A Simultaneous Optimization Approach To Generate Design Specifications and Maintenance Policies for the Multilayer Protective Systems in Chemical Processes

Kuo-Hwa Liang and Chuei-Tin Chang*

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

Generally speaking, a protective system is adopted to perform two basic functions, i.e., alarm and shutdown. The subsystem to perform the former function is equipped with one or more independent sensors. On the basis of the online measurements of these sensors, Boolean logic is applied to determine whether or not alarm signal(s) should be issued. The subsystem for the latter task is usually configured with solenoid valves. In response to the aforementioned signal(s), these valves are energized (or de-energized) to carry out the required shutdown operation. Since the hardware failures are basically random events, the reliability (or availability) of a protective system is highly dependent upon its structural characteristics and also maintenance policies. Traditionally, the alarm logic and shutdown configuration are synthesized according to experience and the maintenance scheme is also established on an ad hoc basis. The aim of this study is to develop an integrated mathematical programming model to minimize the total expected expenditure, i.e., the sum of the capital investments, the expected maintenance costs, and the expected losses due to system failures. From the optimal solution, one should be able to produce the design specifications for every protection layer, i.e., (1) the number of sensors and the corresponding alarm logic, (2) the number of valves and the corresponding shutdown configuration, and (3) the needed repair/replacement policies. In this work, the sensors and valves are assumed to be maintained respectively with the corrective and preventive strategies. Thus, the optimal number of spare sensors stored offline and the best inspection interval for each valve can also be determined by solving this model. Extensive case studies have been carried out to demonstrate the feasibility and effectiveness of the proposed approach.

1. Introduction

In order to mitigate the catastrophic effects caused by accidents in chemical plants, it is a common practice to install protective systems on the processing units operated under hazardous conditions. Generally speaking, a single-layer protective system can be divided into two parts, i.e., the alarm subsystem and the shutdown subsystem. The former is equipped with one or more independent sensors. Based on the online measurements of these sensors, a *predetermined* logic is followed to decide if the alarm signal(s) should be issued. The latter subsystem is usually configured with solenoid valves. In response to the aforementioned signal(s), these valves are energized (or de-energized) to carry out the shutdown operation. Since the inevitable failures of sensors and valves are basically random events, the reliability (or availability) of a protective system is highly dependent upon its structural characteristics and also the corresponding maintenance policies. Finally, it should be noted that, in certain applications, more than one protective system may be nested in multiple layers to reduce the probabilities of detrimental consequences to acceptable levels.

Traditionally, an ad hoc approach has been adopted to design and operate the interlocks and trips used in practical applications. In particular, the system structure and also the maintenance policy are first synthesized on the basis of past experience. The financial implications of having such a protective system in place, i.e., its capital costs, its expected losses due to equipment failures, and its expected maintenance expenditures for inspections, replacements and repairs, are then estimated accordingly. Since these design and evaluation procedures may have to be repeated a number of times on a trial-and-error basis so as to acquire a satisfactory solution, the aforementioned conventional approach can be very tedious and error prone. Thus, suitable computer-aided tools are clearly needed to streamline these procedures.

In fact, a wide variety of systematic risk assessment methods, e.g., fault tree analysis (FTA), event tree analysis (ETA), failure mode and effects analysis (FMEA), hazard and operability study (HAZOP), and layer of protection analysis (LOPA), etc., have already been developed to evaluate the reliability and/or availability of a *given* protective system. Green and Dowell III[1] applied a FTA-based computation procedure to determine the safety integrity level (SIL) of any protective system with given structure. In addition, these authors proposed several typical hardware configurations to satisfy different SIL specifications. On the basis of HAZOP results, Dowell III[2] later presented a design procedure to conjecture systems with more than one independent protection layer in order to reduce the overall risk of process hazards. Kohda and Nakagawa[3] also developed a calculation method on the basis of ETA to estimate the probability of a catastrophic event occurring under the protection of a multilayer interlock.

Due to the obvious need to fix design before applying the risk-evaluation methods, a review of the current approaches for designing the alarm and shutdown subsystems has also been performed in this study and a brief summary is presented below:

Notice first that the misjudgments made in alarm generation may either be spurious, i.e., the alarm fails safely (FS), or result in serious outcomes, i.e., the alarm fails dangerously (FD). The former failure is in general *recoverable* since it is caused mostly by noisy signals, while the latter may require repair or replacement. Obviously, both types of failures must be considered in formulating the alarm logic. A popular practice adopted in the chemical industries is to use multiple independent sensors

* To whom correspondence should be addressed. Tel.: 886-6-2757575 ext 62663. E-mail: ctchang@mail.ncku.edu.tw.

10.1021/ie071188z CCC: $40.75
Published on Web 06/25/2008

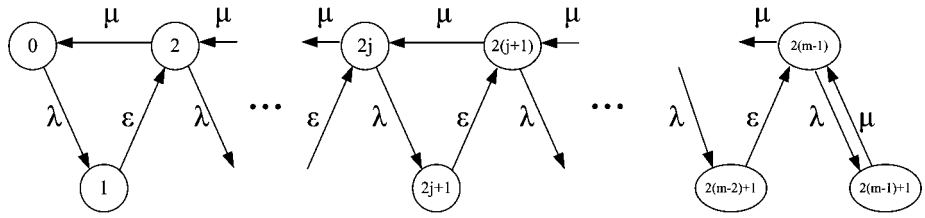

Figure 1. Markov diagram of a spare-supported corrective maintenance program.

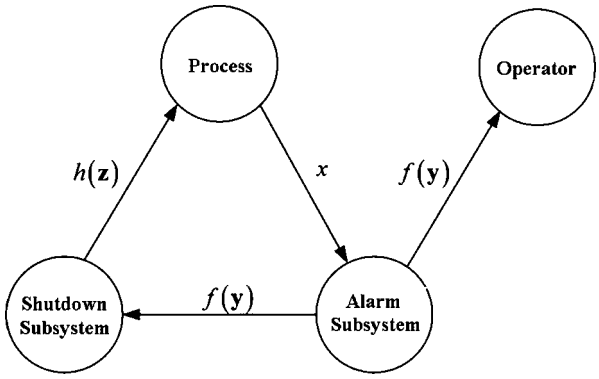

Figure 2. General structure of a protected process.

to monitor the same process condition and a voting device to determine whether or not an alarm should be set off. The objective of this approach is simply to reduce the chance of misjudgments by introducing hardware redundancy. To this end, Tsai and Chang[4] and Chang et al.[5] developed a statistics-based alarm strategy using the reconciled online process data. Another effective means of enhancing the system availability of a sensor network is maintenance. Lai et al.[6] introduced a corrective maintenance policy (with spares) into the system design procedure for improving the sensor availabilities and also the reliability of alarm generation.

On the other hand, notice that the solenoid valves in a shutdown subsystem may also experience FS and FD failures. Since the FD failures are not detectable during normal operations, a *preventive* maintenance strategy must be implemented. More specifically, all such components in a given system are required to be inspected regularly at constant time intervals to identify the *unrevealed* failures. The failed valves are replaced or repaired immediately after inspection, while the normal ones are allowed to be used again in the next interval. Thus, a critical parameter that must be selected in applying the preventive maintenance policy is the length of inspection interval. Vaurio[7] suggested that the proper inspection lengths could be determined so as to minimize the cost rate or accident rate of a given system. The same author later[8] modified this policy by incorporating the age-replacement mechanism, i.e., every component is replaced after a fixed number of inspections and/or repairs. Badia et al.[9] assumed that all failures in the given system are unrevealed and developed accordingly a computation procedure to determine the cost-optimal inspection intervals. They then extended this approach in the next year[10] to other engineering systems in which both revealed and unrevealed failures may be present. Finally, Duarte et al.[11] optimized the preventive maintenance plan of a series system to achieve the minimum cost rate under the assumptions that the repair rate is constant and, also, both the hazard rate and failure rate increase linearly with time.

It should be noted that, even with the above-mentioned advances, a sequential procedure must still be followed to carry out all tasks needed to synthesize a suitable protective system. These tasks include (1) the synthesis of system configuration, (2) the stipulation of maintenance policy, and (3) the estimation of total expected expenditure. Since a sequential approach cannot be used to properly address the tradeoff issues, there is a need to develop an integrated mathematical programming model to perform these steps simultaneously and to generate the optimal design automatically. Andrews and Bartlett[12] utilized a branching search strategy to solve the optimal design problem of a multilayer protective system. Although the system structure could be obtained, the maintenance strategy and also the expected expenditures were not considered in their model.

The aim of this study is to construct an improved mathematical programming model to circumvent all drawbacks mentioned above. From the optimal solution, one should be able to determine, in each protection layer, the following important design specifications: (1) the number of sensors and the corresponding alarm logic, (2) the number of valves and the corresponding shutdown configuration, and (3) the needed maintenance policies for all components. Furthermore, it should be noted that the sensors and valves in the protective systems are assumed to be maintained respectively with the corrective and preventive strategies in this work. Thus, the optimal number of spare sensors stored offline and the best inspection interval for each valve can also be determined by solving the proposed model.

2. Maintenance Policies for Individual Components

Any man-made system can be viewed as a collection of interconnected hardware components. To facilitate formulation of generic mathematical programs for producing the optimal designs of protective systems, it is important to first review the candidate maintenance policies for these components and also possible management measures to enhance system availability.

Reliability and Availability. By definition, *reliability* is the ability of an item to perform a required function for a stated period of time and under specified environmental and operational conditions.[13] In particular, reliability can be regarded as the probability that a *nonrepairable* component survives the time interval $(0,t)$ and is still functioning at time t. In the reliability literature, it is a common practice to assume that the critical hardware, e.g., a sensor or a solenoid valve, is put into service only after the burn-in period and is replaced before it enters the wear-out phase. Thus, the failure rate λ of this component can be treated as a constant parameter and it can be shown that the corresponding reliability $R(t)$ is exponentially distributed over time.[13,14]

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

On the other hand, the term "availability" $A(t)$ refers to the probability that a *repairable* component is normal at time t.[13] The availability function is obviously related to the maintenance policy. The two basic policies adopted in the present study are briefly outlined in the following subsections.

Corrective Maintenance Policy. The corrective maintenance policy can only be applied to the revealed failures which are

unrecoverable. In particular, repair is performed on a failed component to bring it back to the functioning state as quickly as possible. The sensors in the alarm subsystem are assumed to be maintained with this approach to reduce the chance of FD failures. To build the design model, explicit expressions of the availability and the expected numbers of repairs and replacements within a specified time period must be obtained first. Since they can be found in standard textbooks, e.g., Hoyland and Rausand,[13] these formulas are listed below without detailed derivations.

