+1}; \quad j = 1, 2, \ldots, (m-n-1). \tag{23}$$

- Block 3

$$\frac{dP_{(m-n)(n+1)+1}}{dt} = -(\mu + n\lambda)P_{(m-n)(n+1)+1} \tag{24}$$

- Block 4

$$\frac{dP_{j+1}}{dt} = (n+1-j)\lambda P_j - (n-j)\lambda P_{j+1} + \mu P_{(j+n+2)}; \quad j = 1, 2, \ldots, (n-1) \tag{25}$$

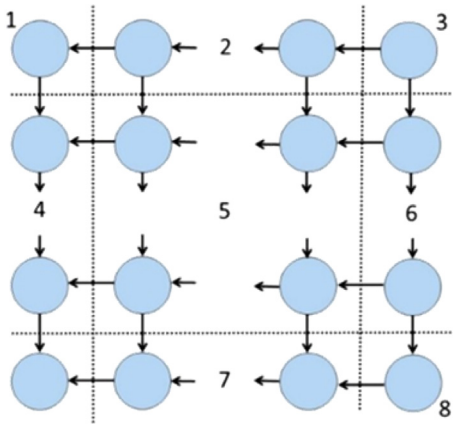

Fig. 6. Classification of the states of a shutdown channel.

- Block 5

$$\frac{dP_{n+2+i+(n+1)(j-1)}}{dt} = -[\mu + (n-i)\lambda]P_{n+2+i+(n+1)(j-1)} + (n-i+1)\lambda P_{n+1+i+(n+1)(j-1)} + \mu P_{n+2+i+(n+1)j};$$
$$i = 1, 2\ldots, (n-1); \quad j = 1, 2, \ldots, (m-n-1). \tag{26}$$

- Block 6

$$\frac{dP_{(m-n)(n+1)+(j+1)}}{dt} = (n+1-j)\lambda P_{(m-n)(n+1)+j} - [\mu + (n-j)\lambda]P_{(m-n)(n+1)+(j+1)}; \quad j = 1, 2, \ldots, (n-1). \tag{27}$$

- Block 7

$$\frac{dP_{(j+1)(n+1)}}{dt} = \lambda P_{(j+1)(n+1)-1} - \mu P_{(j+1)(n+1)} + \mu P_{(j+2)(n+1)}; \quad j = 1, 2, \ldots, (m-n-1). \tag{28}$$

- Block 8

$$\frac{dP_{(m-n+1)(n+1)}}{dt} = \lambda P_{(m-n+1)(n+1)-1} - \mu P_{(m-n+1)(n+1)} \tag{29}$$

Based on the fact that the sum of all state probabilities must equal to one at any time, the probability of state $n+1$ (the only remaining node which is not included in the above eight blocks) can be computed by subtracting all state probabilities in the above eight blocks from 1, i.e.,

$$P_{n+1}(t) = 1 - \sum_{i=1}^{n} P_i(t) - \sum_{j=1}^{(m-n)(n+1)} P_{n+1+j}(t) \tag{30}$$

Let us use T to denote the length of inspection interval and LC the horizon of life cycle. The total number of inspections (st) should be:

$$st = \begin{cases} \dfrac{LC}{T} - 1 & \text{if} \quad \mathrm{mod}\,(LC, T) = 0 \\ \dfrac{LC - \mathrm{mod}\,(LC, T)}{T} & \text{if otherwise} \end{cases} \tag{31}$$

Note that both T and LC are integers in months, and the operand mod (LC, T) returns the remainder of $LC \div T$. Thus the inspections should be performed at the corresponding instances, i.e., $I \times T$ and $I = 1, 2, \ldots, st$. Let us first consider the initial conditions of the entire horizon:

$$P_1(0-\delta) = 1 \tag{32}$$

$$P_{1+i}(0-\delta) = 0; \quad i = 1, \ldots, (m-n+1)(n+1) - 1 \tag{33}$$

where $\delta \to 0$.

The state probabilities at time instance $I \times T (I = 0, 1, 2, \ldots, st)$ can then be expressed in terms of additional parameters K_j^I:

$$K_j^I = P_{1+(j-1)(n+1)}(I \times T) = \sum_{k=0}^{j-1} P_{1+(j-1)(n+1)-nk}(I \times T - \delta), \quad j = 1, 2, \ldots, (m-n) \tag{34}$$

$$K_{m-n+j}^I = P_{(m-n)(n+1)+j}(I \times T) = \sum_{k=0}^{m-n-j+1} P_{(m-n)(n+1)+j-nk}(I \times T - \delta), \quad j = 1, 2, \ldots, (n+1) \tag{35}$$

$$P_{(j-1)(n+1)+k+1}(I \times T) = 0, \quad j = 1, \ldots, m-n+1, \quad k = 1, 2, \ldots, n \tag{36}$$

The resulting analytic expressions of the time-dependent state probabilities can be found in Appendix A. The time-averaged availability of a shutdown channel can then be estimated accordingly on the safe side, i.e., underestimated, with the following formula:

$$\overline{Av}^{Prev} = \frac{1}{LC}\sum_{i=0}^{m-n}\sum_{j=1}^{n}\left[\int_{st\times T}^{LC} P_{i(n+1)+j}(t)dt + \sum_{k=1}^{st}\int_{kT}^{(k+1)T} P_{i(n+1)+j}(t)dt\right] \approx \frac{1}{(st+1)}\sum_{k=1}^{st+1}\left[\sum_{i=0}^{m-n}\sum_{j=1}^{n} P_{i(n+1)+j}(kT)\right] = \frac{1}{st+1}\left[\sum_{k=1}^{st+1} Av_k^{Prev}\right] \tag{37}$$

The corresponding expected number of repairs per unit time period can also be approximated with the following equations

$$ENRr^{Prev} = \frac{\mu}{LC}\sum_{a=1}^{m-n}\sum_{b=1}^{n+1}\left[\int_{st\times T}^{LC} P_{a(n+1)+b}(t)dt + \sum_{k=1}^{st}\int_{(k-1)T}^{kT} P_{a(n+1)+b}(t)dt\right] \approx \frac{\mu}{(st+1)T}\sum_{k=1}^{st+1} T\left[\sum_{a=1}^{m-n}\sum_{b=1}^{n+1} P_{a(n+1)+b}(kT)\right] = \frac{\mu}{st+1}\sum_{k=1}^{st+1} ENRr(kT) \tag{38}$$

To facilitate clear understanding, let us consider a shutdown channel for which two actuators ($n=2$) are purchased together with 2 standbys ($m-n=2$). Let us further assume that the inspection interval is 6 months and the time horizon of life cycle is 60 months. Therefore, the number of inspections should be: $st = 60/6 - 1 = 9$. The initial conditions of every inspection interval can thus be expressed as:

$$\begin{aligned}
K_1^I &= P_1(I\times T) = P_1(I\times T - \delta)\\
K_2^I &= P_4(I\times T) = P_2(I\times T - \delta) + P_4(I\times T - \delta)\\
K_3^I &= P_7(I\times T) = P_3(I\times T - \delta) + P_5(I\times T - \delta) + P_7(I\times T - \delta)\\
K_4^I &= P_8(I\times T) = P_6(I\times T - \delta) + P_8(I\times T - \delta)\\
K_5^I &= P_9(I\times T) = P_9(I\times T - \delta)\\
P_2(I\times T) &= P_3(I\times T) = P_5(I\times T) = P_6(I\times T) = 0
\end{aligned} \tag{39}$$

With a failure rate (λ) of 1.2 month^{-1} and a repair rate (μ) of 2.8 month^{-1}, the above dynamic model can be solved and the resulting availabilities and the expected numbers of repairs at all inspections are listed in Tables 1 and 2 respectively. The time-averaged availability can be approximated with the data in Table 1 as follows:

$$\overline{Av}^{Prev} \approx \frac{Av_1^{Prev} + \cdots + Av_9^{Prev} + Av_{10}^{Prev}}{10} = 0.8840$$

From Table 2, one can estimate the expected number of repairs:

$$ENRr^{Prev} \approx \frac{ENRr_1^{Prev} + \cdots + ENRr_{10}^{Prev}}{10} = 1.3834\,\text{month}^{-1}$$

Table 1
Estimation of $\overline{Av}^{Prev}$.

k	Av_k^{Prev}
1	0.9216
2	0.9216
3	0.9013
4	0.8844
5	0.8751
6	0.8703
7	0.8678
8	0.8665
9	0.8659
10	0.8658

Table 2
Estimation of $ENRr^{Prev}$.

k	$ENRr_k^{Prev}$
1	0
2	1.2192
3	1.4397
4	1.5315
5	1.5765
6	1.5992
7	1.6108
8	1.6168
9	1.6198
10	1.6213

4. Computation procedure for evaluating life-cycle expenditure

Two components of the computation procedure are presented below.

4.1. Encoding scheme

A systematic encoding scheme has been developed in this work to facilitate automatic implementation of genetic algorithm. Notice first that the model parameters used for characterizing the system configuration and the corresponding maintenance programs must first be selected and translated into binary numbers for computing the life-cycle expenditure. To perform the required evolutionary computation, every such number must be placed at its designated location on a string of binary digits (which is referred to as a "chromosome" in the present paper). The template for chromosomes should be constructed first according to the total number of protection layers, the numbers of channels in the alarm and shutdown subsystems in each layer, the maximum numbers of online and spare sensors in every measurement channel, the maximum numbers of online and standby actuators in each shutdown channel, and the maximum length of inspection interval of each shutdown channel. After building the template for a particular application, one can then fill it with the following selections sequentially for each protection layer: (1) the number of online sensors in every measurement channel, (2) the number of spare sensors for every measurement channel, (3) the voting gate in every measurement channel, (4) the alarm logic, (5) the numbers of online and standby units in each shutdown channel, and (6) the length of inspection interval for each shutdown channel.

For illustration convenience, let us consider a single-layer system with $M=3$ and $K=2$ in the superstructure (see Fig. 2) and the corresponding template can be specified as follows:

1. The maximum numbers of online sensors in measurement channels are all selected to be 7 in this example. Thus, 3 binary digits are needed to represent each number and, in the first section of chromosome, a total of 9 digits should be allocated.
2. Similarly, 3 digits should be reserved for determining the number of spare sensors for each of the three measurement channels and a total of 9 digits are placed in the second section of chromosome.
3. The third section is used to stipulate the k-out-of-n voting gates. Note that, for each channel, the corresponding number of online sensors (i.e., n) are given in section 1 and 3 digits are also adopted in the present section to represent the number of spares. Therefore, a total of 9 digits are used in this section. Because these digits are selected randomly, the resulting value of k may be greater than that of n. The following special constraints are imposed to ensure $k \leq n$, i.e.

$$k = \begin{cases} n & \text{if } k > n \\ k & \text{if } 0 < k \leq n \\ 1 & \text{if } k = 0 \end{cases} \tag{40}$$

4. The 6 digits in section 4 are utilized for specifying the alarm logic. Note first that the total number of all possible combinations of the channel outputs should be $2^M = 2^3 = 8$. These eight combinations are labeled numerically in sequence from 0 to 7 and, furthermore, each label simultaneously reflects the collective state of channel outputs with three binary digits, i.e., $y_1y_2y_3$. For examples, 101 denotes the label 5, 011 denotes 3 and 001 denotes 1, etc. Secondly, it should be noted that each combination may result in either an alarm (i.e., 1) or otherwise (i.e., 0). Since it is logically coherent to assume that $f(0)=0$ and $f(1)=1$, where $0 = [\,0 \quad 0 \quad 0\,]^T$ and $1 = [\,1 \quad 1 \quad 1\,]^T$, the alarm decisions of the remaining 6 ($=2^3-2$) combinations can be specified with 6 digits. For example, one possible set of selections can be expressed below with the six underlined binary values in the last column.

