Design and Maintenance of Multichannel Protective Systems

Yue-Cheng Liao and Chuei-Tin Chang*

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

To mitigate the undesirable effects caused by accidents in chemical plants, it is a common practice to install protective systems on processing units operated under hazardous conditions. Because hardware failures are basically random events, the availability of the protective system is highly dependent on its structural properties and also the maintenance programs. The aim of this study is to improve and generalize the current practice[1] for generating the design specifications and maintenance policies. Specifically, instead of monitoring only a single condition, in this work, the emergency system status is detected according to the measurements of several different process variables (or "alarm channels") so as to optimize alarm performance. Because each of these channels can be consist of more than one online sensor, a modified version of the spare-supported corrective maintenance policy is also devised in this study to enhance availability. By solving the corresponding mathematical programming model, the optimal configurations of sensors and shutdown units, the best corrective and preventive maintenance procedures, and alarm/shutdown logic can all be identified automatically. Two examples are provided in this article to demonstrate the feasibility and effectiveness of the proposed approach.

1. Introduction

For the purpose of guarding against the catastrophic consequences of accidents in chemical plants, elaborate protective systems might have to be installed on units that are operated under extreme process conditions. Because hardware failures are inevitable but random, the reliability (or availability) of such a system is highly dependent on its structural characteristics and also the corresponding maintenance policies. A sequential approach is traditionally taken to specify and analyze every interlock or trip system in process design. In particular, the protective structure and also its maintenance policy are first synthesized on the basis of past experience. The corresponding financial implications (i.e., the capital investments; expected losses due to malfunctions; and expected maintenance costs for inspections, replacements, and repairs) are then estimated accordingly. Notice that these design and evaluation tasks might have to be performed repeatedly on a trial-and-error basis before reaching a satisfactory final solution. Because this ad hoc approach is clearly tedious and error-prone, suitable computer aids are needed to streamline the aforementioned procedures.

Generally speaking, a protective system is used to perform two basic functions, namely, alarm and shutdown. The former is facilitated by one or more independent sensors. Based on online measurements obtained with these sensors, a predetermined logic can be applied to determine whether an alarm should be set off. The latter function is usually fulfilled with solenoid valves or power switches. In response to the alarm decision, the solenoid valves can be either energized or de-energized to realize the shutdown actions. Similarly, the shutdown operations can be performed by switching off the power supply in certain applications. A brief review of the current approaches for configuring alarm and shutdown subsystems is presented in the following.

It should be noted first that both spurious and detrimental alarm failures are considered in this work. In particular, it is assumed that the hazard detection function in a protective system can fail either safely (FS) or dangerously (FD). The former malfunctions are recoverable because they can usually be attributed to noisy measurement signals, whereas the latter often require repair or replacement. To achieve a desired availability level, a common practice in the process industries is to introduce hardware redundancy in protective system design. Specifically, each critical process condition is monitored with more than one sensor, and the resulting alarm decision is then made by feeding all online measurement signals to a voting device. Tsai and Chang[2] and Chang et al.[3] developed a statistics-based alarm strategy using redundant online process data. In addition, notice that the system availability of a sensor network can also be enhanced with a corrective maintenance approach, that is, every online sensor is repaired or replaced immediately after a failure is detected. By using this strategy, Lai et al.[4] developed a novel maintenance management program (with spares) for improving sensor availability and also the reliability of the alarm-generation mechanism.

On the other hand, it should be pointed out that shutdown equipment can experience FD failures also. Because these failures are not detectable under normal conditions, a preventive maintenance strategy must be applied to enhance availability. More specifically, all shutdown units are required to be inspected regularly at constant time intervals to determine whether there are unrevealed faulty conditions. Broken valves or switches must be replaced or repaired as soon as they are identified, whereas the normal ones should be allowed to stay online after inspection. Thus, the length of the inspection interval should be regarded as a critical parameter in stipulating a preventive maintenance policy. Vaurio[5] suggested that the optimal lengths must be determined so as to minimize the cost rate or accident rate of a given system. The same author later[6] modified this strategy by incorporating the age-replacement mechanism, that is, every component is replaced after a fixed number of inspections and/or repairs even if it is still functional. Badia et al.[7] assumed that all failures in a given system are unrevealed and developed a computation procedure to determine the cost-optimal inspection interval. They then extended this approach in a subsequent study[8] to other systems in which both revealed and unrevealed failures might be present. Finally, Duarte et al.[9] optimized the preventive maintenance plan of a series system to achieve the minimum cost rate under the assumptions that

* To whom correspondence should be addressed. E-mail: ctchang@mail.ncku.edu.tw. Tel: 886-6-2757575 ext. 62663. Fax: 886-6-2344496.