Let us first assume that the failure rate (λ) and repair rate (μ) of an online sensor (*without* spares) are independent of time. The availability function under these assumptions can be written as[13,14]

$$A(t) = \frac{\mu}{\mu+\lambda} + \frac{\lambda}{\mu+\lambda} e^{-(\mu+\lambda)t} \tag{2}$$

Notice that since a positive steady-state availability exists, i.e.,$A(\infty) = \mu/(\mu + \lambda)$, the *average* availability is essentially the same as this limiting value. Specifically,

$$\bar{A} \triangleq \lim_{\theta\to\infty} \frac{\int_0^\theta A(\eta)\, d\eta}{\theta} = A(\infty) \tag{3}$$

It can also be derived that the expected number of repairs during a specified time period, ENRpr(t_1,t_2), can be approximated with the following formula[14]

$$\mathrm{ENRpr}(t_1, t_2) \approx \frac{\mu\lambda}{\mu+\lambda}(t_2 - t_1) \tag{4}$$

where t_1 and t_2 are two assigned time instances and $t_1 < t_2$. Finally, since the spares are not available in this case, the expected number of replacements should be zero in any period.

To ensure a high safety integrity level, a more comprehensive program is adopted in the present study to maintain the sensors in alarm subsystem. In particular, spares are allowed to improve availability. This spare-supported strategy can be summarized as follows:

• A total of m sensors are purchased for measuring a particular process condition. One of them is installed online, while the remaining $m - 1$ sensors are stored offline and treated as spares. It is assumed that a normal spare sensor can never fail.

• If an online sensor fails and at least one offline sensor is functional, then replace the former with a spare. The failed sensor is taken offline and then placed in a queue for repair. This practice is due to the belief that replacement is much faster than repair.

• The repair process of the failed offline sensors is in effect only when the online sensor is working. It is also assumed that these failed sensors can only be repaired one at a time in sequence.

• The repair process of the failed *online* sensors can only take place if none of the offline sensors are functional. It is again assumed that these failed sensors can only be repaired one by one in sequence.

The corresponding Markov diagram can be found in Figure 1. Notice that there are $2m$ different nodes in this model. Each node reflects a collective state of the m sensors and every state can be characterized by specifying (1) whether or not the online sensor is working and (2) the number of failed (and working) offline sensors. The definitions of these states are given below:

State $2j$ ($j = 0, 1, 2,..., m - 1$): The online sensor is normal. Among the $m - 1$ offline sensors, j of them are out of order but the rest are functional.

State $2j + 1$ ($j = 0, 1, 2,..., m - 2$): The online sensor is not working. The conditions of the offline sensors are the same as those in state $2j$, i.e., the number of failed offline sensors is j.

State $2m - 1$: All online and offline sensors are broken.

Notice that the transition rates are marked next to the arcs connecting the states. In particular, λ, μ, and ε denote respectively the failure rate, repair rate, and replacement rate of a single sensor. Let us further assume that the entire operation period is long enough so that the steady-state probabilities of all the aforementioned states can be reached within a relatively short time period. These probabilities can be related with a set of state equations derived according to the Markov diagram in Figure 1.[6,15,16] For the sake of brevity, the detailed derivations are again omitted and only the resulting formulas are given below:

$$P_{2j} = \frac{\left(\frac{\lambda}{\mu}\right)^j}{\left(1+\frac{\lambda}{\varepsilon}\right)\sum_{k=0}^{m-2}\left(\frac{\lambda}{\mu}\right)^k + \left(1+\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)^{m-1}}; \quad j = 0, 1, \ldots, m-1 \tag{5}$$

$$P_{2j+1} = \frac{\left(\frac{\lambda}{\mu}\right)^j\left(\frac{\lambda}{\varepsilon}\right)}{\left(1+\frac{\lambda}{\varepsilon}\right)\sum_{k=0}^{m-2}\left(\frac{\lambda}{\mu}\right)^k + \left(1+\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)^{m-1}}; \quad j = 0, 1, \ldots, m-2 \tag{6}$$

$$P_{2(m-1)+1} = \frac{\left(\frac{\lambda}{\mu}\right)^m}{\left(1+\frac{\lambda}{\varepsilon}\right)\sum_{k=0}^{m-2}\left(\frac{\lambda}{\mu}\right)^k + \left(1+\frac{\lambda}{\mu}\right)\left(\frac{\lambda}{\mu}\right)^{m-1}} \tag{7}$$

where P_k denotes the existence probability of state$k$ and $k = 0$, 1, 2,..., $2m - 1$. The limiting (or average) availability can be computed accordingly, i.e.

$$A(\infty) = \bar{A}^{\mathrm{Corr}} = \sum_{j=0}^{m-1} P_{2j} \tag{8}$$

The expected numbers of repairs and replacements can also be approximated with the probabilities presented in eqs 5–7, i.e.

$$\mathrm{ENRpr}(t_1, t_2) \approx \mu(t_2 - t_1)\left(P_{2(m-1)+1} + \sum_{j=1}^{m-1} P_{2j}\right) \tag{9}$$

$$\mathrm{ENRpl}(t_1, t_2) \approx \varepsilon(t_2 - t_1)\sum_{j=0}^{m-2} P_{2j+1} \tag{10}$$

Finally, notice that eqs 8, 9, and 10 are valid only when $m \geq 2$. If $m = 1$, eqs 2, 3, and 4 should be used to evaluate these parameters.

Preventive Maintenance Policy. As mentioned previously, the FD failures of passive components, e.g., solenoid valves, safety valves, and rupture discs, used in a protective system in general cannot be observed online and such failures are often referred to as the *unrevealed* or *hidden* failures. It is therefore necessary to use a preventive maintenance scheme to bring the availability of a shutdown subsystem to an acceptable level. In this study, the required maintenance tasks are restricted to those associated with the periodic inspection, the repair, and replacement of every passive component. After inspection (and may be repair or replacement later), the component is considered to be "as good as new".

Table 1. Four Possible Scenarios of Protective System Failures

	failure type	x	f	h
scenario 1	FD (alarm)	1	0	0
scenario 2	FD (shutdown)	1	1	0
scenario 3	FS (alarm)	0	1	1
scenario 4	FS (shutdown)	0	0	1

Under the assumptions given above, it is obvious that the availability of a passive component in the period between inspections should be the same as the reliability of a nonrepairable component, i.e.

$$A(t) = e^{-\lambda(t-k\tau)}; \quad k\tau \le t < (k+1)\tau \tag{11}$$

where τ is the length of an inspection interval and $k = 0, 1, 2,...,$. The average availability in this case can be derived accordingly:

$$\overline{A}^{\text{Prev}} = \frac{1}{\lambda\tau}(1 - e^{-\lambda\tau}) \tag{12}$$

Finally, it should be noted that the inspection interval τ is regarded as a design parameter in this work.

3. Single-Layer System Designs

A generic design model for the single-layer protective systems is described in this section. Since this model serves as the basis for further extension to the multilayer applications, the detailed derivations of its constraints are also included.

General Process Structure. The general structure of a protected process is sketched in Figure 2. A binary variable $x \in \{0,1\}$ is used here to represent the *process state*, i.e.

$$x = \begin{cases} 1 & \text{if the process is in an unsafe state} \\ 0 & \text{otherwise} \end{cases} \tag{13}$$

If this state can be verified by measuring a critical process variable, e.g., temperature, pressure, or flow rate, etc., then another binary variable $y \in \{0,1\}$ can be used to reflect the condition of sensor output, i.e.

$$y = \begin{cases} 1 & \text{if the sensor detects an unsafe process state} \\ 0 & \text{otherwise} \end{cases} \tag{14}$$

If, for safety reasons, a total of M sensors are adopted to measure the same process condition, the outputs of these sensors form an M-dimensional binary vector, i.e., $\mathbf{y} = [y_1\ y_2...\ y_M]^T$ and $y_1, y_2,..., y_M \in \{0,1\}$. Notice that the total number of sensors used for alarm generation (M) is treated as a design parameter in this study.

A logic operation can be applied to the above M binary values to decide whether or not an alarm should be set off. This logic can also be regarded as an alarm function $f(\mathbf{y})$, i.e.

$$f(\mathbf{y}) = \begin{cases} 1 & \text{if the alarm subsystem sets off an alarm} \\ 0 & \text{otherwise} \end{cases} \tag{15}$$

Synthesis of alarm generation logic is one of the basic tasks in designing a protective system. In particular, the values of alarm function should be properly assigned for *all* possible $\mathbf{y}$ and, if possible, an explicit expression of $f(\mathbf{y})$ should also be identified. Having established this unique mapping between $\mathbf{y}$ and $f(\mathbf{y})$, the corresponding logic can be implemented either as a hardwired circuit or as a computer program.

Depending on the process needs, the alarm signal may be handled either manually by the operator(s) or automatically with a shutdown subsystem. Only the latter is considered here. To facilitate the model formulation, a third binary variable z is used to denote whether or not a designated emergency-response operation is executed by a shutdown unit. As an example, this operation can be opening or closing of a solenoid valve. More specifically

$$z = \begin{cases} 1 & \text{if the shutdown unit performs the designated operation} \\ 0 & \text{otherwise} \end{cases} \tag{16}$$

To ensure success in shutting down the given process upon demand, a total of N redundant units can be installed for this purpose. The conditions of these units can be represented with another binary vector, i.e., $\mathbf{z} = [z_1\ z_2...\ z_N]^T$ and $z_1, z_2,..., z_N \in \{0,1\}$. Notice that the total number of shutdown units (N) is also treated as a design parameter in this study.

Since a protective system is needed mainly to guard against the more hazardous FD failures, it is assumed that the logic of OR is always adopted to configure the shutdown subsystems. Let us define a binary shutdown function accordingly:

$$h(\mathbf{z}) = \begin{cases} 1 & \text{if the subsystem performs the shutdown operation successfully} \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

This function can thus be written explicitly as

$$h(\mathbf{z}) = 1 - \prod_{j=1}^{N}(1 - z_j) \tag{18}$$

Total Expected Loss. Let us use the symbol p to denote the average existence probability of an unsafe process state in one year, i.e.

$$p = \Pr\{x = 1\} \tag{19}$$

Also, let us use a_i and b_i to represent, respectively, the conditional probabilities of FS and FD failures of the ith sensor in alarm subsystem, i.e.

$$\begin{aligned} a_i &= \Pr\{y_i = 1 | x = 0\} \\ b_i &= \Pr\{y_i = 0 | x = 1\} \end{aligned} \tag{20}$$

Notice that a_i is regarded as a *given* model parameter in this work and

$$b_i = 1 - \overline{A}_i^{\text{Corr}}(m) \tag{21}$$

where $\overline{A}_i^{\text{Corr}}(m)$ is the average availability of the ith online sensor. Notice that this value is computed according to eq 8 and it can be adjusted by varying the number of spares.