No.	y_1	y_2	y_3	$f(y_1, y_2, y_3)$
0	0	0	0	0
1	1	0	0	<u>0</u>
2	0	1	0	<u>1</u>
3	1	1	0	<u>1</u>
4	0	0	1	<u>0</u>
5	1	0	1	<u>1</u>
6	0	1	1	<u>0</u>
7	1	1	1	1

5. The maximum numbers of online actuators in shutdown channels are all chosen to be 7 in this example. Thus, 3 binary digits are needed to represent each number and, in the fifth section of chromosome, a total of 6 digits should be allocated.
6. Similarly, 3 digits should be reserved for determining the number of cold standbys for each of the two shutdown channels and a total of 6 digits are placed in the sixth section of chromosome.
7. It is assumed that the maximum length of inspection interval for each channel is 15 months. Thus, 4 digits should be used to represent the length of each interval and 8 digits should be placed in the last section.

Based on the above specifications, a 53-digit chromosome can be constructed to characterize the interlock. To illustrate the encoding scheme more clearly, let us consider the arbitrarily selected chromosome given below:

100 010 101|100 010 001|100 100 010|11111|100 100|101 100|1100 1010

The structural features of interlock can be extracted section-by-section sequentially from this chromosome, i.e., numbers of online sensors: 1, 2, 5; numbers of spare sensors: 1, 2, 4; voting gates: 1oo1, 1oo2, 2oo5; alarm logic: OR; numbers of online actuators: 1, 1; numbers of standby actuators: 5, 1; lengths of inspection intervals: 3, 5.

In addition, notice the template strings for characterizing different layers in an interlock can be built *independently* and placed in sequence to form a single chromosome. For example, let us assume that a second layer ($M = 2$ and $K = 1$) can be added to the aforementioned single-layer interlock. Let us also chose the same parameters, i.e., the maximum numbers of online and spare sensors in every measurement channel, the maximum numbers of online and standby units in each shutdown channel, and the maximum length of inspection interval of each shutdown channel, to construct the second part of a template for the second layer. For illustration convenience, an arbitrarily selected chromosome is also given below:

100 010 101|100 010 001|100 100 010|111111|100 100|101 100|1100 1010||010 111|101 110|100 011|01|011|101|0011

Note that in this chromosome a double vertical line is used to separate the strings representing the two layers. The structure of the first layer is the same as before, while that of the second can be decoded as follows: the numbers of online sensors are 2 and 7; the numbers of spare sensors are 5 and 3; the voting gates are 1oo2 and 6oo7; the alarm logic is trivial; the number of online actuators is 6; the number of standbys is 5; the length of inspection intervals is 12.

4.2. Evaluation procedure

The total life-cycle expenditure includes the total expected life-cycle loss and the life-cycle costs of alarm and shutdown subsystems. Although the expected life-cycle loss for operating a single-layer protective system (L_1^{LC}) has already been derived previously (Liang and Chang, 2008; Liao and Chang, 2010), a summary of the critical formulations is still presented in Appendix B for the sake of completeness. The resulting expression in Eq. (B24) in this appendix is repeated below:

$$L_1^{LC} = \left[C_a(1-p)\left(P_{FS}^{SD} + (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y_1,y_2,\ldots,y_M} \left\{ f(y_1, y_2, \ldots, y_M) \prod_{i=1}^{M} [A_i^{y_i}(1-A_i)^{1-y_i}] \right\} \right) + C_b p \left((1 - P_{FS}^{SD}) - (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y_1,y_2,\ldots,y_M} \left\{ f(y_1, y_2, \ldots, y_M) \prod_{i=1}^{M} [B_i^{1-y_i}(1-B_i)^{y_i}] \right\} \right) \right] CFS_{LC} \tag{41}$$

where C_a and C_b respectively denotes the financial losses incurred from FS and FD interlock failures; p denotes the time-averaged probability of an unsafe process state occurring in a year; A_i and B_i respectively denote the conditional probabilities of FS and FD failures of the ith measurement channel; P_{FS}^{SD} and P_{FD}^{SD} respectively denote the conditional probabilities of FS and FD failures of the shutdown subsystem; CFS_{LC} is a multiplication factor that takes the time value of money into consideration. Notice that all symbols in the above equation are also defined mathematically in Appendix B.

On the other hand, the life-cycle cost of alarm subsystem ($C_{AL,1}^{LC}$) is the sum of (1) the total purchase cost, (2) the total expected repair cost and (3) the total expected replacement cost of sensors, while that of shutdown subsystem ($C_{SD,1}^{LC}$) is the sum of (1) the total purchase cost, (2) the total inspection/replacement cost and (3) the total expected repair cost of actuators. More specifically, these two life-cycle costs can be expressed as

$$C_{AL,1}^{LC} = \sum_{i=1}^{M} \{ m_i PCS_i + CFS_{LC}[ENRr_i(m_i, n_i)\overline{RprsC_i} + ENRpl_i(m_i, n_i)\overline{RplsC_i}] \} \tag{42}$$

$$C_{SD,1}^{LC} = \sum_{j=1}^{K} \{ m_j PCV_j + CFS_{LC}[ENRr_j^{Prev}(m_j, n_j)\overline{RprsC_j} + st_j InspC_j] \} \tag{43}$$

where PCS_i, $\overline{RprsC}_i$ and $\overline{RplsC}_i$ respectively denote the purchase cost, repair and replacement costs of a sensor in measurement channel i; and PCV_j $\overline{RprsC}_j$ and $InspC_j$ respectively denote the purchase cost, repair and inspection costs of an actuator in inspection channel j. The objective function of the mathematical program for a single protection layer can thus be written as:

$$obj_1 = L_1^{LC} + C_{AL,1}^{LC} + C_{SD,1}^{LC} \tag{44}$$

In fact, this objective function can be extended to represent the total life-cycle expenditure of a multilayer interlock (obj_Ω), i.e.

$$obj_\Omega = L_\Omega^{LC} + C_{AL,\Omega}^{LC} + C_{SD,\Omega}^{LC} \tag{45}$$

where Ω denotes the total number of protection layers. To fix ideas, let us consider the CSTR system in Fig. 7 as an example. Note that the interlock of this system consists of three layers. The first layer is a flow interlock, in which the feed flow is cut off when the flow rate exceeds a predetermined value. If this protection mechanism fails, the resulting abnormal flow rate could raise the reactor temperature and trigger the temperature interlock in the second layer. A subsequent trip operation is supposed to cut off the inlet flow. If a FD failure occurs in this second layer, the temperature increase may continue. As a result, the reactor pressure may be driven to a very high level. To prevent the catastrophic runaway reaction and explosion, a pressure relief system is installed to vent the reactor contents at a set pressure.

The total life-cycle cost of the alarm subsystems in all layers ($C_{AL,\Omega}^{LC}$) can be expressed by introducing an additional index r to distinguish different layers as follows:

$$C_{AL,\Omega}^{LC} = \sum_{r=1}^{\Omega} \sum_{i=1}^{M_r} \{ m_{r,i} PCS_{r.i} + CFS_{LC}[ENRr_{r,i}(m_{r,i}, n_{r,i})\overline{RprsC_{r,i}} + ENRpl_{r,i}(m_{r,i}, n_{r,i})\overline{RplsC_{r,i}}] \} \tag{46}$$

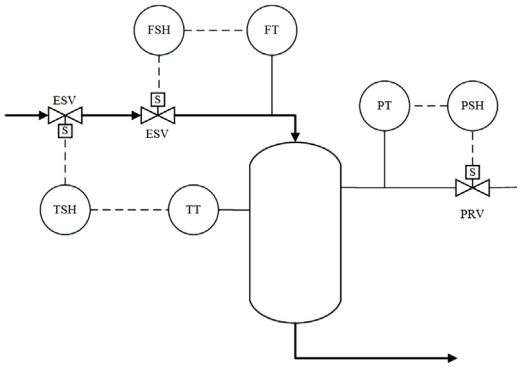

Fig. 7. A CSTR with three protection layers.

Similarly, the total life-cycle cost of the shutdown subsystems in all layers ($C^{LC}_{SD,\Omega}$) can be written as:

$$C^{LC}_{SD,\Omega} = \sum_{r=1}^{\Omega}\sum_{j=1}^{K_r}\{m_{r,j}PCV_{r,j} + CFS_{LC}[ENRr^{Prev}_{r,j}(m_{r,j}, n_{r,j})\overline{RprsC_{r,j}} + st_{r,j}InspC_{r,j}]\} \tag{47}$$

In order to obtain an explicit expression for computing the corresponding total expected life-cycle loss in the aforementioned example, three binary variables are introduced to represent the process states of three distinct layers respectively, that is

$$x^{(1)} = x^F = \begin{cases} 1 & \text{if the inlet flow rate exceeds the alarm limit} \\ 0 & \text{otherwise} \end{cases} \tag{48}$$

$$x^{(2)} = x^T = \begin{cases} 1 & \text{if the reactor temperature exceeds the alarm limit} \\ 0 & \text{otherwise} \end{cases} \tag{49}$$

$$x^{(3)} = x^P = \begin{cases} 1 & \text{if the reactor pressure exceeds the alarm limit} \\ 0 & \text{otherwise} \end{cases} \tag{50}$$

From each of the two possible initial states in the first layer, an event tree can be constructed as shown in Fig. 8. The labels FS^F, FS^T, and FS^P represent the FS failures of the flow, temperature and pressure interlocks respectively, while FD^F, FD^T, and FD^P denote the corresponding FD failures.

Notice that three branches in the first event tree represent undesirable scenarios with different financial penalties. A fail-safe failure of the pressure-relief layer (FS^P) usually ends up with the undesirable consequences of venting reactor contents and prolonged down time, while it may take considerable effort to resume normal operation if another layer fails safely (FS^F or FS^T). Thus it is reasonable to assume that $C^F_a \le C^T_a \le C^P_a$.

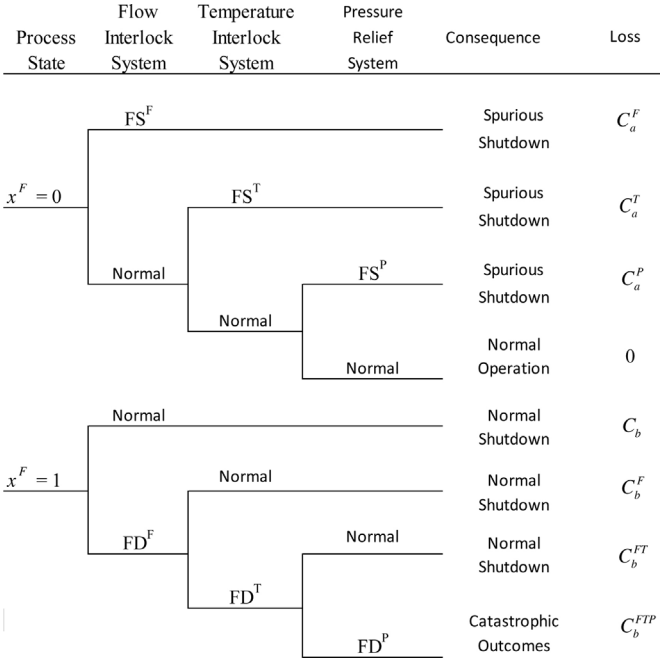

Fig. 8. Event trees for a CSTR with three protection layer.