10.1021/ie901818e
Published on Web 10/21/2010

the repair rate is constant and that both the hazard rate and failure rate increase linearly with time.

Because a sequential approach cannot properly address the tradeoff issues, there have been a few attempts in the past to generate the optimal configurations and/or the corresponding maintenance policies simultaneously with a mathematical programming model. Andrews and Bartlett[10] 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 method. To circumvent these drawbacks, Liang and Chang[1] developed an integer programming model to minimize the expected expenditure of assembling and operating a multilayer protective system. From the optimal solution, the following important design and maintenance specifications were identified: (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, because the sensors and valves in the protective systems were assumed to be maintained with the appropriate corrective and preventive strategies, the optimal number of spare sensors stored off-line and the best inspection interval for each valve were also determined by their model.

Although the above-mentioned model is applicable in simple cases, further improvement is still needed. In particular, it should be noted that the alarm function in each layer of a realistic protective system is often multichanneled. For example, more than one safety interlock, each measuring a distinct variable, might be installed to stop the compressor in an industrial refrigeration system so as to prevent surging.[11] This unique multichanneled protection feature is often needed in complex practical applications mainly for the purpose of producing a balanced assessment of the system state. Therefore, the main objective of the present study is to improve and generalize the available model[1] for producing the design specifications and maintenance policies of protective systems. More specifically, instead of monitoring only one single condition, the emergency status of given system is detected according to the measurements of several different process variables so as to optimize alarm performance. Because each of these alarm channels can be assembled with more than one online sensor, an improved version of the spare-supported corrective maintenance policy is also devised in this study to enhance availability. By solving the improved mathematical programming model, the optimal configurations of sensors and shutdown units, the best corrective and preventive maintenance policies, and alarm/shutdown logic can all be identified automatically.

2. Maintenance of Critical Components

As mentioned previously, a single-layer protective system can be further divided into alarm and shutdown subsystems. The sensors in the former subsystem and the solenoid valves (or power switches) in the latter are the most critical components that require rigorous maintenance. Detailed descriptions of the proposed strategies are presented in the following subsections.

2.1. Sensors. As mentioned previously, the corrective maintenance policy should be applied to the revealed failures that are unrecoverable. In particular, repair must be 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 for the availability and the expected numbers of repairs and replacements within a specified time period must be obtained first. Because they can be found in standard textbooks (e.g., Hoyland and Rausand),[12] these formulas are listed below without detailed derivations.

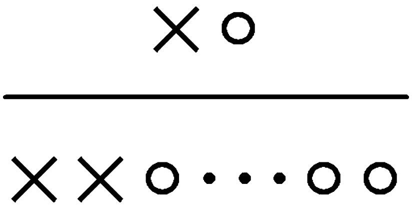

Figure 1. System state of an alarm channel.

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[12]

$$\mathrm{Av}(t) = \frac{\mu}{\mu + \lambda} + \frac{\lambda}{\mu + \lambda}\mathrm{e}^{-(\mu+\lambda)t} \tag{1}$$

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

$$\overline{\mathrm{Av}} = \lim_{\theta \to \infty} \frac{\int_0^\theta \mathrm{Av}(\eta)\,\mathrm{d}\eta}{\theta} = \mathrm{Av}(\infty) \tag{2}$$

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.[13]

$$\mathrm{ENRpr}[t_1, t_2] \approx \frac{\mu\lambda}{\mu + \lambda}(t_2 - t_1) \tag{3}$$

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

To ensure high integrity in a multichannel alarm structure, the spare-supported program proposed by Liang and Chang[1] has been improved and generalized in the present study to maintain the sensors in each and every channel. This comprehensive corrective maintenance strategy can be summarized as follows:

(i) A total of m identical sensors are purchased for measuring a particular process condition in an alarm channel. n of them are installed online, whereas the remaining $m - n$ sensors are stored off-line and treated as spares. Notice that $1 \le n \le m$. It is also assumed that a normal spare sensor can never fail.

(ii) If an online sensor fails and at least one spare is functional, then replace the former with the latter immediately. The failed sensor is taken off-line and then placed in a queue for repair.