It was shown in Henley and Kumamoto[15,17] that the conditional probabilities of the FS and FD failures of the alarm subsystem can be written, respectively, as

$$\begin{aligned} P_{\text{FS}}^{\text{AL}} &= \Pr\{f(\mathbf{y}) = 1 | x = 0\} = \sum_{\mathbf{y}} f(\mathbf{y}) \Pr\{\mathbf{y} | x = 0\} \\ P_{\text{FD}}^{\text{AL}} &= \Pr\{f(\mathbf{y}) = 0 | x = 1\} = \sum_{\mathbf{y}} [1 - f(\mathbf{y})] \Pr\{\mathbf{y} | x = 1\} \end{aligned} \tag{22}$$

Let us temporarily assume that the shutdown subsystem is always functional. The expected loss of operating the given process in this situation can be formulated as

$$L_{AL} = C_a \Pr\{x=0\} P_{FS}^{AL} + C_b \Pr\{x=1\} P_{FD}^{AL} = C_b p - \sum_{\mathbf{y}} f(\mathbf{y}) g(\mathbf{y}) \quad (23)$$

where

$$g(\mathbf{y}) = C_b p \Pr\{\mathbf{y}|x=1\} - C_a(1-p)\Pr\{\mathbf{y}|x=0\} \quad (24)$$

In the above two equations, C_a and C_b denote respectively the financial losses incurred from FS and FD failures of the protective system. If the sensor outputs are statistically independent, the conditional probabilities in the above equations, i.e., $\Pr\{\mathbf{y}|x=0\}$ and $\Pr\{\mathbf{y}|x=1\}$, can be transformed into functions of a_is and b_is, respectively, i.e.

$$\Pr\{\mathbf{y}|x=0\} = \prod_{i=1}^{M} \Pr\{y_i|x=0\} = \prod_{i=1}^{M} \left[a_i^{y_i}(1-a_i)^{1-y_i}\right]$$
$$\Pr\{\mathbf{y}|x=1\} = \prod_{i=1}^{M} \Pr\{y_i|x=1\} = \prod_{i=1}^{M} \left[b_i^{1-y_i}(1-b_i)^{y_i}\right] \quad (25)$$

To generate the comprehensive protective system designs, four possible failure scenarios are considered in this work (see Table 1). Notice that the FD and FS failures of the protective system can be attributed to the corresponding failures in each of the two subsystems. The probabilities that both subsystems fail simultaneously are assumed to be negligible and thus ignored. The expected yearly loss caused by the failures listed in Table 1 can be expressed as,[15,17]

$$L_{PT,1} = C_a(1-p)\sum_{\mathbf{y}} \Pr\{\mathbf{y}|x=0\}\varphi_a(\mathbf{y}) + C_b p \sum_{\mathbf{y}} \Pr\{\mathbf{y}|x=1\} \times \varphi_b(\mathbf{y}) \quad (26)$$

where

$$\varphi_a(\mathbf{y}) = (1 - P_{FD}^{SD}) f(\mathbf{y}) + P_{FS}^{SD}[1 - f(\mathbf{y})] \quad (27)$$

$$\varphi_b(\mathbf{y}) = (1 - P_{FS}^{SD})[1 - f(\mathbf{y})] + P_{FD}^{SD} f(\mathbf{y}) \quad (28)$$

According to eqs 17 and 18, the conditional probabilities of FS and FD failures of the shutdown subsystem can be expressed as

$$P_{FS}^{SD} = \Pr\{h(\mathbf{z})=1|f(\mathbf{y})=0\} = 1 - \prod_{j=1}^{N}(1-\alpha_j) \quad (29)$$

$$P_{FD}^{SD} = \Pr\{h(\mathbf{z})=0|f(\mathbf{y})=1\} = \prod_{j=1}^{N} \beta_j \quad (30)$$

where α_j and β_j denote respectively the conditional probabilities of the FS and FD failures of the jth shutdown unit. Notice that α_j is also regarded as a *given* model parameter and

$$\beta_j = 1 - \bar{A}_j^{Prev}(\tau_j) \quad (31)$$

where $\bar{A}_j^{Corr}(\tau_j)$ is the average availability of the jth shutdown unit. Notice that this value is computed according to eq 12 in the proposed model and it can be manipulated by changing the inspection interval.

By substituting eqs 19, 20, 25, and 27–30 into eq 26, one can then obtain a compact expression of the expected loss for operating the protective system, i.e.

$$L_{PT,1} = (1 - P_{FS}^{SD}) C_b p - P_{FS}^{SD} C_a (1-p) - (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{\mathbf{y}} f(\mathbf{y}) g(\mathbf{y}) \quad (32)$$

Notice that the definition of function $g(\mathbf{y})$ in this equation has already been given in eqs 24 and 25. Notice also that the expected loss in eq 32 can be minimized by constructing the alarm logic according to the following rules:

- when $1 - P_{FS}^{SD} - P_{FD}^{SD} \geq 0$: $f(\mathbf{y}) = \begin{cases} 1 & \text{if } g(\mathbf{y}) > 0 \\ 0 & \text{if } g(\mathbf{y}) \leq 0 \end{cases}$ (33)

- when $1 - P_{FS}^{SD} - P_{FD}^{SD} < 0$: $f(\mathbf{y}) = \begin{cases} 1 & \text{if } g(\mathbf{y}) < 0 \\ 0 & \text{if } g(\mathbf{y}) \geq 0 \end{cases}$ (34)

The overall expected loss of protective system during its entire operating life (H) can thus be determined by converting the loss in every year to the same time basis and then summing them together. Specifically, this overall loss (L_{PT}^{LC}) can be expressed as

$$L_{PT,1}^{LC} = \sum_{k=1}^{H} \frac{L_{PT,1}(k-1,k)}{(1+r)^{k-1}} \quad (35)$$

where $L_{PT,1}(k-1,k)$ denotes the expected loss in the kth year and r is the interest rate. It is assumed in this study that the existence probability of unsafe process state, i.e., p, and the conditional probabilities of FS and FD failures of all components in the protective system, i.e., a_i, b_i, α_j, and β_j, are independent of time. Consequently, L_{PT}^{LC} can be computed according to eqs 24, 25, and 32 by respectively replacing the costs of FS and FD failures, i.e., C_a and C_b, with the following cost parameters:

$$C_a^{LC} = \sum_{k=1}^{H} \frac{C_a(k-1,k)}{(1+r)^{k-1}} \quad (36)$$

$$C_b^{LC} = \sum_{k=1}^{H} \frac{C_b(k-1,k)}{(1+r)^{k-1}} \quad (37)$$

where $C_a(k-1,k)$ and $C_b(k-1,k)$ represent the costs of FS and FD failures respectively in the kth year.

Table 2. Optimization Results of Case Study No. 1: Part 1

	run no.				
	1.1	1.2	1.3	1.4	1.5
objective function (obj_1)	14475	14475	14475	16744	22538
budget limit (C_{budget})	10000	7000	5000	4000	3000
total expected cost ($C_{AL}^{LC} + C_{SD}^{LC}$)	4940	4940	4940	3997	2950
no. of solenoid valves ($\sum_{j=1}^{N} s_j$)	2	2		2	2
inspection interval of solenoid valves (τ_j)	3	3	3	5	6
no. of online sensors ($\sum_{i=1}^{M} \sum_{m=1}^{\Omega_i} w_{i,m}$)	3	3	3	3	2
alarm logic	2oo3	2oo3	2oo3	2oo3	1oo2
no. of online and spare components purchased for sensor 1 (type I)	3	3	3	2	2
no. of online and spare components purchased for sensor 2 (type I)	3	3	3	3	2
no. of online and spare components purchased for sensor 3 (type I)	3	3	3	3	0
no. of online and spare components purchased for sensor 4 (type I)	0	0	0	0	0

Life-Cycle Cost for a Single Online Component. Since the spare-supported corrective maintenance policy is adopted in this work to improve the availability of every online sensor, the related expenditures can be divided into three parts, i.e., (a) the purchase cost, (b) the expected repair cost, and (c) the expected replacement cost. Let us assume that, for every online sensor in the alarm subsystem, a total of $m - 1$ redundant spares are purchased. Only the one-line component is used to produce the value of corresponding binary variable in the alarm function. The total life-cycle cost of every online sensor and its spares can be expressed as

$$\begin{aligned} \mathrm{LCC}_i^{\mathrm{sensor}} &= m \times \mathrm{PCS}_i + \mathrm{ENRpr}_i(m) \sum_{k=1}^{H} \frac{\mathrm{RprsC}_i(k-1,k)}{(1+r)^{k-1}} + \\ &\quad \mathrm{ENRpl}_i(m) \sum_{k=1}^{H} \frac{\mathrm{RplsC}_i(k-1,k)}{(1+r)^{k-1}} \\ &= m \times \mathrm{PCS}_i + \mathrm{ENRpr}_i(m) \times H \times \overline{\mathrm{RprsC}_i} + \\ &\quad \mathrm{ENRpl}_i(m) \times H \times \overline{\mathrm{RplsC}_i} \end{aligned} \tag{38}$$

where PCS_i denotes the purchase cost of one sensor i; $\mathrm{RprsC}_i(k-1,k)$ and $\mathrm{RplsC}_i(k-1,k)$ represent respectively the repair and replacement costs of sensor i in the kth year. Notice that the remaining cost parameters in this equation are defined as

$$\overline{\mathrm{RprsC}_i} = \frac{1}{H} \sum_{k=1}^{H} \frac{\mathrm{RprsC}_i(k-1,k)}{(1+r)^{k-1}}$$

and

$$\overline{\mathrm{RplsC}_i} = \frac{1}{H} \sum_{k=1}^{H} \frac{\mathrm{RplsC}_i(k-1,k)}{(1+r)^{k-1}}$$