On the other hand, notice that only one scenario is undesirable in the second event tree, i.e., when all protection layers fail dangerously. Since the other scenarios are in fact *anticipated* in the original interlock design, the implied costs are not included in the objective function to be minimized. Furthermore, since $C_b \le C_b^F \le C_b^{FT} \ll C_b^{FTP}$, it is logical to ignore these anticipated scenarios.

The total expected loss of operating 3 protection layers in Fig. 8 can therefore be expressed as:

$$L_3^{LC} = LCC_a^{(1)}(1-p^{(1)})Pr\{FS^{(1)}\} + LCC_a^{(2)}(1-p^{(1)})(1-Pr\{FS^{(1)}\})Pr\{FS^{(2)}\} + LCC_a^{(3)}(1-p^{(1)})(1-Pr\{FS^{(1)}\})(1-Pr\{FS^{(2)}\})Pr\{FS^{(3)}\} + LCC_b p^{(1)} Pr\{FD^{(1)}\}Pr\{FD^{(2)}\}Pr\{FD^{(3)}\} \quad (51)$$

where $LCC_a^{(1)} = C_a^F \times CFS_{LC}$; $LCC_a^{(2)} = C_a^T \times CFS_{LC}$; $LCC_a^{(3)} = C_a^P \times CFS_{LC}$; $LCC_b = C_b^{FTP} \times CFS_{LC}$; CFS_{LC} is a multiplication factor defined in Eq. (B17). Notice that the probabilities of triggering the first, second and third interlock layers can be expressed respectively as

$$p^{(1)} = Pr\{x^F = 1\} \quad (52)$$

$$p^{(2)} = Pr\{x^T = 1\} = p^{(1)}Pr\{FD^{(1)}\} \quad (53)$$

$$p^{(3)} = Pr\{x^P = 1\} = p^{(1)}Pr\{FD^{(1)}\}Pr\{FD^{(2)}\} \quad (54)$$

The conditional probabilities of FS and FD failures in the above equations can be expressed as

$$Pr\{FS^{(1)}\} = \sum_{\mathbf{y}^{(1)}} Pr\{\mathbf{y}^{(1)} \,|\, x^{(1)} = x^F = 0\} \times [Pr\{h^{(1)}(\mathbf{z}^{(1)}) = 0 \,|\, f^{(1)}(\mathbf{y}^{(1)}) = 1\} f^{(1)}(\mathbf{y}^{(1)}) + Pr\{h^{(1)}(\mathbf{z}^{(1)}) = 1 \,|\, f^{(1)}(\mathbf{y}^{(1)}) = 0\}(1 - f^{(1)}(\mathbf{y}^{(1)}))]$$

$$= P_{FS}^{SD^{(1)}} + (1 - P_{FS}^{SD^{(1)}} - P_{FD}^{SD^{(1)}}) \sum_{\mathbf{y}^{(1)}} f^{(1)}(\mathbf{y}^{(1)}) Pr\{\mathbf{y}^{(1)} \,|\, x^{(1)} = x^F = 0\} \quad (55)$$

$$Pr\{FD^{(1)}\} = \sum_{\mathbf{y}^{(1)}} Pr\{\mathbf{y}^{(1)} \,|\, x^{(1)} = x^F = 1\} \times [Pr\{h^{(1)}(\mathbf{z}^{(1)}) = 0 \,|\, f^{(1)}(\mathbf{y}^{(1)}) = 1\} f^{(1)}(\mathbf{y}^{(1)}) + Pr\{h^{(1)}(\mathbf{z}^{(1)}) = 1 \,|\, f^{(1)}(\mathbf{y}^{(1)}) = 0\}(1 - f^{(1)}(\mathbf{y}^{(1)}))$$

$$= (1 - P_{FS}^{SD^{(1)}}) - (1 - P_{FS}^{SD^{(1)}} - P_{FD}^{SD^{(1)}}) \sum_{\mathbf{y}^{(1)}} f^{(1)}(\mathbf{y}^{(1)}) Pr\{\mathbf{y}^{(1)} \,|\, x^{(1)} = x^F = 1\} \quad (56)$$

$$Pr\{FS^{(2)}\} = \sum_{\mathbf{y}^T} Pr\{\mathbf{y}^{(2)} \,|\, x^{(2)} = x^T = 0\} \times [Pr\{h^{(2)}(\mathbf{z}^{(2)}) = 0 \,|\, f^{(2)}(\mathbf{y}^{(2)}) = 1\} f^{(2)}(\mathbf{y}^{(2)}) + Pr\{h^{(2)}(\mathbf{z}^{(2)}) = 1 \,|\, f^{(2)}(\mathbf{y}^{(2)}) = 0\}(1 - f^{(2)}(\mathbf{y}^{(2)}))]$$

$$= P_{FS}^{SD^{(2)}} + (1 - P_{FS}^{SD^{(2)}} - P_{FD}^{SD^{(2)}}) \sum_{\mathbf{y}^{(2)}} f^{(2)}(\mathbf{y}^{(2)}) Pr\{\mathbf{y}^{(2)} \,|\, x^{(2)} = x^T = 0\} \quad (57)$$

$$Pr\{FD^{(2)}\} = \sum_{\mathbf{y}^{(2)}} Pr\{\mathbf{y}^{(2)} \,|\, x^{(2)} = x^T = 1\} \times [Pr\{h^{(2)}(\mathbf{z}^{(2)}) = 0 \,|\, f^{(2)}(\mathbf{y}^{(2)}) = 1\} f^{(2)}(\mathbf{y}^{(2)}) + Pr\{h^{(2)}(\mathbf{z}^{(2)}) = 1 \,|\, f^{(2)}(\mathbf{y}^{(2)}) = 0\}(1 - f^{(2)}(\mathbf{y}^{(2)}))$$

$$= (1 - P_{FS}^{SD^{(2)}}) - (1 - P_{FS}^{SD^{(2)}} - P_{FD}^{SD^{(2)}}) \sum_{\mathbf{y}^{(2)}} f^{(2)}(\mathbf{y}^{(2)}) Pr\{\mathbf{y}^{(2)} \,|\, x^{(2)} = x^T = 1\} \quad (58)$$

$$Pr\{FS^{(3)}\} = \sum_{\mathbf{y}^P} Pr\{\mathbf{y}^{(3)} \,|\, x^{(3)} = x^P = 0\} \times [Pr\{h^{(3)}(\mathbf{z}^{(3)}) = 0 \,|\, f^{(3)}(\mathbf{y}^{(3)}) = 1\} f^{(3)}(\mathbf{y}^{(3)}) + Pr\{h^{(3)}(\mathbf{z}^{(3)}) = 1 \,|\, f^{(3)}(\mathbf{y}^{(3)}) = 0\}(1 - f^{(3)}(\mathbf{y}^{(3)}))]$$

$$= P_{FS}^{SD^{(3)}} + (1 - P_{FS}^{SD^{(3)}} - P_{FD}^{SD^{(3)}}) \sum_{\mathbf{y}^{(3)}} f^{(3)}(\mathbf{y}^{(3)}) Pr\{\mathbf{y}^{(3)} \,|\, x^{(3)} = x^P = 0\} \quad (59)$$

$$Pr\{FD^{(3)}\} = \sum_{\mathbf{y}^{(3)}} Pr\{\mathbf{y}^{(3)} \,|\, x^{(3)} = x^P = 1\} \times [Pr\{h^{(3)}(\mathbf{z}^{(3)}) = 0 \,|\, f^{(3)}(\mathbf{y}^{(3)}) = 1\} f^{(3)}(\mathbf{y}^{(3)}) + Pr\{h^{(3)}(\mathbf{z}^{(3)}) = 1 \,|\, f^{(3)}(\mathbf{y}^{(3)}) = 0\}(1 - f^{(3)}(\mathbf{y}^{(3)}))$$

$$= (1 - P_{FS}^{SD^{(3)}}) - (1 - P_{FS}^{SD^{(3)}} - P_{FD}^{SD^{(3)}}) \sum_{\mathbf{y}^{(3)}} f^{(3)}(\mathbf{y}^{(3)}) Pr\{\mathbf{y}^{(3)} \,|\, x^{(3)} = x^P = 1\} \quad (60)$$

where $\mathbf{y}(r)$ is a vector of outputs from the measurement channels in layer r (r = 1, 2, 3) and $f^{(r)}(\cdot)$ represents the corresponding alarm function; $\mathbf{z}^{(r)}$ is a vector of outputs from the shutdown channels in layer r (r = 1, 2, 3) and $h^{(r)}(\cdot)$ represents the corresponding shutdown function; $P_{FS}^{SD^{(r)}}$ and $P_{FD}^{SD^{(r)}}$ represent respectively the conditional probabilities of FS and FD failures in the shutdown subsystem of layer r (r = 1, 2, 3). More specifically,

$$P_{FS}^{SD^{(r)}} = Pr\{h^{(r)}(\mathbf{z}^{(r)}) = 1 \,|\, f^{(r)}(\mathbf{y}^{(r)}) = 0\} = \prod_{j=1}^{K^{(r)}} ASD_j^{(r)} \quad (61)$$

$$P_{FD}^{SD(r)} = Pr\{h^{(r)}(\mathbf{z}^{(r)}) = 0 \,|f^{(r)}(\mathbf{y}^{(r)}) = 1\} = 1 - \prod_{j=1}^{K^{(r)}}(1 - BSD_j^{(r)}) \tag{62}$$

The remaining conditional probabilities concerning the FS and FD failures of the measurement channels in Eqs. (55)–(60) can be expressed as

$$Pr\{\mathbf{y}^{(r)} \,|x^{(r)} = 0\} = \prod_{i=1}^{M^{(r)}}[A_i^{y_i^{(r)}}(1 - A_i)^{1-y_i^{(r)}}] \tag{63}$$

$$Pr\{\mathbf{y}^{(r)} \,|x^{(r)} = 1\} = \prod_{i=1}^{M^{(r)}}[B_i^{1-y_i^{(r)}}(1 - B_i)^{y_i^{(r)}}] \tag{64}$$

where $r = 1, 2, 3$. Thus, on the basis of Eq. (51), the generalized formula for computing the total expected life-cycle loss associated with a multilayer protective system can be expressed as:

$$L_{\Omega}^{LC} = (1 - p^{(1)})\sum_{r=1}^{\Omega} LCC_a^{(r)}\left[\prod_{i=0}^{r-1}(1 - Pr\{FS^{(i)}\})\right] Pr\{FS^{(r)}\} + LCC_b p^{(1)}\prod_{r=1}^{\Omega} Pr\{FD^{(r)}\} \tag{65}$$

where Ω is the total number of protection layers and $\Omega = 3$ in the above example.

5. Genetic algorithms

The genetic algorithm (GA) is an optimization technique developed from the principles of genetics and natural selection. A generalized flowchart can be found in Fig. 9, and the basic code to realize these steps is obtained from Haupt and Haupt (2004). The resulting computer program allows some of the chromosomes evolve to a state that minimizes the total life-cycle expenditure or so-called "fitness function".

5.1. Chromosome generation

The population size N_{pop} must be determined a priori before generating the chromosomes and, in this work, it is set at 180 in most cases. Notice that the general structure of a chromosome has already been outlined previously in section 4, and every embedded binary digit is generated randomly with the MATLAB function "randi". To make sure that the resulting interlock structure is always valid, a screening procedure is applied to check every randomly-generated chromosome if zeros appear in the designated sections (i.e., those represent the numbers of online sensors and spares in each measurement channel, the parameter "k" of the corresponding voting gate, the numbers of online actuators and standbys in each shutdown channel and the length of inspection interval.). All such chromosomes are removed from the current population and, to make up for these unqualified candidates, the same number of additional chromosomes should be generated and checked again.