(iii) The repair process of the failed off-line sensors is in effect only when all online sensors are working. It is also assumed that these failed sensors can be repaired only one at a time in sequence.

(iv) The repair process of the failed online sensors can take place only if none of the off-line sensors are functional. It is again assumed that these failed sensors can only be repaired sequentially.

In this article, the system state of an alarm channel is represented with a special notation. An example can be found in Figure 1, in which the working and failed sensors are denoted as "○" and "×", respectively. The online sensor states are specified in the top row, whereas the states of spares are given

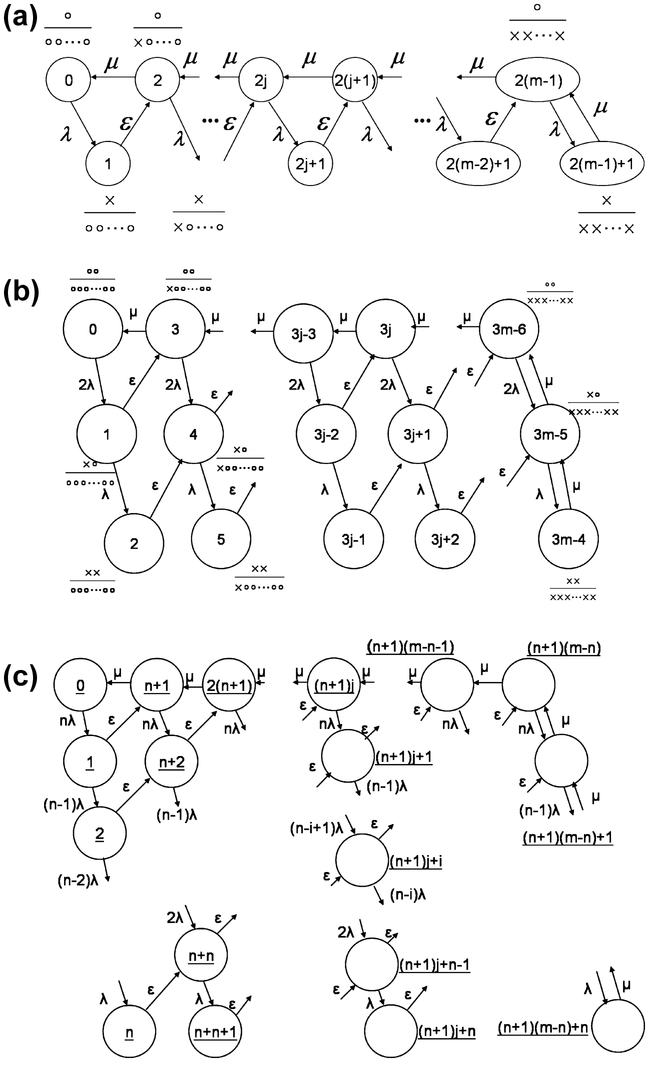

Figure 2. Markov diagrams of (a) a spare-supported corrective maintenance program for an alarm channel with $n = 1$, (b) a spare-supported corrective maintenance program for an alarm channel with $n = 2$, (c) a generalized spare-supported corrective maintenance program for an alarm channel.

at the bottom. Figure 2a is the Markov diagram (or state transition diagram) of the proposed maintenance system with a single online sensor. 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 with the notation described in Figure 1. Notice that the transition rates are marked next to the connecting arcs. In particular, λ, μ, and ε denote the failure rate, repair rate, and replacement rate, respectively, for a single sensor. This representation of the maintenance system can be extended to $n = 2$ in Figure 2b and to the generalized case in Figure 2c. Notice that the overall failure rate of each node equals $n_{\text{ol}}\lambda$, where n_{ol} is the number of working online sensors.

According to the connection structure of the generalized Markov diagram, the system states can be divided into seven blocks, as shown in Figure 3. Let us further assume that the entire operating period is long enough that the steady-state probabilities of all of the states can be reached within a relatively short time period. These probabilities are related by a set of state equations derived according to the Markov diagrams in Figures 2 and 3.[14] To further clarify this point, let us consider a specific example when $m = 4$ and $n = 1$. The corresponding steady-state relations can be derived according to the state transition diagram given in Figure 4.