From eqs 5–10, it is obvious that the expected numbers of repairs and replacements per year, i.e., $\mathrm{ENRpr}_i(m)$ and $\mathrm{ENRpl}_i(m)$, can be manipulated by adjusting the number of purchased sensors m. To facilitate a rigorous model formulation, it is also defined in this study that

$$\mathrm{ENRpr}_i(0) = \mathrm{ENRpl}_i(0) = 0 \tag{39}$$

On the other hand, since the preventive strategy is used to maintain the shutdown subsystem, the corresponding life-cycle expenditures should include: (a) the purchase cost, (b) the inspection cost and (c) the expected repair/replacement cost. For convenience, let us assume that the length of inspection interval for each shutdown unit (τ_j) can only be an integer number of months. Specifically, the life-cycle cost associated with a solenoid valve in the shutdown subsystem can be written as

$$\begin{aligned} \mathrm{LCC}_j^{\mathrm{valve}} &= \mathrm{PCV}_j + \frac{12}{\tau_j} \sum_{k=1}^{H} \frac{\mathrm{InspC}_j(k-1,k)}{(1+r)^{k-1}} + \\ &\quad \frac{12}{\tau_j}\left[1 - \exp\left(-\frac{\lambda_j \tau_j}{12}\right)\right] \sum_{k=1}^{H} \frac{\mathrm{RprlC}_j(k-1,k)}{(1+r)^{k-1}} \\ &= \mathrm{PCV}_j + \frac{12}{\tau_j} \times H \times \overline{\mathrm{InspC}_j} + \\ &\quad \frac{12}{\tau_j}\left[1 - \exp\left(-\frac{\lambda_j \tau_j}{12}\right)\right] \times H \times \overline{\mathrm{RprlC}_j} \end{aligned} \tag{40}$$

where PCV_j denotes the purchase cost of unit j; $\mathrm{InspC}_j(k-1,k)$ and $\mathrm{RprlC}_j(k-1,k)$ represent respectively the corresponding inspection and repair (or replacement) costs in the kth year. Notice also that

$$\overline{\mathrm{InspC}_j} = \frac{1}{H} \sum_{k=1}^{H} \frac{\mathrm{InspC}_j(k-1,k)}{(1+r)^{k-1}}$$

and

$$\overline{\mathrm{RprlC}_j} = \frac{1}{H} \sum_{k=1}^{H} \frac{\mathrm{RprlC}_j(k-1,k)}{(1+r)^{k-1}}$$

in this equation.

Integer Program—IP1. As mentioned before, the expected expenditures associated with a protective system can be divided into three categories, i.e., (a) the purchase cost of alarm subsystem and its expected repair and replacement expenditures, (b) the purchase and inspection costs of shutdown subsystem and its expected repair cost, and (c) the total expected loss due to FS and FD failures of the overall protective system. In the proposed mathematical program, the sum of all aforementioned expenditures is used as the objective function.

Let us first consider the purchase and maintenance costs of the alarm subsystem. Since the number of components used in the alarm logic and the number of spares used to support each of these online sensors are both unknown before the optimization problem is solved, a binary variable $w_{i,m}$ is adopted in the mathematical programming model to reflect if the ith online sensor is adopted and also if the number of corresponding spares is $m - 1$. More specifically

$$w_{i,m} = \begin{cases} 1 & \text{if the } i\text{th online sensor is adopted} \\ & \quad \text{and there are } m-1 \text{spares} \\ 0 & \text{otherwise} \end{cases} \tag{41}$$

where $i = 1, 2, \ldots, M$ and $m = 1, 2, \ldots, \Omega_i$. Notice that $\Omega_i - 1$ is the maximum number of spares supporting the ith online sensor. Since at most one of the above options can be selected for every online sensor, the following inequality constraint must be used to stipulate such a requirement:

$$\sum_{m=1}^{\Omega_i} w_{i,m} \le 1 \tag{42}$$

It should be noted that this formulation accommodates the possibility of not incorporating the ith online sensor in the alarm logic, i.e., $w_{i,1} = w_{i,2} = \cdots = w_{i,\Omega_i} = 0$. In addition, since it is sometimes desirable to ensure that at least one online sensor is included in alarm logic, another inequality constraint may be added in the model:

$$\sum_{i=1}^{M} \sum_{m=1}^{\Omega_i} w_{i,m} \ge 1 \tag{43}$$

The total life-cycle cost of the alarm subsystem can thus be expressed as

$$\begin{aligned} C_{\mathrm{AL}}^{\mathrm{LC}} = \sum_{i=1}^{M} \sum_{m=1}^{\Omega_i} w_{i,m} \big[& m \times \mathrm{PCS}_i + \mathrm{ENRpr}_i(m) \times H \times \overline{\mathrm{RprsC}_i} + \\ & \mathrm{ENRpl}_i(m) \times H \times \overline{\mathrm{RplsC}_i} \big] \end{aligned} \tag{44}$$

Let us next consider the purchase and maintenance costs associated with a shutdown subsystem. Since the number of shutdown units is treated as a decision variable in the proposed design problem, another binary variable s_j is adopted to represent whether or not the jth unit is selected for online implementation, i.e.

$$s_j = \begin{cases} 1 & \text{if the } j\text{th shutdown unit is adopted for implementation} \\ 0 & \text{otherwise} \end{cases} \tag{45}$$

Again, due to the need to incorporate at least one shutdown unit, it is necessary to impose the following constraint:

$$\sum_{j=1}^{N} s_j \geq 1 \tag{46}$$

The total life-cycle cost of a shutdown subsystem can be expressed with the aid of these binary variables, i.e.

$$C_{\mathrm{SD}}^{\mathrm{LC}} = \sum_{j=1}^{N} s_j \left[\mathrm{PCV}_j + \frac{12}{\tau_j} \times H \times \overline{\mathrm{InspC}}_j + \frac{12}{\tau_j}\left[1 - \exp\left(-\frac{\lambda_j \tau_j}{12}\right)\right] \times H \times \overline{\mathrm{RprlC}}_j \right] \tag{47}$$

Finally, let us consider the expected loss given in eq 32. It can be observed that the conditional probabilities of FS and FD failures of the shutdown subsystem must be expressed as functions of the binary variables s_js. In other words, eqs 29 and 30 should be rewritten to account for the possibility of excluding one or more units, i.e.

$$P_{\mathrm{FS}}^{\mathrm{SD}} = 1 - \prod_{j=1}^{N} (1 - \alpha_j s_j) \tag{48}$$

$$P_{\mathrm{FD}}^{\mathrm{SD}} = \prod_{j=1}^{N} \beta_j^{s_j} \tag{49}$$

From eqs 24, 25, and 32, it is clear that the function $g(\mathbf{y})$ must be reformulated in terms of the binary variables $w_{i,m}$s. Specifically, eq 25 should be modified as

$$\begin{aligned} &\Pr\{\mathbf{y}|x=0\} = \\ &\prod_{i=1}^{M} \left[a_i y_i (1-a_i)^{1-y_i} \sum_{m=1}^{\Omega_i} w_{i,m} + (1-y_i)\left(1 - \sum_{m=1}^{\Omega_i} w_{i,m}\right)\right] \\ &\Pr\{\mathbf{y}|x=1\} = \\ &\prod_{i=1}^{M} \left[\sum_{m=1}^{\Omega_i} b_{i,m}^{1-y_i} (1-b_{i,m})^{y_i} w_{i,m} + (1-y_i)\left(1 - \sum_{m=1}^{\Omega_i} w_{i,m}\right)\right] \end{aligned} \tag{50}$$

As mentioned previously, a_i is a *fixed* model parameter, while b_i is a function of m according to eq 21. Notice that a set of new parameters are adopted in eq 50 to represent the latter for different m, i.e., $b_{i,m} = 1 - \bar{A}_i^{\mathrm{Corr}}(m)$ and $m = 1, 2, ..., \Omega_i$. It is important to note that the values of these parameters can be computed in advance before solving the optimization problem. Notice also that the same term $(1 - y_i)(1 - \sum_{m=1}^{\Omega_i} w_{i,m})$ appears in the expressions for both $\Pr\{\mathbf{y}|x=0\}$ and $\Pr\{\mathbf{y}|x=1\}$. These formulations are designed to provide correct probability values when the ith sensor is excluded from alarm logic ($w_{i,1} = w_{i,2} = ... = w_{i,\Omega_i} = 0$), i.e.,$\Pr\{y_i=0|x=0\} = 1$, $\Pr\{y_i=0|x=1\} = 1$, $\Pr\{y_i=1|x=0\} = 0$ and $\Pr\{y_i=1|x=1\} = 0$. In other words, this scenario can be viewed as having a fictitious online sensor which does not send out any alarm signal under all circumstances. Substituting eq 50 into eq 24 yields a modified version of $g(\mathbf{y})$ in the expression for total expected loss $L_{\mathrm{PT},1}^{\mathrm{LC}}$ in eq 32.

The objective function of the mathematical program for generating the optimal configuration and maintenance policy of a single-layer protective system can thus be written as

$$\mathrm{obj}_1 = C_{\mathrm{AL}}^{\mathrm{LC}} + C_{\mathrm{SD}}^{\mathrm{LC}} + L_{\mathrm{PT},1}^{\mathrm{LC}} \tag{51}$$

In certain applications, there is also a need to impose a general budget constraint, i.e.

$$C_{\mathrm{AL}}^{\mathrm{LC}} + C_{\mathrm{SD}}^{\mathrm{LC}} \leq C_{\mathrm{budget}} \tag{52}$$

where C_{budget} is a given constant. The solutions of the corresponding mathematical program include (a) the integer values of variables s_j, τ_j, and $w_{i,m}$ and (b) the binary values of function $f(\mathbf{y})$ for all possible $\mathbf{y}$.

4. Multilayer System Design

As mentioned before, the expected loss in the operating life of a single-layer protective system can be attributed to FS and FD failures. The former loss is in general far less than the latter, i.e., $C_a \ll C_b$. Thus, it is possible to reduce the total expected loss significantly by adding one or more additional protection layers to lower the chance of FD failures.

Illustrative Examples. To fix idea, let us consider the CSTR in Figure 3 as an illustrative example. The protective system here consists of a hierarchy of three layers. At the lowest level is a flow-control loop. The inlet flow is kept at the set point with a flow sensor/transmitter (FT), a flow controller (FRC), and a flow control valve (FCV). If the flow-control system fails, the resulting abnormal flow rate could raise the reactor temperature to an upper limit and trigger the temperature interlock in the second layer. A subsequent trip operation is supposed to be carried out by cutting off the inlet flow with a temperature sensor/transmitter (TT), a switch (TSH), and a solenoid valve (ESV). However, this temperature increase may continue if a FD failure occurs in the interlock system. As a result, the reactor pressure could also be driven to a very high level by the high temperature. To prevent the catastrophic outcomes of a runaway reaction and explosion, a pressure-relief system is installed here to vent the reactor contents at a set pressure. This last protection layer is equipped with a pressure sensor/transmitter (PT), a switch (PSH), and a solenoid valve (PRV). It should be pointed out that the pressure-relief operations are in general realized in industrial applications with safety valves or rupture discs. The protective system configuration in Figure 3 can thus be modified by replacing its third layer with one of the aforementioned pressure-relief devices (see Figure 4). Notice that no pressure sensors are needed in this modified design. For convenience, the protective systems described in Figures 3 and 4 will later be referred to as *scheme A* and *scheme B*, respectively, in this paper.