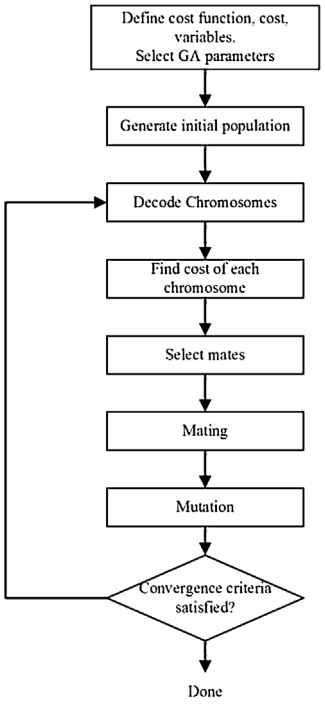

Fig. 9. General flowchart of binary GA (Haupt and Haupt, 2004).

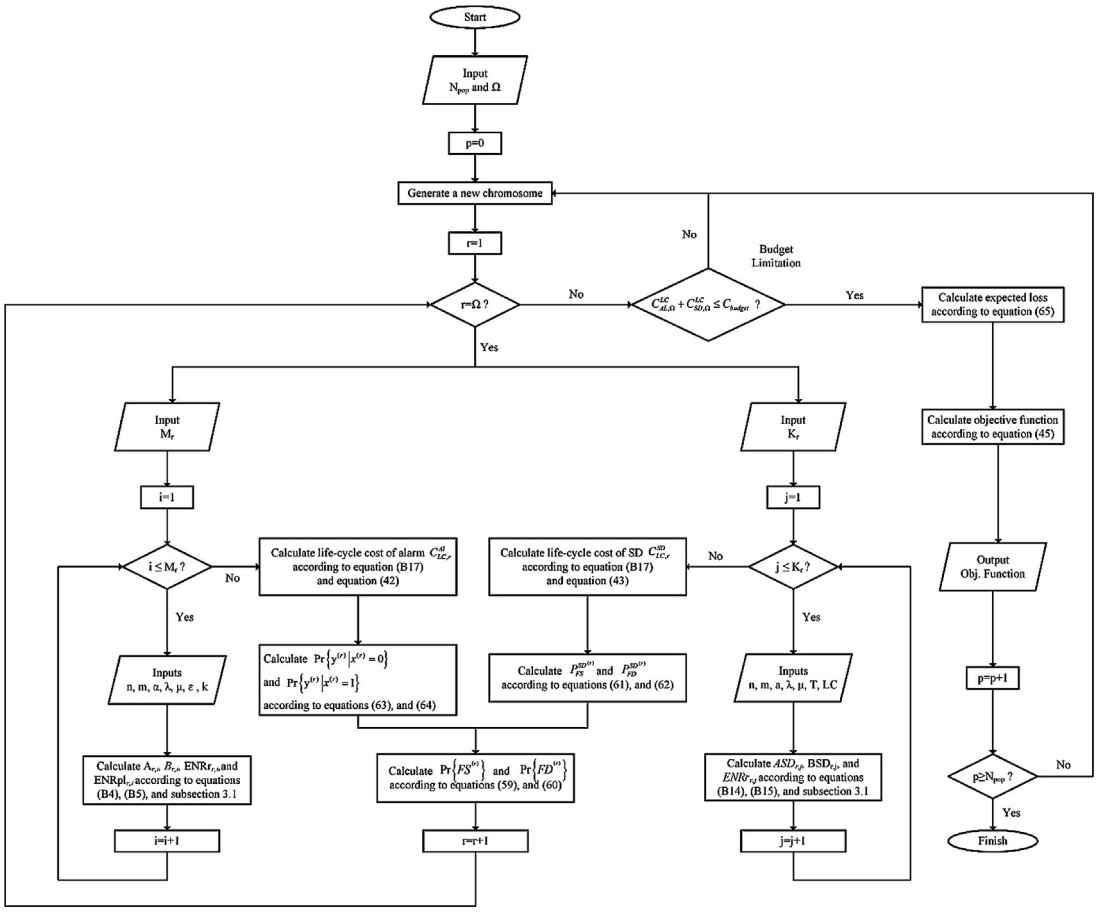

Fig. 10. Flowchart for fitness evaluation.

5.2. Fitness evaluation

After producing a complete population, the interlock parameters decoded from each chromosome can then be used to compute the fitness measure, i.e., the corresponding total life-cycle expenditure, according to the flowchart in Fig. 10. In certain applications, it is also necessary to impose the budget constraint as follows:

$$C^{LC}_{AL,\Omega} + C^{LC}_{SD,\Omega} \le C_{budget} \tag{66}$$

This constraint can be easily incorporated in the computation procedure by performing a check just before the calculations of total expected loss and after those of the life-cycle costs of alarm and shutdown subsystems (see Fig. 10).

5.3. Evolution procedure: selection, mating and mutation

In the selection step, the survival-of-the-fittest law translates into the practice of discarding chromosomes with higher costs. To this end, the chromosomes in a population are ranked according to their objective values, i.e., the total life-cycle expenditures. The one with the lowest objective value is ranked first and has the biggest chance of being selected with roulette. A so-called “selection rate” is applied to control the percentage of a population that is allowed to reproduce (mate) in the next generation (e.g., 0.5). To accelerate the convergence speed, an additional selection practice is also adopted, i.e., always keeping the elite chromosome(s). In other words, a clone of the best individual (i.e., the one with the minimum objective value) in the previous generation is included for mating in the current generation.

The mating step is adopted for creation of one or more offspring from the parents selected in the pairing process. The most common form of this matting involves two parents that produce two offspring. A single-point crossover is used on this research. The crossover point is placed at the middle of the chromosome.

To avoid premature convergence before sampling a large enough portion of the cost surface, the random mutation step should be performed. Not all chromosomes in a population need to be mutated. When a single-point mutation occurs on the selected chromosome, a 1 is changed to a 0 at the designated digit, and vice versa.

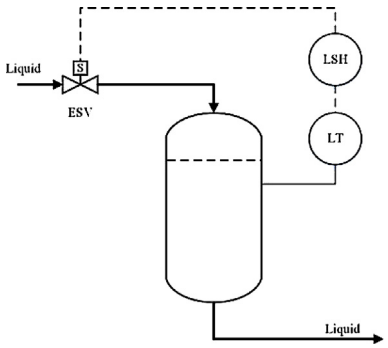

Fig. 11. A liquid storage vessel with level interlock.

5.4. Convergence criteria

Two convergence criteria are adopted in this work. Firstly it is necessary to impose upper and lower limits on the iteration number n, i.e.

$$N_{iteration}^{\min} \le n \le N_{iteration}^{\max} \tag{67}$$

The upper limit $N_{iteration}^{\max}$ is used primarily to avoid overwhelmingly large computation time, while $N_{iteration}^{\min}$ to promote the chance of reaching global optimum. Note that using a large lower bound may also result in a longer-than-necessary convergence time.

The second criterion is imposed on the basis of the convergence error, which is defined in this work as follows

$$\text{error}_n = \left| \frac{obj_n - obj_{n+1}}{obj_n} \right| \le \text{tolerance} \tag{68}$$

where obj_n is the total life-cycle expenditure at iteration n and tolerance is a constant (e.g., 10^{-4}). To establish convergence in a GA run, a series of $N_{tolerance}$ (e.g., 10) consecutive errors are all required to satisfy Eq. (68). To facilitate checking at iteration n, a check counter ($tolerancecounter_n$) and the corresponding total number of confirmed checks ($Ntest_n$) are defined respectively as follows

$$tolerancecounter_n = \begin{cases} 1 & \text{tolerance} \ge \text{error}_n \\ 0 & \text{otherwise} \end{cases} \tag{69}$$

$$Ntest_n = \sum_{i=n-N_{tolerance}+1}^{n} tolerancecounter_i \tag{70}$$

The decision to terminate the evolution process can then be expressed with a binary variable *stop*, i.e.

$$stop = \begin{cases} 1 & \text{if}(n \ge N_{iteration}^{\min} \text{ and } Ntest_n \ge N_{tolerance}) \text{ or } (n \ge N_{iteration}^{\max}) \\ 0 & \text{otherwise} \end{cases} \tag{71}$$

5.5. Example 1

To further illustrate the aforementioned computation procedure, let us consider the single-layer single-channel high-level interlock installed on a liquid storage vessel (see Fig. 11). It is assumed that the system's operating life (H) is 5 years and the time-averaged probability of an unsafe state (p) in each year is constant at 0.2. At an interest rate of 6% per year, the life-cycle cost parameters adopted for the FS and FD failures are $LCC_a = 4.4651 \times 10^4$ USD and $LCC_b = 4.4651 \times 10^6$ USD respectively.

Since there is only one measurement channel in this example, the alarm logic should be always 1oo1. Let us assume that there can be at most 15 online level sensors (4 binary digits) and 15 spares (4 binary digits) in this channel. Thus, 4 additional digits must also be allocated in the chromosome to represent the corresponding voting gate. The maintenance and cost parameters of the level-measurement channel are listed below:

$$\lambda_i = 0.2\,\text{yr}^{-1}; \quad \mu_i = 0.9\,\text{yr}^{-1}; \quad \varepsilon_i = 50\,\text{yr}^{-1}; \quad a_i = 0.1; \quad PCS_i = 200\,\text{USD}; \quad \overline{RprsC_i} = 35.7\,\text{USD}; \quad \overline{RplsC_i} = 17.9\,\text{USD}.$$

On the other hand, it is assumed that there are at most three solenoid valves available in the shutdown subsystem (2 binary digits), the maximum number of spares is fifteen (4 binary digits), and the maximum length of inspection period is 15 months (4 binary digits). There is only one valve type and its specifications are

$$\lambda_j = 0.35\,\text{yr}^{-1}; \quad a_j = 0.1; \quad PCV_j = 150\,\text{USD}; \quad \overline{InsPC_j} = 44.7\,\text{USD}; \quad \overline{RprlC_j} = 267.9\,\text{USD}$$

On the basis of the aforementioned specifications, one can deduce that the length of each chromosome should be 22 digits. To facilitate implementation of GA, the following algorithmic parameters were also used: mating rate = 0.90; mutation rate = 0.10; selection rate = 0.5; $N_{pop} = 180$. Five optimization runs have been performed according to different levels of budget constraint, and the corresponding optimization results are summarized in Table 3 and Fig. 12.

Table 3
Optimization results in Example 1.