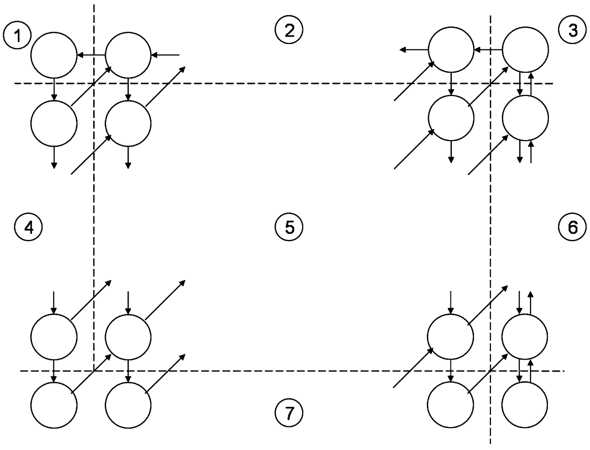

Figure 3. Classification of system states in a generalized Markov diagram.

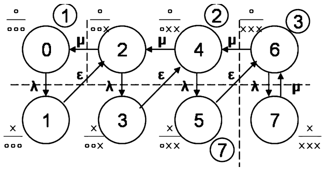

Figure 4. Markov diagram of a spare-supported corrective maintenance program for an alarm channel ($m = 4$, $n = 1$).

For node 0 in block 1

$$P_2 = \frac{\lambda}{\mu}P_0 \tag{4}$$

For nodes 2 and 4 in block 2

$$P_4 = \frac{\mu + \lambda}{\mu}P_2 - \frac{\varepsilon}{\mu}P_1 \tag{5}$$

$$P_6 = \frac{\mu + \lambda}{\mu}P_4 - \frac{\varepsilon}{\mu}P_3 \tag{6}$$

For node 6 in block 3

$$P_7 = \frac{\mu + \lambda}{\mu}P_6 - \frac{\varepsilon}{\mu}P_5 \tag{7}$$

For nodes 1, 3, and 5 in block 7

$$P_1 = \frac{\lambda}{\varepsilon}P_0 \tag{8}$$

$$P_3 = \frac{\lambda}{\varepsilon}P_2 \tag{9}$$

$$P_5 = \frac{\lambda}{\varepsilon}P_4 \tag{10}$$

These formulas have been generalized to any combination of m and n ($m \geq n$) and a complete listing can be found in Appendix I. It is clear from eqs 4–10 and also from the combinations presented in Appendix I that all probabilities can be expressed as a linear function of P_0. Notice that the sum of all probabilities should be unity, that is

$$\sum_{k=0}^{(n+1)(m-n)+n} P_k = 1 \tag{11}$$

Thus, the steady-state probability at node 0 can be determined with a formula derived by substituting all equations in Appendix I into eq 11, and all other probabilities can then be computed accordingly.

It is assumed in this study that a k-out-of-n voting gate is used in each channel for triggering an alarm. Specifically, the channel issues an alarm if at least k out of the n online sensors detect an unsafe condition. The limiting (or average) availability can then be computed accordingly as

$$\mathrm{Av}(\infty) = \overline{\mathrm{Av}}^{\mathrm{Corr}} = \sum_{j=0}^{m-n}\sum_{i=0}^{k-1} P_{j(n+1)+i} \tag{12}$$

The expected numbers of repairs and replacements per year can also be approximated with the aforementioned steady-state probabilities as

$$\mathrm{ENRpr}(m, n) \approx \mu\left(\sum_{j=1}^{m-n} P_{j(n+1)} + \sum_{i=1}^{n} P_{(m-n)(n+1)+i}\right) \tag{13}$$

$$\mathrm{ENRpl}(m, n) \approx \varepsilon \sum_{j=0}^{m-n-1}\sum_{i=1}^{n} P_{j(n+1)+i} \tag{14}$$

Note that these expected numbers depend on the values of m and n chosen for the alarm channel.

2.2. Shutdown Units. As mentioned previously, the FD failures of passive components, such as solenoid valves, safety valves, and rupture discs, used in a protective system generally cannot be observed online, and such failures are often referred to as the unrevealed or hidden failures. It is therefore necessary to adopt a preventive maintenance scheme to bring down the unavailability of a shutdown subsystem to an acceptable level. In this study, the required maintenance tasks are restricted to those associated with the periodic inspection, repair, and replacement of every passive component. After inspection (and possible later repair or replacement), the component is considered to be "as good as new".