To simplify model derivation, let us limit the scope of the present analysis to only the temperature-interlock and the

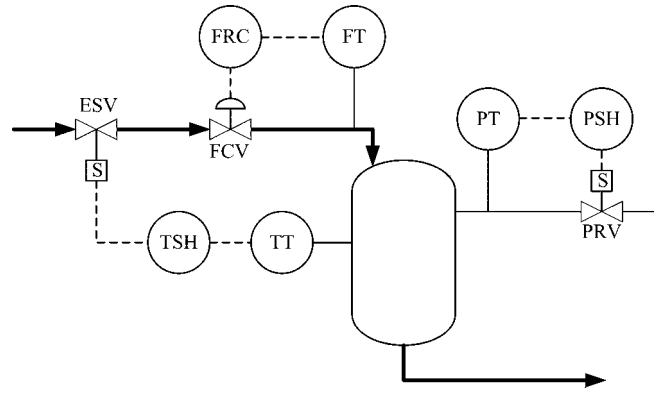

Figure 3. A CSTR with multilayer protective system (scheme A).

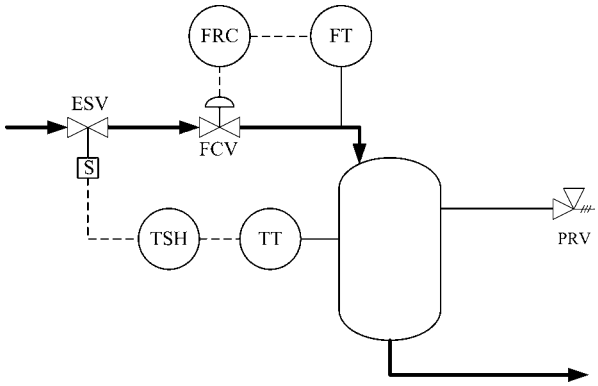

Figure 4. A CSTR with multilayer protective system (scheme B).

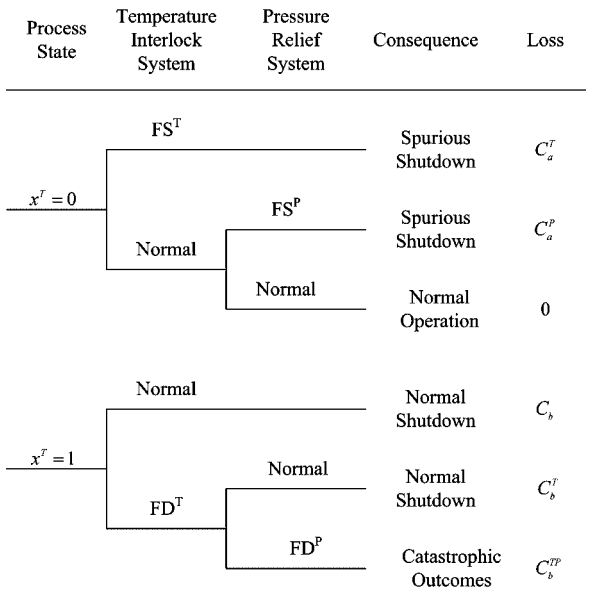

Figure 5. Event trees for a CSTR with two protection layers.

pressure-relief mechanisms in the CSTR systems. Two binary variables are thus needed to specify the process states, i.e.

$$x^T = \begin{cases} 1 & \text{if the reactor temperature exceeds its upper limit} \\ 0 & \text{otherwise} \end{cases} \tag{53}$$

$$x^P = \begin{cases} 1 & \text{if the reactor pressure exceeds its upper limit} \\ 0 & \text{otherwise} \end{cases} \tag{54}$$

For every possible initial system state, i.e., $x^T = 0$ and $x^T = 1$, a corresponding event tree can be constructed (see Figure 5). The branch labels in the first event tree, i.e., FS^T and FS^P, represent the fail-safe failures of temperature-interlock and pressure-relief systems respectively, while FD^T and FD^P in the second tree denote respectively the fail-dangerous failures of the corresponding protection systems. It can be observed that both FS^T and FS^P failures result in spurious system shutdown. The fail-safe pressure-relief scenarios always end up with the undesirable consequences of venting reactor contents and prolonged down time, while it usually takes less time and effort to resume normal operation in the FS^T related cases. Thus, it is assumed in our study that $C_a^T < C_a^P$. Notice that a single FD^T failure alone could also activate the pressure-relief devices. Since the FD failures are in general unrecoverable, it is assumed that $C_a^P < C_b^T$. It can also be observed that, under the initial condition $x^T = 1$, simultaneous FD^T and FD^P events may result in catastrophic outcomes. Therefore, the corresponding financial loss is assumed to be much greater than those in other scenarios, i.e., $C_b^T \ll C_b^{TP}$. Finally, notice that the total expected loss of the present multilayer protective system should not include the cost of normal shutdown performed by the temperature interlock. This is due to the fact that there are no failures in this situation.

Total Expected Loss. The total expected loss of operating the two-layer protective system in Figure 3 or Figure 4 can be expressed in a general form according to the two event trees given in Figure 5. In particular

$$\begin{aligned} L_{\mathrm{PT},2}^{\mathrm{LC}} = {} & C_a^{T,\mathrm{LC}}(1-p^T)\Pr\{\mathrm{FS}^{\mathrm{T}}\} + \\ & C_a^{P,\mathrm{LC}}(1-p^T)(1-\Pr\{\mathrm{FS}^{\mathrm{T}}\})\Pr\{\mathrm{FS}^{\mathrm{P}}\} + \\ & C_b^{T,\mathrm{LC}}p^T\Pr\{\mathrm{FD}^{\mathrm{T}}\}(1-\Pr\{\mathrm{FD}^{\mathrm{P}}\}) + \\ & C_b^{TP,\mathrm{LC}}p^T\Pr\{\mathrm{FD}^{\mathrm{T}}\}\Pr\{\mathrm{FD}^{\mathrm{P}}\} \end{aligned} \tag{55}$$

where $p^T = \Pr\{x^T=1\}$ and the cost parameters in this equation (i.e., $C_a^{T,\mathrm{LC}}$, $C_a^{P,\mathrm{LC}}$, $C_b^{T,\mathrm{LC}}$, and $C_b^{TP,\mathrm{LC}}$) are defined according to eqs 36 and 37. Notice also that, the product $p^T\Pr\{\mathrm{FD}^{\mathrm{T}}\}$ in the fourth term of the above equation can be expressed as $p^T\Pr\{\mathrm{FD}^{\mathrm{T}}\} = \Pr\{x^P=1\} = p^P$.

Let us consider the expected loss of *scheme A* first. The conditional probabilities of FS and FD failures in eq 55 can be expressed as

$$\begin{aligned} \Pr\{\mathrm{FS}^{\mathrm{T}}\} = {} & \sum_{\mathbf{y}^T}\Pr\{\mathbf{y}^T|x^T=0\}\times \\ & [\Pr\{h^T(\mathbf{z}^T)=1|f^T(\mathbf{y}^T)=1\}f^T(\mathbf{y}^T) + \\ & \Pr\{h^T(\mathbf{z}^T)=1|f^T(\mathbf{y}^T)=0\}(1-f^T(\mathbf{y}^T))] \\ = {} & P_{\mathrm{FS}}^{SD^T} + \left(1-P_{\mathrm{FS}}^{SD^T}-P_{\mathrm{FD}}^{SD^T}\right)\sum_{\mathbf{y}^T}f^T(\mathbf{y}^T)\Pr\{\mathbf{y}^T|x^T=0\} \end{aligned} \tag{56}$$

$$\begin{aligned} \Pr\{\mathrm{FD}^T\} = {} & \sum_{\mathbf{y}^T}\Pr\{\mathbf{y}^T|x^T=1\}\times \\ & [\Pr\{h^T(\mathbf{z}^T=0)|f^T(\mathbf{y}^T)=1\}f^T(\mathbf{y}^T) + \\ & \Pr\{h^T(\mathbf{z}^T=0)|f^T(\mathbf{y}^T)=0\}(1-f^T(\mathbf{y}^T))] \\ = {} & \left(1-P_{\mathrm{FS}}^{SD^T}\right) - \\ & \left(1-P_{\mathrm{FS}}^{SD^T}-P_{\mathrm{FD}}^{SD^T}\right)\sum_{\mathbf{y}^T}f^T(\mathbf{y}^T)\Pr\{\mathbf{y}^T|x^T=1\} \end{aligned} \tag{57}$$

$$\begin{aligned} \Pr\{\mathrm{FS}^P\} = {} & \sum_{\mathbf{y}^P}\Pr\{\mathbf{y}^P|x^P=0\}\times \\ & [\Pr\{h^P(\mathbf{z}^P)=1|f^P(\mathbf{y}^P)=1\}f^P(\mathbf{y}^P) + \\ & \Pr\{h^P(\mathbf{z}^P)=1|f^P(\mathbf{y}^P)=0\}(1-f^P(\mathbf{y}^P))] \\ = {} & P_{\mathrm{FS}}^{\mathrm{SD}^P} + \left(1-P_{\mathrm{FS}}^{\mathrm{SD}^P}-P_{\mathrm{FD}}^{\mathrm{SD}^P}\right)\sum_{\mathbf{y}^P}f^P(\mathbf{y}^P)\Pr\{\mathbf{y}^P|x^P=0\} \end{aligned} \tag{58}$$

$$\begin{aligned} \Pr\{\mathrm{FD}^{\mathrm{P}}\} = {} & \sum_{\mathbf{y}^P}\Pr\{\mathbf{y}^P|x^P=1\}\times \\ & [\Pr\{h^P(\mathbf{z}^P)=0|f^P(\mathbf{y}^P)=1\}f^P(\mathbf{y}^P) + \\ & \Pr\{h^P(\mathbf{z}^P)=0|f^P(\mathbf{y}^P)=0\}(1-f^P(\mathbf{y}^P))] \\ = {} & \left(1-P_{\mathrm{FS}}^{\mathrm{SD}^P}\right) - \\ & \left(1-P_{\mathrm{FS}}^{\mathrm{SD}^P}-P_{\mathrm{FD}}^{\mathrm{SD}^P}\right)\sum_{\mathbf{y}^P}f^P(\mathbf{y}^P)\Pr\{\mathbf{y}^P|x^P=1\} \end{aligned} \tag{59}$$