	Run no.				
	1.1	1.2	1.3	1.4	1.5
Objective function (obj_1)	17,934.6	17,934.6	18,461.1	20,316.8	24,848.0
Budget limit (USD)	10,000	7000	6000	3500	2500
Total expected loss (USD)	11,566.5	11,556.5	12,897.5	16,848.5	22,397.8
Total purchase cost (USD)	3650	3650	3650	1650	1250
Total expected maint. cost (USD)	2728.1	2728.1	1913.6	1818.3	1200.2
Number of online sensors/spares	3/13	3/13	3/13	1/5	1/3
Voting gate	2oo3	2oo3	2oo3	1oo1	1oo1
Number of solenoid valves/standbys	3/15	3/15	3/15	3/15	3/15
Inspection interval (months)	5	5	8	8	12
Run time (s)	5	5	7	8	12

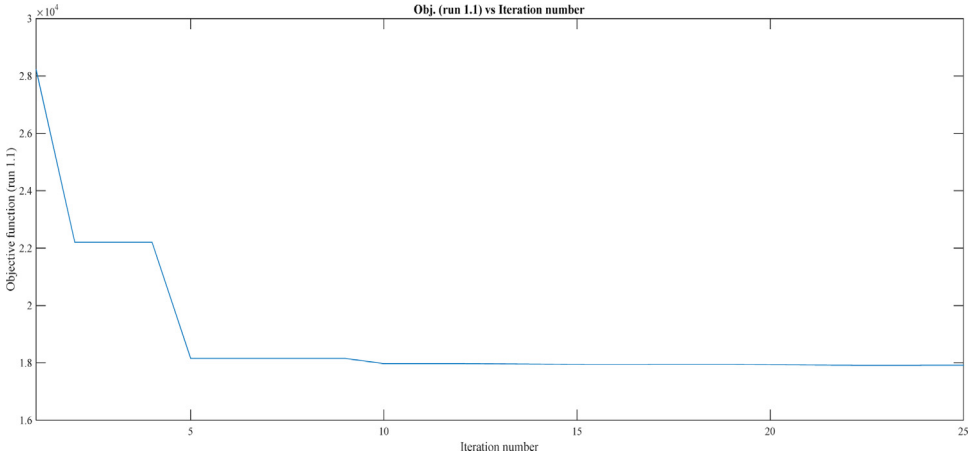

Fig. 12. The convergence behavior of run 1.1 in Example 1.

It can be observed from these results that the objective value can be reduced by relaxing budget constraint. However, this value tends to reach a constant as the upper limit exceeds a threshold. This is due to the fact that, although the expected loss caused by FD failures can be lowered by adding redundant components and shorting the inspection intervals, additional loss from FS failures and also extra capital costs should also incur due to such a practice as well. Although the run time increases as the budget constraint tightens, it can be observed from the typical convergence behavior in run 1.1 (see Fig. 12) that the optimum can be reached quickly (only 10 iterations in this case).

6. Additional examples

Three additional examples are presented in the sequel to demonstrate the capabilities of GA-based generic optimization method. The first example is concerned with a single-layer multi-channel safety interlock installed on a refrigeration unit, the second is a fire extinguisher of similar structure but maintained with a slightly modified maintenance scheme, and the third is a multilayer multichannel interlock used to protect the CSTR given in Fig. 7. All examples were solved in the MATLAB 2015a environment on a Pentium 4 3.00 GHz PC.

6.1. Example 2

Let us consider the refrigeration unit shown in Fig. 13 (Liptak, 1987). A high degree of operational safety can be achieved in this system with a variety of different interlocks. One of them stops the compressor if any of the following six conditions occurs while the compressor is running: (1) chilled water flow rate is low, as measured by FSL-3; (2) compressor discharge pressure (and, therefore, pressure in the condenser) is high, as indicated by PSH-4; (3) evaporator temperature has dropped near the freezing point, as detected by TSL-7; (4) refrigerated water temperature is dangerously low, approaching freezing, as sensed by TSL-6; (5) temperature of motor bearing or winding is high, as detected by TSH-5; (6) lubricating oil pressure is low (not shown in Fig. 13). It is assumed that at least one of the two power switches must function to shutdown the compressor. The proposed optimization strategies were applied to this interlocking system with the assumed parameters in Tables 4 and 5.

It is also assumed that the system's operating life (H) is 5 years and the time-averaged probability of an unsafe state (p) in each year is constant at 0.1. At an interest rate (ir) of 3% per year, the life-cycle cost parameters adopted for the FS and FD failures are $LCC_a = 4.7171 \times 10^4$ USD and $LCC_a = 4.7171 \times 10^7$ USD respectively.

Since there are six measurement channels in this example, the alarm logic can be specified with 62 ($= 2^6 - 2$) binary digits. Let us assume that there can be at most 7 online level sensors (3 binary digits) and 7 spares (3 binary digits) in each channel. Thus, additional 3 digits must also be allocated in the chromosome to represent the voting gate in each measurement channel. On the other hand, it is assumed

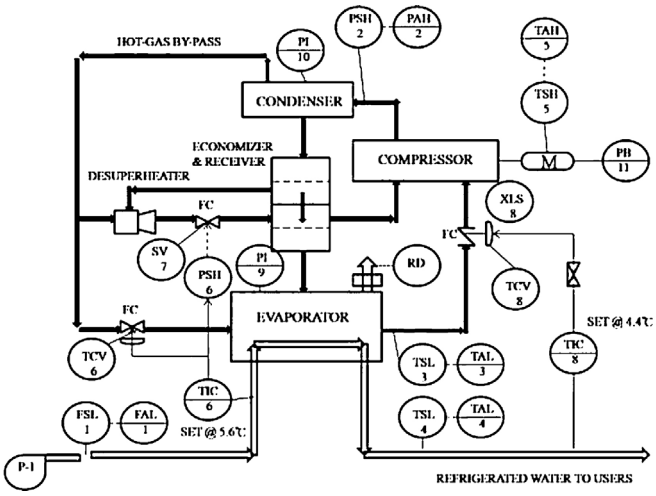

Fig. 13. Piping and instrumentation diagram (P&ID) of a typical refrigeration unit.

Table 4
Maintenance and cost parameters of sensors in refrigeration system.

Channels	FSL-3 1	PSH-4 2	TSL-7 3	TSL-6 4	TSH-5 5	Lube oil pressure 6
λ_i (yr^{-1})	1.8	2.5	1.5	0.3	2	1.6
μ_i (yr^{-1})	3.5	3	3	3	4	3
ε_i (yr^{-1})	365	365	365	365	365	365
α_i (yr^{-1})	0.1	0.1	0.1	0.1	0.1	0.1
PCS_i (USD)	80	100	100	250	60	90
$RprsC_i$ (USD)	7	10	10	20	5	15
$RplsC_i$ (USD)	5	10	5	10	5	5

Table 5
Maintenance and cost parameters of actuators in refrigeration system.

Channels	Power switch 1	Power switch 2
λ_j (yr^{-1})	1.2	0.4
μ_j (yr^{-1})	2.8	3.6
α_j (yr^{-1})	0.1	0.1
PCV_j (USD)	130	200
$InspC_j$ (USD)	15	15
$RprsC_j$ (USD)	50	70

that there are two shutdown channels and, in each channel, at most seven online solenoid valves (3 binary digits) and seven standbys (3 binary digits) are available, and the maximum length of inspection period is 15 months (4 binary digits).

Based on the above specifications, one can deduce that the total length of the chromosome should be 136 digits. To facilitate implementation of genetic algorithm, N_{pop} is set at 180 and the mating rate, mutation rate and selection rate are chosen to be 0.90, 0.10 and 0.5, respectively. Five optimization runs have been performed according to different levels of budget constraint, and the corresponding results are given in Tables 6 and 7. From these results, one can see that the objective value can also be reduced by relaxing the budget constraint. If we want to reduce the total expected loss, increasing the total life-cycle costs of both shutdown and alarm subsystems is needed (see run 2.4 and run 2.5). However, at certain point the decrease in total life-cycle expenditure stabilizes as the upper budget limit exceeds a threshold (see run 2.1 and run 2.2). It can also be observed that a reduction in the number of channels from 6 (run 2.3) to 4 (run 2.6) results in an increase in the total expected life-cycle expenditure. Thus, it is clear that more the diversified channels in the former case facilitate better flexibility in design and, thus, a higher degree of interlock reliability.

6.2. Example 3

Let us next consider a simplified version of the fire extinguishing system located in a production room (see Fig. 14). There are three measurement "channels" respectively equipped with (1) the smoke detectors, (2) the temperature sensors, and (3) the human operators. It is assumed that only one operator works on the field with at least one back-up worker staying in the control room. Since none of the smoke-detector failures in the first channel are observable, a preventive maintenance strategy should be adopted to enhance availability. When computing the conditional probabilities of FS and FD failures of the first measurement channel with Eqs. (B4) and (B5) in Appendix B, it is necessary to follow the procedure described in Section 3.2 (instead of Section 3.1).

On the other hand, the sprinklers placed at two separate locations are treated as two distinct channels of the shutdown subsystem. It is assumed that at least one of the two channels must function properly to put out the fire.

Again we assumed that the system's operating life (H) is 5 years and the time-averaged probability of an unsafe state (p) in each year is constant at 0.15. At an interest rate (ir) of 3% per year, the life-cycle cost parameters adopted for the FS and FD failures are $LCC_a = 4.7171 \times 10^4$

Table 6
Optimization results of Example 2.

	Run no.					
	2.1	2.2	2.3	2.4	2.5	2.6
Costs						
Objective function (USD)	26,513.8	26,513.8	32,651.8	42,246.5	45,149.5	34,157.5
Budget limit (USD)	12,000	10,000	9000	8500	8000	9000
Total expected lost (USD)	16,802.2	16,802.2	23,652.1	34,033.5	37,183.5	25,357.3
C_{AL}^{LC} (USD)	5527.9	5527.9	3690.4	3860.2	3804.9	4469.9
C_{SD}^{LC} (USD)	4178.7	4178.7	5308.3	4352.8	4161.1	4380.3
Alarm channels						
(a) FSL-3						
Number of online sensors/spares	4/2	4/2	2/4	1/3	1/3	5/2
Voting gate	4oo4	4oo4	2oo2	1oo1	1oo1	4oo5
(b) PSH-4						
Number of online sensors/spares	7/2	7/2	6/1	1/7	3/1	3/4
Voting gate	7oo7	7oo7	6oo6	1oo1	3oo3	3oo3
(c) TSL-7						
Number of online sensors/spares	1/4	1/4	1/6	3/1	6/4	2/6
Voting gate	1oo1	1oo1	1oo1	3oo3	6oo6	2oo2
(d) TSL-6						
Number of online sensors/spares	1/2	1/2	4/2	2/2	1/3	2/5
Voting gate	1oo1	1oo1	1oo2	2oo2	3oo3	2oo2
(e) TSH-5						
Number of online sensors/spares	1/6	1/6	1/4	3/1	4/2	-
Voting gate	1oo1	1oo1	1oo1	3oo3	1oo4	-
(f) Lube oil pressure						
Number of online sensors/spares	2/2	2/2	7/1	3/4	1/3	-
Voting gate	2oo2	2oo2	7oo7	3oo3	1oo1	-
Shutdown channels						
(a) Power switch 1						
Number of online units/standby units	2/4	2/4	4/3	6/2	4/4	4/3
Inspection interval of power switch (months)	7	7	7	4	14	6
(b) Power switch 2						
Number of online units/standby units	2/7	2/7	2/2	1/1	1/2	4/1
Inspection interval of power switch (months)	8	8	8	13	4	4
Run time (s)	163	163	175	285	402	120

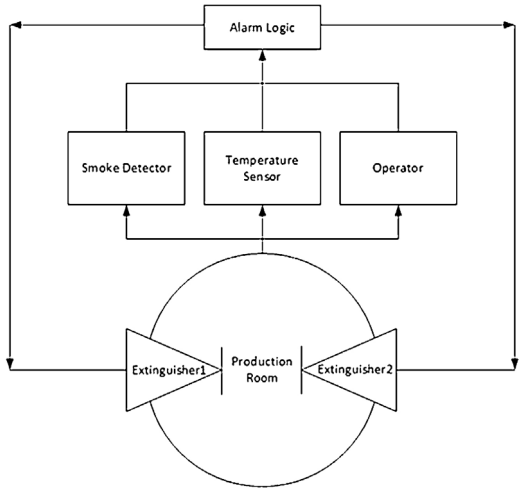

Fig. 14. Fire extinguishing system in Example 3.