Under the assumptions given above, it is obvious that the availability of a shutdown unit at a time between inspections should be the same as the reliability of a nonrepairable component,[12] that is

$$\mathrm{Av}(t) = \mathrm{e}^{-\lambda(t-k\tau)}, \quad k\tau \le t < (k+1)\tau \tag{15}$$

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

$$\overline{\mathrm{Av}}^{\mathrm{Prev}} = \frac{1}{\lambda\tau}(1 - \mathrm{e}^{-\lambda\tau}) \tag{16}$$

3. General Framework of a Protected System

The general structure of a protected process is sketched in Figure 5.

A binary variable $\xi \in \{0,1\}$ is used here to denote whether a particular unsafe process state is present, that is

$$\xi = \begin{cases} 1 & \text{if the process is in a specific unsafe state} \\ 0 & \text{otherwise} \end{cases} \tag{17}$$

Usually, this dangerous process state is reflected in several different process variables, such as temperature, pressure, and flow rate. A binary vector $\mathbf{x} = [x_1\ x_2 \cdots x_M]^{\mathrm{T}}$ is used in this work to characterize the actual values of these variables, that is

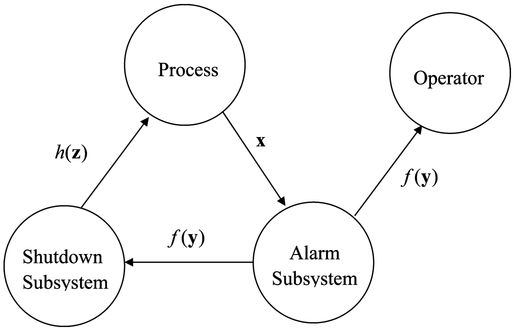

Figure 5. General structure of a protected process.

$$x_i = \begin{cases} 1 & \text{if the } i\text{th process variable exceeds the specified safety limit} \\ 0 & \text{otherwise} \end{cases} \tag{18}$$

It is assumed that every process variable is measured with one or more online sensor of identical specifications in an alarm channel. The channel outputs also form a binary vector, $y = [y_1\ y_2 \cdots y_M]^{\mathrm{T}}$ and $y_1, y_2, ..., y_M \in \{0,1\}$, indicating whether the unsafe state is detected. A logic operation can then be applied to these binary values to determine whether an alarm should be set off. This logic can be expressed with an alarm function $f(\mathbf{y})$

$$f(\mathbf{y}) = \begin{cases} 1 & \text{if the alarm subsystem sets off an alarm} \\ 0 & \text{otherwise} \end{cases} \tag{19}$$

A sketch of this multichannel alarm structure can be found in Figure 6a,b. Notice that the synthesis of alarm-generation logic is one of the basic tasks in designing a protective system. In particular, the values of the alarm function should be properly assigned for all possible $\mathbf{y}$, and if possible, the explicit function form of $f(\mathbf{y})$ should also be identified. Once this unique mapping between $\mathbf{y}$ and $f(\mathbf{y})$ has been established, the corresponding logic can be implemented either as a hard-wired circuit or as a computer program.

Depending on the process needs, the alarm signal can 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 vector $\mathbf{z}$ is used to denote whether the designated emergency-response operations are executed by the shutdown units. More specifically

$$z_j = \begin{cases} 1 & \text{if the } j\text{th shutdown unit completes the designated operation} \\ 0 & \text{otherwise} \end{cases} \tag{20}$$

where $j = 1, 2, ..., N$. Because a protective system is needed mainly to guard against hazardous FD failures, it is assumed that OR logic is always adopted to configure the shutdown subsystems. We define a binary shutdown function accordingly as

$$h(\mathbf{z}) = \begin{cases} 1 & \text{if the subsystem performs the shutdown operation successfully} \\ 0 & \text{otherwise} \end{cases} \tag{21}$$

This function can thus be written explicitly as

$$h(\mathbf{z}) = 1 - \prod_{j=1}^{N}(1 - z_j) \tag{22}$$

A sketch of this standard shutdown structure can be found in Figure 7.