where $\mathbf{y}^T$ and $\mathbf{y}^P$ denote respectively the temperature and pressure sensor outputs; $\mathbf{z}^T$ and $\mathbf{z}^P$represent the outcomes of temperature and pressure tripping operations respectively performed by the solenoid valves; $f^T(\bullet)$ and $f^P(\bullet)$ are the temperature and pressure alarm functions; $h^T(\bullet)$ and $h^P(\bullet)$ are the temperature and pressure shutdown functions. Notice that, in the above equations, $P_{\mathrm{FS}}^{\mathrm{SD}^T}$, $P_{\mathrm{FS}}^{\mathrm{SD}^P}$, $P_{\mathrm{FD}}^{\mathrm{SD}^T}$, and $P_{\mathrm{FD}}^{\mathrm{SD}^P}$denote the conditional probabilities of FS and FD failures in the temperature and pressure shutdown subsystems and their definitions can be found in eqs 48 and 49. The remaining undefined conditional probabilities in eqs 56 – 59 can be written as

$$\Pr\{\mathbf{y}^\eta|\, x^\eta = 0\} = \prod_{i=1}^{M^\eta}\left[\left(a_i^\eta\right)^{y_i^\eta}\left(1-a_i^\eta\right)^{1-y_i^\eta}\sum_{m=1}^{\Omega_i^\eta} w_{i,m}^\eta + (1-y_i)\left(1-\sum_{m=1}^{\Omega_i^\eta} w_{i,m}^\eta\right)\right] \quad (60)$$

$$\Pr\{\mathbf{y}^\eta|\, x^\eta = 1\} = \prod_{i=1}^{M^\eta}\left[\sum_{m=1}^{\Omega_i^\eta}\left(b_{i,m}^\eta\right)^{1-y_i^\eta}\left(1-b_{i,m}^\eta\right)^{y_i^\eta} w_{i,m}^\eta + (1-y_i^\eta)\left(1-\sum_{m=1}^{\Omega_i^\eta} w_{i,m}^\eta\right)\right] \quad (61)$$

Notice that the variables used in these two equations are essentially the same as those in eq 50 except that there are additional superscripts ($\eta = T$ or P). A superscript T refers to the temperature interlock, while P denotes the pressure-relief system.

Let us next consider the expected loss of *scheme B*. All aforementioned equations in this subsection are still applicable except $\Pr\{\mathrm{FS^P}\}$ and $\Pr\{\mathrm{FD^P}\}$ in eqs 58 and 59. Since no pressure sensors are needed, the conditional probabilities of FS and FD failures of the second protection layer are essentially the same as those of the safety valves (or rupture discs), i.e.

$$\Pr\{\mathrm{FS^P}\} = 1 - \prod_{j=1}^{N}\left(1-\alpha'_j s_j\right)$$
$$\Pr\{\mathrm{FD^P}\} = \prod_{j=1}^{N}\beta'^{\,s_j}_j \quad (62)$$

where α'_j and β'_j denote respectively the conditional probabilities of the FS and FD failures of the jth pressure-relief unit.

Integer Programs—IP2A and IP2B. Two slightly different integer programs can be formulated to generate optimal designs of *scheme A* and *scheme B*. The objective functions of these two programs can be expressed respectively as

$$\mathrm{obj}_{2A} = \left(C_{\mathrm{AL},T}^{\mathrm{LC}} + C_{\mathrm{SD},T}^{\mathrm{LC}}\right) + \left(C_{\mathrm{AL},P}^{\mathrm{LC}} + C_{\mathrm{SD},P}^{\mathrm{LC}}\right) + L_{\mathrm{PT},2A}^{\mathrm{LC}}$$
$$\mathrm{obj}_{2B} = \left(C_{\mathrm{AL},T}^{\mathrm{LC}} + C_{\mathrm{SD},T}^{\mathrm{LC}}\right) + C_{\mathrm{SD},P}^{\mathrm{LC}} + L_{\mathrm{PT},2B}^{\mathrm{LC}} \quad (63)$$

where $C_{\mathrm{AL},T}^{\mathrm{LC}}$ and $C_{\mathrm{SD},T}^{\mathrm{LC}}$ denote the life-cycle costs of alarm and shutdown subsystems, respectively, in the temperature interlock; $C_{\mathrm{AL},P}^{\mathrm{LC}}$ and $C_{\mathrm{SD},P}^{\mathrm{LC}}$ denote the life-cycle costs of alarm and shutdown subsystems respectively in the pressure-relief system; $L_{\mathrm{PT},2A}^{\mathrm{LC}}$ and $L_{\mathrm{PT},2B}^{\mathrm{LC}}$ represent the expected losses of scheme A and scheme B, respectively. Notice that since the alarm subsystem is not needed in the pressure-relief system of scheme B, the corresponding cost term is not present in the objective function obj_{2B}. Notice also that both $L_{\mathrm{PT},2A}^{\mathrm{LC}}$ and $L_{\mathrm{PT},2B}^{\mathrm{LC}}$ can be expressed with the general form presented in eq 55. The conditional probabilities of FS and FD failures of the pressure-relief system in scheme A should be computed with eqs 58 and 59, while these probabilities in scheme B must be calculated according to eq 62. Finally, the budget constraints can be respectively imposed in these two programs in a way similar to eq 52, i.e.

$$\left(C_{\mathrm{AL},T}^{\mathrm{LC}} + C_{\mathrm{SD},T}^{\mathrm{LC}}\right) + \left(C_{\mathrm{AL},P}^{\mathrm{LC}} + C_{\mathrm{SD},P}^{\mathrm{LC}}\right) \le C_{\mathrm{budget}}^{2A}$$
$$\left(C_{\mathrm{AL},T}^{\mathrm{LC}} + C_{\mathrm{SD},T}^{\mathrm{LC}}\right) + C_{\mathrm{SD},P}^{\mathrm{LC}} \le C_{\mathrm{budget}}^{2B} \quad (64)$$

5. Case Studies

Three case studies are presented in the sequel to demonstrate the capabilities of integer programs IP1, IP2A, and IP2B. The first case is concerned with a liquid storage process and the other two are based on the CSTR systems given in Figures 3 and 4, respectively.

Case 1. Let us consider the single-layer protective system installed on a liquid storage vessel to prevent overflow. It is assumed in this case study that the system's operating life (H) is 5 years and the probability of an abnormally high liquid level (p) in each year is constant at 0.2. At an interest rate (r) of 6% per year, the life-cycle cost parameters adopted for the FS and FD failures are $C_a^{\mathrm{LC}} = 4.4651 \times 10^4$ USD and $C_b^{\mathrm{LC}} = 4.4651 \times 10^6$ USD.

Let us first assume that there are at most four online sensors for use in the alarm logic ($M = 4$) and also assume that each is supported by at most 3 spares, i.e., $\Omega_i = 4$ and $i = 1, 2, 3, 4$. There is only one type of level sensors (type I) available for use in the alarm subsystem and its maintenance and cost parameters are listed below:

$$\lambda_i = 0.2\ \mathrm{yr}^{-1};\ \mu_i = 0.9\ \mathrm{yr}^{-1};\ \varepsilon_i = 50\ \mathrm{yr}^{-1};\ a_i = 0.1;$$
$$\mathrm{PCS}_i = 200\ \mathrm{USD};\ \overline{\mathrm{RprsC}}_i = 35.7\ \mathrm{USD};\ \overline{\mathrm{RplsC}}_i = 17.9\ \mathrm{USD} \quad (65)$$

On the other hand, it is assumed that there are at most four solenoid valves available for implementation in the shutdown subsystem, i.e., $N = 4$. There is also only one valve type and its specifications are

$$\lambda_j = 0.35\ \mathrm{yr}^{-1};\ \alpha_j = 0.1;$$
$$\mathrm{PCV}_j = 150\ \mathrm{USD};\ \overline{\mathrm{InspC}}_j = 44.7\ \mathrm{USD};\ \overline{\mathrm{RprlC}}_j = 267.9\ \mathrm{USD} \quad (66)$$

where $j = 1, 2, 3, 4$. Notice that the relatively high repair/replacement cost used here is due to our assumption that a failed valve is replaced with a new one immediately after inspection. Five optimization runs have been carried out according to different levels of budget constraint. In particular, the integer program IP1 was solved with the module DICOPT in the commercial software GAMS on a Pentium 4 3.00 GHz PC. No more than 3 s are needed to complete each run. The results are summarized in Table 2. Notice that the abbreviations "2oo3" and "1oo2" are used in this table to represent the logics of "2 out of 3" and "1 out of 2", respectively. It can be observed from Table 2 that the objective value can in general be reduced by relaxing the budget constraint. However, this value tends to reach a constant as the upper budget limit exceeds a threshold. This is due to the fact that, although the expected loss caused by FD failures can be reduced by adding redundant components, additional loss of FS failures and also extra capital cost are also incurred by such a practice as well.

Next let us try to improve the objective value by introducing more sensor types for use in more complex alarm logics. Let us assume that, other than the sensor specifications given in eq 65, there is another type of level sensors (type II) available for evaluating additional 4 binary variables, i.e., y_i and $i = 5, 6, 7,$

Table 3. Optimization Results of Case Study No. 1: Part 2

	run no.	
	1.6	1.7
objective function (obj_1)	14444	14721
budget limit (C_{budget})	10000	10000
total expected cost ($C_{AL}^{LC} + C_{SD}^{LC}$)	5318	5404
no. of solenoid valves ($\sum_{j=1}^{N} s_j$)	2	2
inspection interval of solenoid valves (τ_j)	3	3
no. of online sensors ($\sum_{i=1}^{M} \sum_{m=1}^{\Omega_i} w_{i,m}$)	5	6
alarm logic	3oo5	Figure 6
no. of online and spare components purchased for sensor 1 (type I)	2	2
no. of online and spare components purchased for sensor 2 (type I)	2	2
no. of online and spare components purchased for sensor 3 (type I)	2	3
no. of online and spare components purchased for sensor 4 (type I)	2	0
no. of online and spare components purchased for sensor 5 (type II)	4	2
no. of online and spare components purchased for sensor 6 (type II)	0	2
no. of online and spare components purchased for sensor 7 (type II)	0	2
no. of online and spare components purchased for sensor 8 (type II)	0	0

8, which can also be incorporated into the alarm function. The maintenance and cost parameters of this type-II sensors are

$$\lambda_i = 0.4\ \text{yr}^{-1};\ \mu_i = 0.9\ \text{yr}^{-1};\ \varepsilon_i = 50\ \text{yr}^{-1};\ a_i = 0.15;$$
$$\text{PCS}_i = 120\ \text{USD};\ \overline{\text{RprsC}_i} = 21.4\ \text{USD};\ \overline{\text{RplsC}_i} = 10.7\ \text{USD} \tag{67}$$

The corresponding optimization results in Table 3 were thus produced by setting the maximum budget level at 10,000 USD (which is the same as that used in run 1.1 in Table 2). From the design obtained in run 1.6, it can be observed that the improvement in objective value is insignificant. On the other hand, it should also be noted that other more interesting (and more complicated) alarm logics may be synthesized with the integer program IP1 by imposing modified constraints. For example, run 1.7 was performed by replacing eq 42 with

$$\sum_{m=1}^{\Omega_i} w_{i,m} = 1 \quad i = 1, 2, 3, 5, 6, 7$$
$$\sum_{m=1}^{\Omega_i} w_{i,m} = 0 \quad i = 4, 8 \tag{68}$$

Notice that the corresponding objective value is again very close to those obtained in run 1.1 and run 1.6. Thus, from a practical standpoint, it may be beneficial to select the simplest design among these three, i.e., the one in run 1.1, due to the relative ease in implementation.