USD and $LCC_b = 4.7171 \times 10^7$ USD respectively. Since there are three measurement channels in this example, the alarm logic can be described with 6 ($=2^3-2$) binary digits. Let us assume that there can be at most 7 online level sensors (3 binary digits) and 7 spares (3 binary digits) on each channel. Thus, additional 3 digits on each channel must also be allocated in the chromosome to represent the corresponding voting gate. The maintenance and cost parameters of the sensors are listed in Table 8.

On the other hand, it is again assumed that there are two shutdown channels and at most seven solenoid valves in each channel (3 binary digits), the maximum number of spares is seven (3 binary digits), and the maximum length of inspection period is 15 months (4 binary digits). The maintenance and cost parameters of the shutdown channels are listed in Table 9.

From the above specifications, one can deduce that the length of a chromosome should be 53 digits. To facilitate implementation of genetic algorithm, N_{pop} is also fixed at 180 and the same mating rate, mutation rate and selection rate are used, i.e., they are set to be 0.90, 0.10 and 0.5, respectively. Six optimization runs have been performed according to different levels of budget constraint, and the

Table 7
The optimal alarm functions in Example 2.

y_1	y_2	y_3	y_4	y_5	y_6	Logics $f(\mathbf{y})$ Run no.						y_1	y_2	y_3	y_4	y_5	y_6	Logics $f(\mathbf{y})$ Run no.					
						2.1	2.2	2.3	2.4	2.5	2.6							2.1	2.2	2.3	2.4	2.5	2.6
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	–
1	0	0	0	0	0	0	0	1	0	1	1	1	0	0	0	0	1	0	0	1	0	1	–
0	1	0	0	0	0	1	1	1	0	1	1	0	1	0	0	0	1	1	1	1	0	1	–
1	1	0	0	0	0	1	1	1	0	1	1	1	1	0	0	0	1	1	1	1	0	1	–
0	0	1	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	0	0	0	0	0	–
1	0	1	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1	1	1	1	0	0	–
0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	0	0	1	0	0	0	0	0	–
1	1	1	0	0	0	1	1	1	0	0	1	1	1	1	0	0	1	0	0	1	1	1	–
0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	1	0	1	1	–
1	0	0	1	0	0	1	1	1	0	1	1	1	0	0	1	0	1	1	1	1	1	1	–
0	1	0	1	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	–
1	1	0	1	0	0	1	1	1	0	0	1	1	1	0	1	0	1	1	1	0	1	1	–
0	0	1	1	0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1	1	1	0	–
1	0	1	1	0	0	1	1	1	0	0	1	1	0	1	1	0	1	1	1	1	1	1	–
0	1	1	1	0	0	1	1	1	0	1	1	0	1	1	1	0	1	1	1	0	1	0	–
1	1	1	1	0	0	1	1	1	1	0	1	1	1	1	1	0	1	1	1	1	1	1	–
0	0	0	0	1	0	0	0	1	0	1	–	0	0	0	0	1	1	1	1	1	0	1	–
1	0	0	0	1	0	1	1	0	1	1	–	1	0	0	0	1	1	1	1	0	1	1	–
0	1	0	0	1	0	1	1	0	1	0	–	0	1	0	0	1	1	1	1	1	1	1	–
1	1	0	0	1	0	1	1	0	1	0	–	1	1	0	0	1	1	1	1	1	1	1	–
0	0	1	0	1	0	1	1	0	0	1	–	0	0	1	0	1	1	1	1	1	1	1	–
1	0	1	0	1	0	1	1	1	0	1	–	1	0	1	0	1	1	1	1	1	0	1	–
0	1	1	0	1	0	1	1	0	0	1	–	0	1	1	0	1	1	1	1	1	1	0	–
1	1	1	0	1	0	1	1	1	1	1	–	1	1	1	0	1	1	0	0	0	0	1	–
0	0	0	1	1	0	1	1	1	1	0	–	0	0	0	1	1	1	1	1	0	1	1	–
1	0	0	1	1	0	1	1	1	1	1	–	1	0	0	1	1	1	1	1	1	1	1	–
0	1	0	1	1	0	1	1	1	1	1	–	0	1	0	1	1	1	1	1	1	1	1	–
1	1	0	1	1	0	1	1	0	1	0	–	1	1	0	1	1	1	1	1	1	1	1	–
0	0	1	1	1	0	1	1	1	0	1	–	0	0	1	1	1	1	1	1	1	1	1	–
1	0	1	1	1	0	1	1	1	1	1	–	1	0	1	1	1	1	1	1	1	0	1	–
0	1	1	1	1	0	1	1	1	1	1	–	0	1	1	1	1	1	1	1	1	1	0	–
1	1	1	1	1	0	1	1	1	1	1	–	1	1	1	1	1	1	1	1	1	1	1	–

Table 8
Maintenance and cost parameters of sensors in Example 3.

Subsystem	Smoke detector	Temperature	Operator
λ_i (yr^{-1})	1.7	0.35	0.25
μ_i (yr^{-1})	60	10	43
ε_i (yr^{-1})	365	365	365
α_i (yr^{-1})	0.15	0.1	0.1
PCS_i (USD)	80	130	500
$RprsC_i$ (USD)	35	45	45
$RplsC_i$ (USD)	20	40	0

Table 9
Maintenance and cost parameters of actuators in Example 3.

Channels	Extinguisher 1	Extinguisher 2
λ_j (yr^{-1})	1.2	3.2
μ_j (yr^{-1})	12	10
α_j (yr^{-1})	0.1	0.1
PCV_j (USD)	350	300
$RprlC_j$ (USD)	130	110
$InspC_j$ (USD)	90	90

corresponding results are given in Tables 10 and 11. As we can see from these results, the expected loss from the FD and FS failures decreases as the budget limit increases and, also, spending on the shutdown subsystem is higher than that of the alarm subsystem. This is due to the fact that, in this example, the failure rates of the actuators are in general higher than those of the sensors. Thus, to reduce the expected loss caused by the FD failures, higher spending in shutdown units is needed. Notice also that the temperature sensors in the optimal designs are always fewer than the smoke detectors. This is due to the fact that, although less reliable, the smoke detector is cheaper. Finally, it can be observed that that the total number of sprinklers used for in channel 1 is larger than that for channel 2. This may be due to the facts that, although the sprinklers in channel 1 are slightly more expensive, they are much more reliable.

Table 10
Optimization results of Example 3.

	Run no.					
	3.1	3.2	3.3	3.4	3.5	3.6
Costs						
Objective function (USD)	45,257.9	46,588.8	51,083.4	77,641.4	129,955	171,832.7
Budget limit (USD)	28,000	24,000	20,000	17,000	16,000	15,000
Total expected lost (USD)	22,832.8	24,220.8	31,112.4	60,795.3	114,367.5	157,372
$C^{LC}_{SD,\ extinguisher\ 1,\ extinguisher\ 2}$ (USD)	17,819.6	16,820.8	16,194.8	13,205	11,537.6	10,142
$C^{LC}_{AL,\ smokedetector,\ temperature,\ operator}$ (USD)	4605.5	5547.2	3776.2	3641.1	4049.9	4318.7
Alarm channels						
(a) Smoke detector						
Number of online sensors/spares	6/3	6/4	5/1	7/2	6/1	6/5
Voting gate	6oo6	4oo4	2oo2	1oo1	1oo1	4oo5
(b) Temperature						
Number of online sensors/spares	3/2	4/2	1/4	1/2	1/4	1/1
Voting gate	3oo3	4oo4	1oo1	1oo1	1oo1	1oo1
(c) Operator						
Number of online sensors/spares	1	1	1	1	1	1
Voting gate	1	1	1	1	1	1
Shutdown channels						
(a) Power switch 1						
Number of online units/standby units	4/5	6/5	5/6	5/6	4/3	7/3
Inspection interval of power switch (months)	3	4	5	8	8	10
(b) Power switch 2						
Number of online units/standby units	1/1	2/4	4/3	2/1	2/4	1/1
Inspection interval of power switch (months)	8	15	13	9	13	13
Run time (s)	14	15	18	21	24	77

Table 11
The optimal alarm logics obtained in Example 3.

Smoke y_1	Temperature y_2	Operator y_3	Logics $f(\mathbf{y})$ Run no.					
			3.1	3.2	3.3	3.4	3.5	3.6
0	0	0	0	0	0	0	0	0
1	0	0	0	0	1	0	1	0
0	1	0	0	0	0	0	1	1
1	1	0	1	1	1	1	1	1
0	0	1	0	0	0	0	0	1
0	1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1

Table 12
Maintenance and cost parameters of sensors in scenario 1 of Example 4.

Subsystem	Temperature Interlock	Pressure relief
λ_i (yr^{-1})	0.2	0.1
μ_i (yr^{-1})	0.9	0.95
ε_i (yr^{-1})	50	50
α_i (yr^{-1})	0.1	0.05
PCS_i (USD)	200	250
$RprsC_i$ (USD)	35.7	44.7
$RplsC_i$ (USD)	17.9	22.3

6.3. Example 4

In this last example, two separate scenarios are considered. Firstly, the CSTR presented in Fig. 7 is simplified and treated as a two-layer interlock triggered by temperature and pressure respectively. It is again assumed that the system operating life (H) is 5 years and the probability of an abnormally high temperature (p^T) in each year is 0.2 with an interest rate (ir) of 6% per year, the life-cycle cost parameters adopted for the FS and FD failures of the temperature-interlock and pressure relief systems.

$$LCC_a^{(1)} = 4.4651 \times 10^4\ \text{USD}; \quad LCC_a^{(2)} = 1.3395 \times 10^5\ \text{USD}; \quad LCC_b = 4.4651 \times 10^8\ \text{USD}$$

Let us also assume that there are at most seven online sensors (3 binary digits) and 15 spares (4 binary digits) in each measurement channel. Thus, the corresponding voting gate requires 3 binary digits. The maximum number of solenoid valves in every protection layer is set to be 3 (2 binary digits) and the maximum number of spares 15 (4 binary digits), while the maximum inspection interval is 15 (4 binary digits). Based on the above specifications, one can deduce that the size of chromosome is 40 digits for the 2-layer system. The cost and maintenance parameters of the sensors and actuators can be found in Tables 12 and 13. To facilitate the implementation of GA, all algorithmic parameters used in Example 3 are also adopted in the present example. Six optimization runs, i.e., runs 4-1.1 to 4-1.6 in

Table 13
Maintenance and cost parameters of actuators in scenario 1 of Example 4.

Subsystem	Temperature interlock	Pressure relief
λ_j (yr^{-1})	0.25	0.3
α_j (yr^{-1})	0.05	0.08
PCV_j (USD)	400	250
$RprlC_j$ (USD)	89.3	71.4
$InspC_j$ (USD)	535.8	334.9

Table 14
Optimization results of Example 4 – scenario 1: 2 protection layers.

	Run no.					
	4-1.1	4-1.2	4-1.3	4-1.4	4-1.5	4-1.6
Costs						
Objective function (USD)	36,292	36,621.6	38,621.6	40,633.1	41,640.6	48,820.1
Budget limit (USD)	15,000	11,000	10,000	9000	8000	7000
Total expected lost (USD)	25,326.6	25,665.9	28,687.1	31,651.8	33,672.4	42,020.3
C_{AL}^{LC} (USD)	6462.5	6300.6	7276	6065.1	6138.7	5404.6
C_{SD}^{LC} (USD)	4502.9	4655.1	2858.5	2916.2	1829.5	1395.2
(a) Temperature interlock system design						
Number of online sensors/spares	3/11	2/8	1/3	1/5	1/4	1/3
Voting gate	2oo3	1oo2	1oo1	1oo1	1oo1	1oo1
Number of solenoid valves/standbys	3/15	3/15	3/15	3/15	3/15	3/15
Inspection interval of solenoid valves	12	9	9	12	12	12
(b) Pressure-relief system design						
Number of online sensors/spares	2/4	2/8	2/5	5/1	1/2	1/1
Voting gate	2oo2	2oo2	2oo2	2oo5	1oo1	1oo1
Number of solenoid valves/standbys	2/15	2/15	2/15	3/15	2/15	3/15
Inspection interval of solenoid valves	8	12	8	10	9	15
Run time (s)	59	63	88	145	151	250

Table 14, have been performed for different levels of budget constraint. It can also be observed that the objective value increases as the budget decreases.