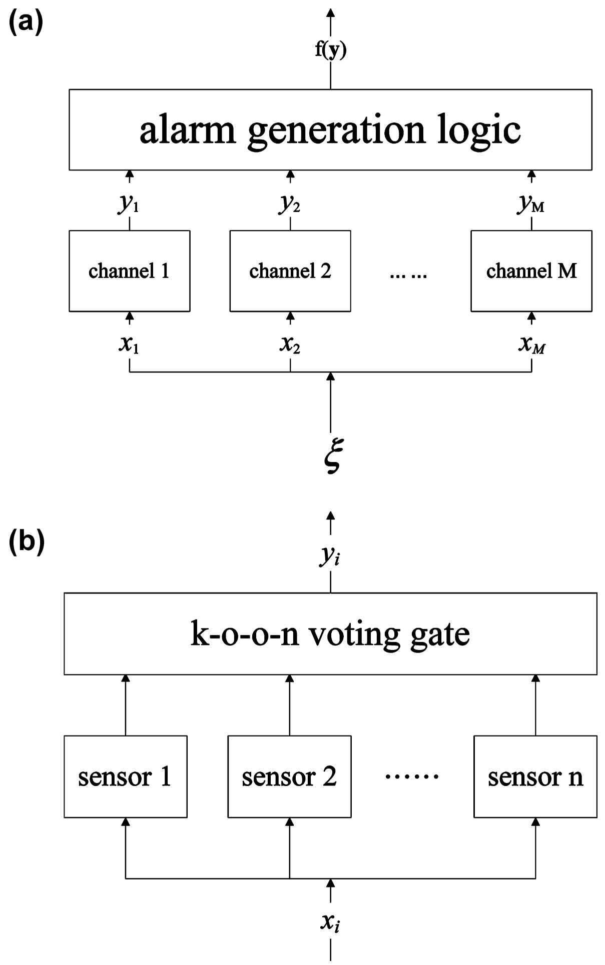

Figure 6. (a) Alarm subsystem, (b) *k*-out-of-*n* voting gate.

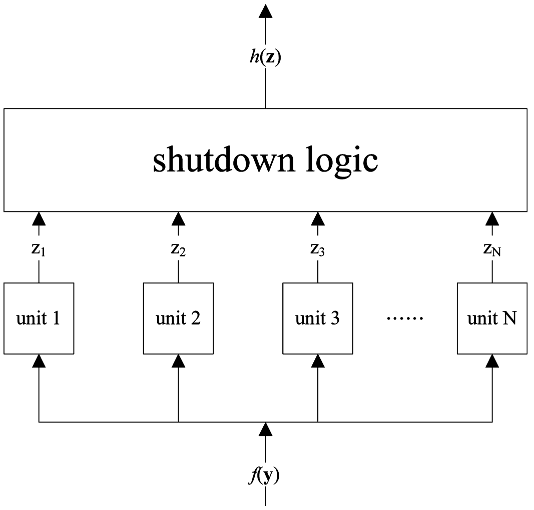

Figure 7. Shutdown subsystem.

4. Total Expected Loss of Protective System

If p denotes the average probability of a given unsafe process state in one year, it can be expressed as

$$p = \Pr\{\xi = 1\} \tag{23}$$

Also, let A_i and B_i represent the conditional probabilities of FS and FD failures, respectively, of the ith alarm channel

$$\begin{aligned} A_i &= \Pr\{y_i = 1|\xi = 0\} \\ B_i &= \Pr\{y_i = 0|\xi = 1\} \end{aligned} \tag{24}$$

If a k-out-of-n voting gate is used to trigger the alarm, the FS probability of channel i can be written as

$$A_i = 1 - (1 - a_i^k)^{n!/k!} \tag{25}$$

where a_i is the FS probability of a single sensor in the ith channel and is regarded as a given model parameter in this work. On the other hand, the FD probability of channel i can be determined with the equation

$$B_i = 1 - \overline{\mathrm{Av}}_i^{\mathrm{Corr}} \tag{26}$$

where $\overline{\mathrm{Av}}_i^{\mathrm{Corr}}$ is the average availability of the ith alarm channel. Notice that this value is computed according to eq 12 and can be adjusted by varying the total number of purchased sensors (m), the number of online sensors (n), and the voting-gate parameter (k).