Case 2. Let us next consider the CSTR system presented in Figure 3. It is again assumed that the system's operating life (H) is 5 years and the probability of an abnormally high temperature (p^T) in each year is 0.2. At an interest rate (r) of 6% per year, the life-cycle cost parameters adopted for the FS and FD failures of the temperature-interlock and pressure-relief systems are

$$C_a^{T,\text{LC}} = 4.4651 \times 10^4\ \text{USD} \quad C_a^{P,\text{LC}} = 1.3395 \times 10^5\ \text{USD}$$
$$C_b^{T,\text{LC}} = 2.2326 \times 10^5\ \text{USD} \quad C_b^{TP,\text{LC}} = 4.4651 \times 10^8\ \text{USD} \tag{69}$$

Let us also assume that there are at most four online sensors in the temperature-interlock system and in the pressure-relief system, respectively ($M^T = M^P = 4$). Each of these sensors is assumed to be supported by at most 3 spares, i.e., $\Omega_i^T = \Omega_i^P = 4$ and $i = 1, 2, 3, 4$. The corresponding cost and maintenance parameters are listed in Table 4. In addition, the maximum number of solenoid valves in each of the two protection layers is set at 3, i.e., $N^T = N^P = 3$. The corresponding data are shown in Table 5.

Table 4. Maintenance and Cost Parameters of Sensors in CSTR System

subsystem	temp 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
a_i	0.10	0.05
$\underline{\text{PCS}_i}$ (USD)	200	250
$\overline{\text{RprsC}_i}$ (USD)	35.7	44.7
$\overline{\text{RplsC}_i}$ (USD)	17.9	22.3

Table 5. Maintenance and Cost Parameters of Shutdown Units in CSTR System

subsystem	temp interlock	pressure relief
λ_j (yr^{-1})	0.25	0.30
α_j	0.05	0.08
$\underline{PCV_j}$ (USD)	400	250
$\overline{\text{InspC}_j}$ (USD)	89.3	71.4
$\overline{\text{RprlC}_j}$ (USD)	535.8	334.9

Six optimization runs, i.e., run 2.1 to run 2.6 in Table 6, have been performed for different levels of budget constraint. The module DICOPT in the commercial software GAMS was used to solve the integer program IP2A. All runs took less than 2 s on a Pentium 4 3.00 GHz PC. It can be observed from Table 6a that, before approaching a minimum, the objective value can be reduced by gradually raising the maximum allowable budget level. The total expected capital and maintenance cost of all hardware items in the entire protective system and also that in the temperature-interlock system both follow the same trend. However, notice that the expected cost of pressure-relief system reaches the lowest value when the upper bound of budget level is 8000 USD (run 2.4).

From the results obtained in runs 2.4, 2.3, 2.2, and 2.1, it can be observed that the increase in capital investment for the temperature system is much larger than that for the pressure system. This is due to the fact that $p^P = p^T \text{Pr}\{\text{FD}^T\}$. Thus, by adding redundant components in the first layer of the protective system, the demand probability of the second layer (p^P) can be significantly lowered. It should also be noted that the financial penalty caused by simultaneous FD failures in both temperature and pressure systems is assumed to be much greater than those in other scenarios. As a result, the objective value can be effectively improved with the aforementioned practices. On the other hand, since adding more components in the protective system inevitably results in higher FS probabilities and also higher capital cost, the objective value eventually reaches a minimum.

Table 6. Optimization Results of Case Study No. 2

	run no.						
	2.1	2.2	2.3	2.4	2.5	2.6	2.7
a. Expenditures and Costs							
objective function (obj_{2A})	26351	26351	26977	34718	49936	63911	38315
budget limit (C^{2A}_{budget})	14000	12000	10000	8000	7000	6000	10000
total expected cost	11191	11191	9957	7978	6960	5963	8617
$C^{LC}_{AL,T} + C^{LC}_{SD,T}$	8327	8327	7567	6123	4270	1916	0
$C^{LC}_{AL,P} + C^{LC}_{SD,P}$	2864	2864	2390	1855	2690	4047	8617
b. Temperature-Interlock System Design							
no. of solenoid valves ($\sum_{j=1}^{N^T} s_j^T$)	3	3	3	3	2	1	−
inspection interval of solenoid valves (τ_j^T)	6	6	7	9	8	8	−
no. of online sensors ($\sum_{i=1}^{M^T} \sum_{m=1}^{\Omega_i{}^T} w_{i,m}^T$)	3	3	4	2	2	1	−
alarm logic	2oo3	2oo3	2oo4	1oo2	1oo2	1oo1	−
no. of online and spare components purchased for sensor 1	4	4	2	3	2	1	−
no. of online and spare components purchased for sensor 2	4	4	2	3	2	0	−
no. of online and spare components purchased for sensor 3	4	4	3	0	0	0	−
no. of online and spare components purchased for sensor 4	0	0	3	0	0	0	−
c. Pressure-Relief System Design							
no. of solenoid valves ($\sum_{j=1}^{N^P} s_j^P$)	1	1	1	1	2	3	3
inspection interval of solenoid valves (τ_j^P)	4	4	5	7	11	11	3
no. of online sensors ($\sum_{i=1}^{M^P} \sum m=1^{\Omega P} w_{i,m}^P$)	2	2	3	1	2	3	4
alarm logic	2oo2	2oo2	2oo3	1oo1	1oo2	1oo3	2oo4
no. of online and spare components purchased for sensor 1	2	2		2	2	1	2
no. of online and spare components purchased for sensor 2	2	2	1	0	0	1	2
no. of online and spare components purchased for sensor 3	0	0	1	0	0	1	2
no. of online and spare components purchased for sensor 4	0	0	0	0	0	0	2

Table 7. Optimization Results of Case Study No. 3

	run no.					
	3.1	3.2	3.3	3.4	3.5	3.6
a. Expenditures and Costs						
objective function (obj_{2B})	25868	25868	28644	34090	42742	37117
budget limit (C^{2B}_{budget})	12000	10000	8000	7000	6000	10000
total expected cost	9719	9719	7906	6937	5880	5985
$C^{LC}_{AL,T} + C^{LC}_{SD,T}$	7724	7724	6365	4313	2364	−
$C^{LC}_{SD,P}$	1995	1995	1541	2624	3516	5985
b. Temperature-Interlock System Design						
no. of solenoid valves ($\sum_{j=1}^{N^T} s_j^T$)	3	3	3	2	1	−
inspection interval of solenoid valves (τ_j^T)	7	7	8	9	8	−
no. of online sensors ($\sum_{i=1}^{M^T} \sum m=1^{\Omega T} w_{i,m}^T$)	3	3	2	2	2	−
alarm logic	2oo3	2oo3	1oo2	1oo2	1oo2	−
no. of online and spare components purchased for sensor 1	3	3	3	2	1	−
no. of online and spare components purchased for sensor 2	4	4	3	3	2	−
no. of online and spare components purchased for sensor 3	4	4	0	0	0	−
no. of online and spare components purchased for sensor 3	0	0	0	0	0	−
c. Pressure-Relief System Design						
no. of safety valves ($\sum_{j=1}^{N^P} s_j^P$)	1	1	1	2	3	3
inspection interval of safety valves (τ_j^P)	2	2	3	4	5	2

Let us next take a closer look at the results obtained in runs 2.4, 2.5, and 2.6. Notice that the number of solenoid valves used in the temperature-interlock system decreases under tightened budget constraint. Notice also that this trend is actually reversed in the case of pressure-relief system. This is due to the fact that the purchase, inspection and repair/replacement costs in the latter system are lower. Since these cheaper components are less reliable, the resulting total expected loss becomes significantly higher as well.

To evaluate the benefits of adding protection layer(s), a final optimization run (i.e., run 2.7 in Table 6, a and c) was also carried out in this case study by removing the temperature interlock from the CSTR system in Figure 3. In this situation, $p^P = p^T = 0.2$. All model parameters can be found in Tables 4 and 5. From Table 6a, notice that the budget levels of run 2.3 and 2.7 are the same. However, the objective value in the former case is significantly lower than that in the latter. Specifically, a reduction of about 30% in the total expected expenditure is achieved by switching from a single-layer protection structure to a double-layer one. This improvement is brought about by increasing the total expected capital and maintenance cost from 8617 USD to 9957 USD.