The second scenario considered in this example is the entire three-layer interlock on the CSTR in Fig. 7. The maintenance and cost data of the alarm subsystem in the first-layer flow interlock are given below:

$$\lambda_i = 1.8\,\mathrm{yr}^{-1};\quad \mu_i = 3.5\,\mathrm{yr}^{-1};\quad \varepsilon_i = 365\,\mathrm{yr}^{-1};\quad a_i = 0.1;\quad PCS_i = 80\,\mathrm{USD};\quad \overline{RprsC_i} = 7\,\mathrm{USD};\quad \overline{RplsC_i} = 8\,\mathrm{USD}$$

The corresponding assumptions on the maximum online sensors and spares in flow interlock with its voting gate are the same as those in the previous scenario. The life-cycle cost parameter for the FS failures is chosen to be $LCC_a^{(1)} = 2.34651 \times 10^4$ USD. Finally, the

Table 15
Optimization results of Example 4 – scenario 2: 3 protection layers.

	Run no.					
	4-2.1	4-2.2	4-2.3	4-2.4	4-2.5	4-2.6
Costs						
Objective function (USD)	24,861.9	24,861.9	25,790.2	26,447.3	26,478	27,177.5
Budget limit (USD)	15,000	14,000	13,000	12,000	11,000	10,000
Total expected lost (USD)	14,237.3	14,237.3	15,254.8	16,114.6	16,116.6	17,181.5
C_{AL}^{LC} (USD)	6876.9	6876.9	7286.4	7351	7017.1	6935.1
C_{SD}^{LC} (USD)	3747.7	3747.7	3249	2980.3	3343.9	3060.8
(a) Flow interlock system design						
Number of online sensors/spares	1/8	1/8	1/7	1/8	1/7	1/8
Voting gate	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1
Number of solenoid valves/standbys	3/14	3/15	3/13	3/15	3/15	3/13
Inspection interval of solenoid valves	15	15	15	12	12	12
(b) Temperature interlock system design						
Number of online sensors/spares	2/8	2/8	1/6	2/3	2/4	1/2
Voting gate	2oo2	2oo2	1oo1	2oo2	2oo2	1oo1
Number of solenoid valves/standbys	3/10	3/10	3/14	2/12	2/9	2/13
Inspection interval of solenoid valves	12	12	10	12	12	15
(c) Pressure-relief system design						
Number of online sensors/spares	2/1	2/1	2/2	2/2	2/3	3/3
Voting gate	2oo2	2oo2	2oo2	2oo2	2oo2	3oo3
Number of solenoid valves/standbys	1/11	1/11	1/3	2/15	2/11	2/10
Inspection interval of solenoid valves	15	15	14	12	15	12
Run time (s)	14	14	20	28	34	41

last assumption given for the maximum number of solenoid valves with its standby units and the maximum inspection intervals of the shutdown units are the same with the previous case. The size of the chromosome is 60 digits.

The maintenance and cost parameters of the actuators in the flow interlock are:

$$\lambda_i = 0.6\,\mathrm{yr}^{-1};\quad a_i = 0.1;\quad PCV_j = 300\,\mathrm{USD};\quad \overline{InsPC_j} = 64.1\,\mathrm{USD};\quad \overline{RprlC_j} = 349.8\,\mathrm{USD}.$$

Six optimization runs, i.e., runs 4-2.1 to 4-2.6 in Table 15, have been performed for different levels of budget constraint. Similar to the previous case, raising the budget limit can also reduce the total expected lost. If we compare the optimization results of three-layer system (run 4-2.1, 4-2.5, and 4-2.6) with those of the double-layer system (run 4-1.1, 4-1.2, and 4-2.3), one can see that adding another layer under the same budget constraint drives the total expected loss to almost one half of the original level. This is because the additional protection layer could reduce probability of FS failures significantly. Notice that, based on Eq. (65), the FD probability of the entire system equals the product of all single-layer FD probabilities, the 3-layer configuration naturally outperforms the 2-layer counterpart.

7. Conclusions

In this study, we have developed a generic GA-based MATLAB code to identify the optimal configurations of multilayer multichannel protective systems and the corresponding maintenance programs. Any interlock design problem can be solved with the same general code without constructing a new computer program. The maintainability of this code is ensured by its modularity, and this benefit has been clearly demonstrated in Example 3.

Based on the optimization results obtained in case studies, the following conclusions can be drawn:

1. The reliabilities of sensors and actuators, their purchase and maintenance costs and the financial implications of FD and FS failures obviously dictate the optimal interlock configurations and maintenance strategies.
2. Under a given budget constraint, it is beneficial to introduce as many protection layers as possible.
3. Increasing measurement/shutdown channels provides design flexibility for enhancing interlock reliability.
4. The run time increases as the budget tightens.

Acknowledgement

This work is supported by the Ministry of Science and Technology of the ROC government under grant NSC 102-2221-E-006-255-MY3.

Appendix A. Time-dependent state probabilities under preventive maintenance program

For illustration convenience let us also use the following recurrence formulas to construct a series of constants:

$$\Theta_{(1,k)} = k;\quad k = 1, 2, \ldots, n. \tag{A1}$$

$$\Theta_{(i+1,j)} = \sum_{k=1}^{j} \Theta_{(i,k)};\quad i = 1, 2, \ldots, (n-1),\quad j = 1, 2, \ldots, (n-i). \tag{A2}$$

Let us then introduce separate time scales for the individual intervals respectively, i.e., $\tau = t - I \times T$, to transform any interval $I \times T < t < (I+1) \times T$ to the same one, i.e., $0 < \tau < T$. Based on the above definitions, the analytic solution of Eqs. (22)–(30) can be expressed in general form as follows:

- Blocks 1 and 4

$$P_k(\tau) = \Theta_{(n-k+1,k)} \left[\sum_{i=1}^{m-n} \sum_{j=0}^{k-1} K_i^I (-1)^j \binom{k-1}{j} e^{-(r+j)\lambda\tau} - \sum_{i=2}^{m-n} \sum_{j=0}^{k-1} \sum_{g=0}^{i-2} K_i^I (-1)^j \binom{k-1}{j} \frac{(\mu\tau)^g}{g!} e^{-[(r+j)\lambda+\mu]\tau} \right]$$
$$+ \sum_{i=1}^{k} \sum_{j=0}^{i-1} \sum_{g=0}^{m-n-1} \Theta_{(r,i)} K_{m-n+1+k-i}^I (-1)^j \binom{i-1}{j} \left(e^{-(r+j)\lambda\tau} - \frac{(\mu\tau)^g}{g!} e^{-[(r+j)\lambda+\mu]\tau} \right);\quad r = n-k+1;\quad k = 1, 2, \ldots, n. \tag{A3}$$

- Blocks 2 and 5

$$P_k(\tau) = \Theta_{(m-n+1-y,y)} \sum_{i=1}^{f} \sum_{j=0}^{y-1} K_{(m-n)-(f-i)}^I (-1)^j \binom{y-1}{j} \frac{(\mu\tau)^{i-1}}{(i-1)!} e^{-[(g+j)\lambda+\mu]\tau} - \frac{(\mu\tau)^f}{f!} \sum_{i=1}^{y} \sum_{j=0}^{i-1} \Theta_{(g,i)} K_{m-n+1+y-i}^I (-1)^j$$
$$\times \binom{i-1}{j} e^{-[(g+j)\lambda+\mu]\tau};\quad k = x(n+1)+y;\ f = m-n-x;\ g = n-y+1;\ x = 1, 2, \ldots, (m-n-1);\ y = 1, 2, \ldots, n. \tag{A4}$$

- Blocks 3 and 6

$$P_k(\tau) = \sum_{i=0}^{n-r} \sum_{j=0}^{i} \Theta_{(r,i+1)} K_{m+1-r-i}^I (-1)^j \binom{i}{j} e^{-[(r+j)\lambda+\mu]\tau};\ k = x + (m-n)(n+1);\ r = (m-n+1)(n+1) - k;\ x = 1, 2, \ldots, n. \tag{A5}$$

• Blocks 7 and 8

$$P_k(\tau) = \sum_{i=0}^{c}\sum_{j=0}^{n} K^I_{(m-n+1)-i}(-1)^j \binom{n}{j} \frac{(\mu\tau)^{c-i}}{(c-i)!} e^{-(j\lambda+\mu)\tau} + \sum_{i=1}^{n}\sum_{j=0}^{n-i} K^I_{(m-n+1)+i}(-1)^j \times \binom{n-i}{j} \frac{(\mu\tau)^{c}}{c!} e^{-(j\lambda+\mu)\tau}; \quad k=(x+1)(n+1); \quad c=m-n-x; \quad x=1,2,\ldots,(m-n). \tag{A6}$$

Appendix B. Expected life-cycle loss for a single protection layer

A constant p is used to denote the time-averaged probability if an unsafe process state occurred during the operation of the protective system in a year and it can be expressed as:

$$p = Pr\{\xi = 1\} \tag{B1}$$

Also, symbols A_i and B_i are used, respectively, to represent the conditional probabilities of FS and FD failures of the ith measurement channel, i.e.

$$A_i = Pr\{y_i = 1 \,|\, \xi = 0\} \tag{B2}$$

$$B_i = Pr\{y_i = 0 \,|\, \xi = 1\} \tag{B3}$$

If a k_i-out-of-n_i voting gate is used to trigger the alarm, the FS probability of the ith measurement channel can be expressed as

$$A_i = 1 - (1-\alpha_i^{k_i})\frac{n_i!}{k_i!(n_i-k_i)!} \tag{B4}$$

where α_i is a constant representing the FS probability of an online sensor in the ith channel. On the other hand, the value of the FD probability of the ith measurement channel should be approximated as

$$B_i = 1 - \overline{Av_i}^{Corr} \tag{B5}$$

where $\overline{Av_i}^{Corr}$ is the average availability of the ith measurement channel.