It was shown by Henley and Kumamoto[13−15]that the conditional probabilities of the FS and FD failures of the alarm subsystem can be written as

$$\begin{aligned} P_{\mathrm{FS}}^{\mathrm{AL}} &= \Pr\{f(\mathbf{y}) = 1|\xi = 0\} = \sum_{\mathbf{y}} f(\mathbf{y}) \Pr\{\mathbf{y}|\xi = 0\} \\ P_{\mathrm{FD}}^{\mathrm{AL}} &= \Pr\{f(\mathbf{y}) = 0|\xi = 1\} = \sum_{\mathbf{y}} [1 - f(\mathbf{y})]\Pr\{\mathbf{y}|\xi = 1\} \end{aligned} \tag{27}$$

If the shutdown subsystem is always functional, the expected loss of operating the given process in this situation can be formulated as

$$\begin{aligned} L_{\mathrm{AL}} &= C_{\mathrm{a}}\Pr\{\xi = 0\}P_{\mathrm{FS}}^{\mathrm{AL}} + C_{\mathrm{b}}\Pr\{\xi = 1\}P_{\mathrm{FD}}^{\mathrm{AL}} \\ &= C_{\mathrm{b}}p - \sum_{\mathbf{y}} f(\mathbf{y})\, g(\mathbf{y}) \end{aligned} \tag{28}$$

where

$$g(\mathbf{y}) = C_{\mathrm{b}}p\Pr\{\mathbf{y}|\xi = 1\} - C_{\mathrm{a}}(1 - p)\Pr\{\mathbf{y}|\xi = 0\} \tag{29}$$

In eqs 28 and 29, C_{a} and C_{b} denote the financial losses incurred from FS and FD failures, respectively, of the protective system. If the outputs of alarm channels are statistically independent, the conditional probabilities in the above equations (i.e., $\Pr\{\mathbf{y}|\xi = 0\}$ and $\Pr\{\mathbf{y}|\xi = 1\}$) can be transformed into functions of A_i and B_i, respectively, that is

$$\begin{aligned} \Pr\{\mathbf{y}|\xi = 0\} &= \prod_{i=1}^{M} \Pr\{y_i|\xi = 0\} = \prod_{i=1}^{M} [A_i^{y_i}(1 - A_i)^{1-y_i}] \\ \Pr\{\mathbf{y}|\xi = 1\} &= \prod_{i=1}^{M} \Pr\{y_i|\xi = 1\} = \prod_{i=1}^{M} [B_i^{1-y_i}(1 - B_i)^{y_i}] \end{aligned} \tag{30}$$

To facilitate comprehensive protective system designs, let us consider all possible failure scenarios (see Figure 8). The FS and FD failures of the entire protective system can obviously be attributed to the failures in subsystems. In particular, scenarios 2 and 4 can be classified as FS system failures, whereas scenarios 5 and 7 are FD system failures. The probabilities that both subsystems fail simultaneously (i.e., scenarios 3 and 6) are assumed to be negligibly low and are thus ignored in the

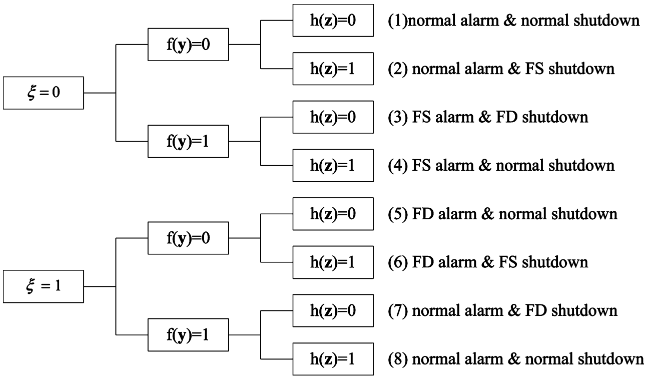
ξ = 0
ξ = 1
f(y)=0
f(y)=1
f(y)=0
f(y)=1
h(z)=0
h(z)=1
h(z)=0
h(z)=1
h(z)=0
h(z)=1
h(z)=0
h(z)=1
(1)normal alarm & normal shutdown
(2) normal alarm & FS shutdown
(3) FS alarm & FD shutdown
(4) FS alarm & normal shutdown
(5) FD alarm & normal shutdown
(6) FD alarm & FS shutdown
(7) normal alarm & FD shutdown
(8) normal alarm & normal shutdown

Figure 8. All possible failure scenarios of a protective system.

present study. Consequently, the expected yearly loss (due to FS and FD system failures) can be expressed as[13,14]

$$L_{\rm PT} = C_{\rm a}(1-p)\sum_{\mathbf{y}}\Pr\{\mathbf{y}|\xi=0\}\phi_{\rm a}(\mathbf{y}) + C_{\rm b}p\sum_{\mathbf{y}}\Pr\{\mathbf{y}|\xi=1\}\phi_{\rm b}(\mathbf{y}) \quad (31)$$

where

$$\phi_{\rm a}(\mathbf{y}) = (1-P_{\rm FD}^{\rm SD})f(\mathbf{y}) + P_{\rm FS}^{\rm SD}[1-f(\mathbf{y})] \quad (32)$$

$$\phi_{\rm b}(\mathbf{y}) = (1-P_{\rm FS}^{\rm SD})[1-f(\mathbf{y})] + P_{\rm FD}^{\rm SD}f(\mathbf{y}) \quad (33)$$