Case 3. In this last case study, let us consider the CSTR system in Figure 4. Since the protective system here is a modified version of the one presented in Figure 3, all model parameters used in the present case are the same as those in Case 2 except the maintenance and cost data associated with the safety valves, i.e.

$$\lambda_j = 0.35\ \text{yr}^{-1};\ \alpha_j = 0.1;$$
$$\text{PCV}_j = 200\ \text{USD};\ \overline{\text{InspC}_j} = 44.7\ \text{USD};\ \overline{\text{RprlC}_j} = 267.9\ \text{USD} \tag{70}$$

Five optimization runs (run 3.1−run 3.5) have been performed with integer program IP2B to synthesize the two-layer protective

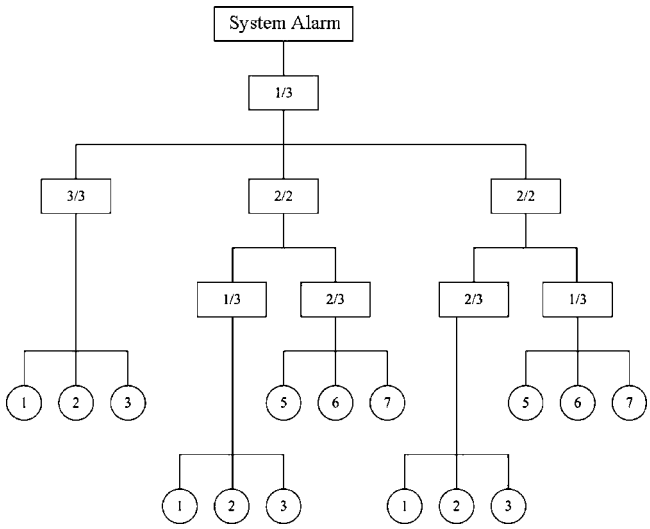

Figure 6. Alarm logic obtained in run 1.7.

system. On the other hand, run 3.6 was carried out to create a single-layer design by ignoring the temperature interlock in Figure 4. The results of these six runs are presented in Table 7. Notice that the trends in objective value and in the expected costs are in general the same as those in the previous case.

Finally, it should be noted that the failure rate of a safety valve (λ_j) in eq 70 is deliberately chosen to be slightly larger than that of a solenoid valve in Table 5. A comparison between the results obtained in run 2.2 and run 3.1 (and also between run 2.7 and run 3.6) shows that a lower objective value can be achieved in the latter case even when the safety valve in scheme B is less reliable than the solenoid valve in scheme A. Notice that scheme B is superior also in the sense that it costs less. Furthermore, it should be pointed out that more realistic failure-rate data can in fact be found in the literature, e.g., see Lees.[18] The reported value for solenoid valve is 0.42 yr^{-1} (which is less reliable than those assumed in Case 2), while that for the safety valve is 0.022 yr^{-1} (which is much more reliable than the ones adopted in Case 3). Thus, there are really no incentives to adopt the solenoid valves in pressure-relief applications in practice.

6. Conclusions

A mathematical programming approach is taken in this study to simultaneously generate the optimal protective system configurations and the corresponding maintenance policies. Several integer programs are formulated for synthesizing the single-layer and double-layer structures with or without the use of safety valves in pressure-relief applications. These programming models can be easily extended to any other multilayer systems. The feasibility and effectiveness of the proposed approach are demonstrated in this paper with three case studies. From the optimization results obtained in these studies, a number of intuitively reasonable conclusions can also be drawn:

1. The protective system design cannot always be improved by adding hardware items. The total expected expenditure reaches a minimum even without budget constraint.

2. For hazardous processes with high risks of catastrophic incidents, the use of multilayer protective structure is an efficient way to reduce the expected loss due to FD failures.

3. From the fact that the reliability of safety valves is higher than that of solenoid valves, it is always advisable to adopt the former in pressure-relief applications.

Nomenclature

$A(t)$ = availability at time t
$\bar{A}$ = average availability
$\bar{A}^{\text{Corr}}$ = average availability in corrective maintenance program
$\bar{A}^{\text{Prev}}$ = average availability in preventive maintenance program
a_i = conditional probability of FS failure of sensor$i$
b_i = conditional probability of FD failure of sensor$i$
C_a = financial loss incurred from FS failures of the protective system
C_b = financial loss incurred from FD failures of the protective system
C_{budget} = upper budget limit
$C_{\text{AL}}^{\text{LC}}$ = life-cycle cost of an alarm subsystem
$C_{\text{SD}}^{\text{LC}}$ = life-cycle cost of a shutdown subsystem
$C_{\text{AL},T}^{\text{LC}}$ = life-cycle cost of alarm subsystem in the temperature interlock
$C_{\text{SD},T}^{\text{LC}}$ = life-cycle cost of shutdown subsystem in the temperature interlock
$C_{\text{AL},P}^{\text{LC}}$ = life-cycle cost of alarm subsystem in pressure-relief system
$C_{\text{SD},P}^{\text{LC}}$ = life-cycle cost of shutdown subsystem in pressure-relief system
$\text{ENRpl}(t_1,t_2)$ = expected number of replacements during time period(t_1,t_2)
$\text{ENRpr}(t_1,t_2)$ = expected number of repairs during time period(t_1,t_2)
$f(\mathbf{y})$ = binary alarm function
H = operating life
$h(\mathbf{z})$ = binary shutdown function
$\text{InspC}_j(k-1,k)$ = inspection cost of valve j in the kth year
L_{AL} = expected loss of operating a process protected only by alarm
$L_{\text{PT},1}$ = yearly expected loss of running a process with a single-layer protective system
$L_{\text{PT},1}^{\text{LC}}$ = overall expected loss of running a process with a single-layer protective system during the entire operating life
$L_{\text{PT},2A}^{\text{LC}}$ = overall expected loss of running a process with a double-layer protective system (scheme A) during the entire operating life
$L_{\text{PT},2B}^{\text{LC}}$ = overall expected loss of running a process with a double-layer protective system (scheme B) during the entire operating life
$\text{LCC}_i^{\text{sensor}}$ = total life-cycle cost of online sensor i and its spares
$\text{LCC}_j^{\text{valve}}$ = life-cycle cost of online solenoid valve j
P_k = existence probability of state k
$P_{\text{FS}}^{\text{AL}}$ = conditional probability of FS failure of the alarm subsystem
$P_{\text{FD}}^{\text{AL}}$ = conditional probability of FD failure of the alarm subsystem
$P_{\text{FS}}^{\text{SD}}$ = conditional probability of FS failure of the shutdown subsystem
$P_{\text{FD}}^{\text{SD}}$ = conditional probability of FD failure of the shutdown subsystem
PCS_i = purchase cost of one sensor i
PCV_j = purchase cost of one solenoid valve j
p = average existence probability of an unsafe process state
$R(t)$ = reliability at time t
$\text{RplsC}_i(k-1,k)$ = replacement cost of sensor i in the kth year
$\text{RprlC}_j(k-1,k)$ = repair/replacement cost of valve j in the kth year
$\text{RprsC}_i(k-1,k)$ = repair cost of sensor i in the kth year
r = interest rate
s_j = binary variable used to denote if the jth shutdown unit is adopted for implementation
t = time
$w_{i,m}$ = binary variable used to denote if the ith online sensor is adopted and there are $m-1$spares
x = binary variable representing the process state
y_i = binary variable used to represent if sensor i detects an unsafe.process state

$\mathbf{y}$ = binary vector representing the states of Msensor outputs
z_j = binary variable used to denote if shutdown unit j performs the designated operation
$\mathbf{z}$ = binary vector representing the outcomes of operations performed by$N$shutdown units

Greek Letters

α_j = conditional probability of the FS failure of the$j$th shutdown unit
β_j = conditional probability of the FD failure of the$j$th shutdown unit
ε_i = replacement rate of sensor i
λ_i = failure rate of sensor i
λ_j = failure rate of shutdown unit j
μ_i = repair rate of sensor i
τ_j = inspection interval of shutdown unit j
FD = fails dangerously
FS = fails safely

Literature Cited

(1) Green, D. L.; Dowell III, A. M. How to Design, Verify and Validate Emergency Shutdown Systems. *ISA Trans.* **1995**, *34*, 261.

(2) Dowell III, A. M. Layer of Protection Analysis for Determining Safety Integrity Level. *ISA Trans.* **1998**, *37*, 155.

(3) Kohda, T.; Nakagawa, M. Accident Sequence Evaluation of Complex Systems with Multiple Independent Protective Systems. In *Proceedings of Reliability and Maintainability Symposium*, Alexandria, VA, Jan. 24−27, 2005; p 577.

(4) Tsai, C. S.; Chang, C. T. Optimal Alarm Logic Design for Mass Flow Networks. *AIChE J.* **1997**, *43*, 11–3021.

(5) Chang, C. T.; Tsai, C. S.; Chen, K. H. Resilient Alarm Logic Design for Process Networks. *Ind. Eng. Chem. Res.* **2000**, *39*, 4974.

(6) Lai, C. A.; Chang, C. T.; Ko, C. L.; Chen, C. L. Optimal Sensor Placement and Maintenance Strategies for Mass-Flow Networks. *Ind. Eng. Chem. Res.* **2003**, *42*, 4366.

(7) Vaurio, J. K. Optimization of Test and Maintenance Intervals Based on Risk and Cost. *Reliab. Eng. Syst. Saf.* **1995**, *49*, 23.

(8) Vaurio, J. K. Availability and Cost Functions for Periodically Inspected Preventively Maintained Unit. *Reliab. Eng. Syst. Saf.* **1999**, *63*, 133.

(9) Badia, F. G.; Berrade, M. D.; Campos, C. A. Optimization of Inspection Intervals Based on Cost. *J. Appl. Probab.* **2001**, *38*, 872.

(10) Badia, F. G.; Berrade, M. D.; Campos, C. A. Optimal Inspection and Preventive Maintenance of Units with Revealed and Unrevealed Failures. *Reliab. Eng. Syst. Saf.* **2002**, *78*, 157.

(11) Duarte, J. A. C.; Craveiro, J. C. T. A.; Trigo, T. P. Optimization of the Preventive Maintenance Plan of a Series Components System. *Int. J. Pressure Vessels Piping* **2006**, *83*, 244.

(12) Andrews, J. D.; Bartlett, L. M. A Branching Search Approach to Safety System Design Optimization. *Reliab. Eng. Syst. Saf.* **2005**, *87*, 23.

(13) Hoyland, A.; Rausand, M. *System Reliability Theory: Models and Statistical Methods*; John Wiley & Sons: New York, 1994.

(14) Henley, E. J.; Kumamoto, H. *Reliability Engineering and Risk Assessment*; Prentice-Hall: Englewood Cliffs, NJ, 1981.

(15) Henley, E. J.; Kumamoto, H. *Designing for Reliability and Safety Control*; Prentice-Hall: Englewood Cliffs, NJ, 1985.

(16) Sasaki, M.; Kaburaki, S.; Yanagi, S. System Availability and Optimum Spare Units. *IEEE Trans. Reliab.* **1977**, *R-26*, 182.

(17) Henley, E. J.; Kumamoto, H. *Probabilistic Risk Assessment: Reliability Engineering, Design, and Analysis*; IEEE Press: New York, 1992.

(18) Lees, F. P. *Loss Prevention in the Process Industries*, 1st ed.; Butterworths: London, 1986.

Received for review September 2, 2007
Revised manuscript received April 10, 2008
Accepted April 14, 2008

IE071188Z