Let us assume that the failure rates, repair rates and replacement rates of sensors are given a priori. All other model parameters needed for calculating A_i and B_i can be extracted from the chromosomes described in Section 4.1. Henley and Kumamoto (1981, 1985) and Sasaki et al. (1977) suggested that the conditional probabilities of the FS and FD failures of the alarm subsystem can be written, respectively, as:

$$P_{FS}^{AL} = Pr\{f(\mathbf{y}) = 1 \,|\, \xi = 0\} = \sum_{y} f(\mathbf{y}) Pr\{\mathbf{y} \,|\, \xi = 0\} \tag{B6}$$

$$P_{FD}^{AL} = Pr\{f(\mathbf{y}) = 0 \,|\, \xi = 1\} = \sum_{y} [1 - f(\mathbf{y})] Pr\{\mathbf{y} \,|\, \xi = 1\} \tag{B7}$$

If the outputs of the alarm channels are statistically independent, the conditional probabilities $Pr\{\mathbf{y} \,|\, \xi = 0\}$ and $Pr\{\mathbf{y} \,|\, \xi = 1\}$ can be written as functions of A_i and B_i, that is

$$Pr\{\mathbf{y} \,|\, \xi = 0\} = \prod_{i=1}^{M} Pr\{y_i \,|\, \xi = 0\} = \prod_{i=1}^{M} [A_i^{y_i}(1-A_i)^{1-y_i}] \tag{B8}$$

$$Pr\{\mathbf{y} \,|\, \xi = 1\} = \prod_{i=1}^{M} Pr\{y_i \,|\, \xi = 1\} = \prod_{i=1}^{M} [B_i^{1-y_i}(1-B_i)^{y_i}] \tag{B9}$$

On the other hand, because usually either OR or AND logics are embedded in the shutdown configuration, the corresponding conditional probabilities of FS and FD failures can be expressed respectively as follows:

• OR

$$P_{FS}^{SD} = Pr\{h(\mathbf{z}) = 1 \,|\, f(y) = 0\} = 1 - \prod_{j=1}^{K} (1 - ASD_j) \tag{B10}$$

$$P_{FD}^{SD} = Pr\{h(\mathbf{z}) = 0 \,|\, f(\mathbf{y}) = 1\} = \prod_{j=1}^{K} BSD_j \tag{B11}$$

• AND

$$P_{FS}^{SD} = Pr\{h(\mathbf{z}) = 1 \,|\, f(\mathbf{y}) = 0\} = \prod_{j=1}^{K} ASD_j \tag{B12}$$

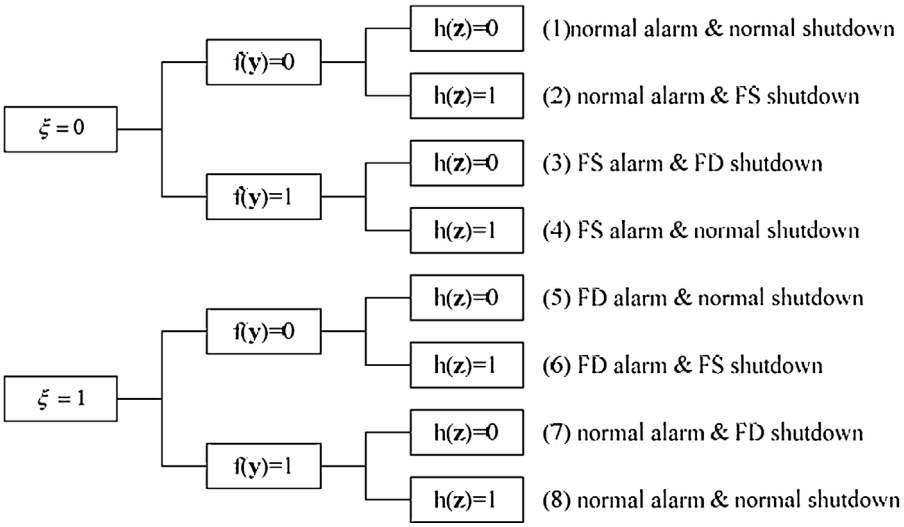

Fig. B1. All possible scenarios of a single-layer protective system.

$$P_{FD}^{SD} = Pr\{h(\mathbf{z}) = 0 \,|\, f(\mathbf{y}) = 1\} = 1 - \prod_{j=1}^{K}(1 - BSD_j) \tag{B13}$$

By assuming a 1-out-of-L_j logic at the jth shutdown channel, the conditional probability of FS failure can be determined as

$$ASD_j = 1 - (1 - a_j)^{L_j} \tag{B14}$$

where a_j is a constant representing the FS probability of an actuator in channel j. On the other hand the value of BSD_j is determined according to

$$BSD_j = 1 - \overline{Av}_j^{Prev} \tag{B15}$$

Let us next enumerate all possible FS and FD scenarios in a single protective layer (see Fig. B1). In particular, scenarios 2 and 4 should be classified as FS system failures, whereas scenarios 5 and 7 FD failures. The probabilities that both alarm subsystem and shutdown subsystem fail simultaneously (i.e., scenarios 3 and 6) are assumed to have low possibilities and thus ignored. Consequently, the life-cycle expected loss due to these FS and FD failures can be expressed according to Henley and Kumamoto (1981, 1985) as

$$L_1^{LC} = CFS_{LC}[C_a(1-p)Pr\{FD_{sys}\} + C_b p Pr\{FS_{sys}\}] \tag{B16}$$

where C_a and C_b denote as financial losses incurred from the aforementioned FS and FD system failures. Since the given parameter p is assumed to be the time-averaged probability of unsafe process state in a single year, the multiplication factor CFS_{LC} is introduced in the above equation primarily to produce an estimate of the total expected loss over a multi-year horizon:

$$CFS_{LC} = \sum_{k=1}^{LC/12} \frac{1}{(1+ir)^{k-1}} \tag{B17}$$

where $LC/12 = 2, 3, \ldots$. Note that ir is the yearly interest rate in this formula while the conditional probabilities of the FS and FD system failures can be expressed as

$$Pr\{FS_{sys}\} = \sum_{y} Pr\{\mathbf{y} \,|\, \xi = 0\}\phi_a(\mathbf{y}) \tag{B18}$$

$$Pr\{FD_{sys}\} = \sum_{y} Pr\{\mathbf{y} \,|\, \xi = 1\}\phi_b(\mathbf{y}) \tag{B19}$$

where

$$\phi_a(\mathbf{y}) = (1 - P_{FD}^{SD})f(\mathbf{y}) + P_{FS}^{SD}[1 - f(\mathbf{y})] \tag{B20}$$

$$\phi_b(\mathbf{y}) = (1 - P_{FS}^{SD})[1 - f(\mathbf{y})] + P_{FD}^{SD} f(\mathbf{y}) \tag{B21}$$

By substituting the Eqs. (B20) and (B21) to Eqs. (B18) and (B19) and combining the results with Eqs. (B8) and (B9), one can obtain

$$Pr\{FS_{sys}\} = P_{FS}^{SD} + (1 - P_{FS}^{SD} - P_{FD}^{SD})\sum_{y} f(\mathbf{y}) Pr\{\mathbf{y} \,|\, \xi = 0\} = P_{FS}^{SD} + (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y_1, y_2, \ldots, y_M} \left\{ f(y_1, y_2, \ldots, y_M) \prod_{i=1}^{M} [A_i^{y_i}(1 - A_i)^{1-y_i}] \right\} \tag{B22}$$

$$Pr\{FD_{sys}\} = (1 - P_{FS}^{SD}) - (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y} f(\mathbf{y}) Pr\{\mathbf{y} \,|\, \xi = 1\}$$

$$= (1 - P_{FS}^{SD}) - (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y_1, y_2, \ldots, y_M} \left\{ f(y_1, y_2, \ldots, y_M) \prod_{i=1}^{M} [B_i^{1-y_i} (1 - B_i)^{y_i}] \right\} \tag{B23}$$

The following expression of the expected loss for operating a single-layer protective system can then be obtained

$$L_1^{LC} = \left[C_a (1-p) \left(P_{FS}^{SD} + (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y_1, y_2, \ldots, y_M} \left\{ f(y_1, y_2, \ldots, y_M) \prod_{i=1}^{M} [A_i^{y_i} (1 - A_i)^{1-y_i}] \right\} \right) \right.$$

$$\left. + C_b p \left((1 - P_{FS}^{SD}) - (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{y_1, y_2, \ldots, y_M} \left\{ f(y_1, y_2, \ldots, y_M) \prod_{i=1}^{M} [B_i^{1-y_i} (1 - B_i)^{y_i}] \right\} \right) \right] CFS_{LC} \tag{B24}$$

Appendix C. Supplementary data

Supplementary data associated with this article can be found, in the online version, at http://dx.doi.org/10.1016/j.compchemeng.2017.02.042.

References

Azaron, A., Perkgoz, C., Katagiri, H., Kato, K., Sakawa, M., 2009. Multi-objective reliability optimization for dissimilar-unit cold-standby systems using a genetic algorithm. Comput. Oper. Res. 36, 1562–1571.

Badía, F., Berrade, M., Campos, C.A., 2001. Optimization of inspection intervals based on cost. J. Appl. Probab. 38, 872–881.

Badía, F.G., Berrade, M.D., Campos, C.A., 2002. Optimal inspection and preventive maintenance of units with revealed and unrevealed failures. Reliab. Eng. Syst. Saf. 78, 157–163.

Dohi, T., Nakagawa, T., 2013. Stochastic Reliability and Maintenance Modeling: Essays in Honor of Professor Shunji Osaki on His 70th Birthday. Springer Science & Business Media.

Duarte, J.A.C., Craveiro, J.C.T.A., Trigo, T.P., 2006. Optimization of the preventive maintenance plan of a series components system. Int. J. Press. Vessels Pip. 83, 244–248.

Haupt, R.L., Haupt, S.E., 2004. Practical Genetic Algorithms. John Wiley & Sons.

Henley, E., Kumamoto, H., 1985. Designing for Reliability and Safety Control. Prentice-Hall, Englewood Cliffs, NJ.

Henley, E.J., Kumamoto, H., 1981. Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis. IEEE.

Hoyland, A., Rausand, M., 1994. System Reliability Theory: Models and Statistical Methods. John Wiley & Sons, New York, NY.

Kouedeu, A.F., Kenne, J.-P., Songmene, V., 2011. Production, Preventive and Corrective Maintenance Planning in Manufacturing Systems Under Imperfect Repairs., pp. 59–64.

Lai, C.-A., Chang, C.-T., Ko, C.-L., Chen, C.-L., 2003. Optimal sensor placement and maintenance strategies for mass-flow networks. Ind. Eng. Chem. Res. 42, 4366–4375.

Liang, K.-H., Chang, C.-T., 2008. A simultaneous optimization approach to generate design specifications and maintenance policies for the multilayer protective systems in chemical processes. Ind. Eng. Chem. Res. 47, 5543–5555.

Liao, Y.-C., Chang, C.-T., 2010. Design and maintenance of multichannel protective systems. Ind. Eng. Chem. Res. 49, 11421–11433.

Liptak, B.G., 1987. Optimization of Unit Operations. Chilton Book Company, Pennsylvania, US, pp. 227.

Mitchell, M., 1998. An Introduction to Genetic Algorithms. MIT Press.

Okasha, N.M., Frangopol, D.M., 2009. Lifetime-oriented multi-objective optimization of structural maintenance considering system reliability, redundancy and life-cycle cost using GA. Struct. Saf. 31, 460–474.

Sasaki, M., Kaburaki, S., Yanagi, S., 1977. System availability and optimum spare units. IEEE Trans. Reliab. R-26, 182–188.

Srivastava, V.K., Fahim, A., 2007. An optimization method for solving mixed discrete-continuous programming problems. Comput. Math. Appl. 53, 1481–1491.

Vaurio, J.K., 1995. Optimization of test and maintenance intervals based on risk and cost. Reliab. Eng. Syst. Saf. 49, 23–36.

Vaurio, J.K., 1999. Availability and cost functions for periodically inspected preventively maintained units. Reliab. Eng. Syst. Saf. 63, 133–140.

Wang, G.J., Zhang, Y.L., 2014. Geometric process model for a system with inspections and preventive repair. Comput. Ind. Eng. 75, 13–19.

Wang, Y., Pham, H., 2011. A multi-objective optimization of imperfect preventive maintenance policy for dependent competing risk systems with hidden failure. IEEE Trans. Reliab. 60, 770–781.

Wibisono, E., Adi, V.S.K., Chang, C.-T., 2014. Model based approach to identify optimal system structures and maintenance policies for safety interlocks with time-varying failure rates. Ind. Eng. Chem. Res. 53, 4398–4412.