According to eqs 21 and 22, the conditional probabilities of FS and FD failures of the shutdown subsystem can be expressed as

$$P_{\rm FS}^{\rm SD} = \Pr\{h(\mathbf{z})=1|f(\mathbf{y})=0\} = 1-\prod_{j=1}^{N}(1-\alpha_j) \quad (34)$$

$$P_{\rm FD}^{\rm SD} = \Pr\{h(\mathbf{z})=0|f(\mathbf{y})=1\} = \prod_{j=1}^{N}\beta_j \quad (35)$$

where α_j and β_j denote the conditional probabilities of FS and FD failures, respectively, of the jth shutdown unit. In the present study, α_j is also regarded as a given model parameter and

$$\beta_j = 1-\overline{\rm Av}_j^{\rm Prev} \quad (36)$$

where $\overline{\rm Av}_j^{\rm Prev}$ is the average availability of the jth shutdown unit. Notice that this value can be computed according to eq 16 and can be manipulated by changing the inspection interval τ_j.

By substituting eqs 23, 24, 30, and 32−35 into eq 31, one can then obtain the following compact expression of the expected loss for operating the protective system

$$L_{\rm PT} = (1-P_{\rm FS}^{\rm SD})C_{\rm b}p - P_{\rm FS}^{\rm SD}C_{\rm a}(1-p) - (1-P_{\rm FS}^{\rm SD}-P_{\rm FD}^{\rm SD})\sum_{\mathbf{y}}f(\mathbf{y})\,g(\mathbf{y}) \quad (37)$$

Notice that the definition of the function $g(\mathbf{y})$ in this equation has already been given in eqs 29 and 30. The overall expected loss of a 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 life-cycle loss ($L_{\rm PT}^{\rm LC}$) can be expressed as

$$L_{\rm PT}^{\rm LC} = \sum_{k=1}^{H}\frac{L_{\rm PT}(k-1,k)}{(1+r)^{k-1}} \quad (38)$$

where $L_{\rm PT}(k-1,k)$ denotes the expected loss in the kth year and r is the interest rate. It is assumed in this study that the probability of the system being in a particular unsafe 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, $L_{\rm PT}^{\rm LC}$ can be computed according to eq 37 by replacing the costs of FS and FD failures (i.e., $C_{\rm a}$ and $C_{\rm b}$, respectively) with the following life-cycle cost parameters

$$C_{\rm a}^{\rm LC} = \sum_{k=1}^{H}\frac{C_{\rm a}(k-1,k)}{(1+r)^{k-1}} \quad (39)$$

$$C_{\rm b}^{\rm LC} = \sum_{k=1}^{H}\frac{C_{\rm b}(k-1,k)}{(1+r)^{k-1}} \quad (40)$$

where $C_{\rm a}(k-1,k)$ and $C_{\rm b}(k-1,k)$ represent the costs of FS and FD failures, respectively, in the kth year.

5. Life-Cycle Costs of Critical Components

Because the spare-supported corrective maintenance policy is employed in this work to improve the availability of every alarm channel, the related expenditures can be divided into three parts: (a) the purchase cost, (b) the expected repair cost, and (c) the expected replacement cost. The total life-cycle cost of every alarm channel can therefore be expressed as

$${\rm LCC}_i^{\rm AL} = m{\rm PCS}_i + {\rm ENRpr}_i(m,n)H\overline{{\rm RprsC}_i} + {\rm ENRpl}_i(m,n)H\overline{{\rm RplsC}_i} \quad (41)$$

where ${\rm PCS}_i$ denotes the purchase cost of one sensor in channel i and $\overline{{\rm RprsC}_i}$ and $\overline{{\rm RplsC}_i}$ denote the average repair and replacement costs, respectively. These average costs are defined as

$$\overline{{\rm RprsC}_i} = \frac{1}{H}\sum_{k=1}^{H}\frac{{\rm RprsC}_i(k-1,k)}{(1+r)^{k-1}} \quad (42)$$

$$\overline{{\rm RplsC}_i} = \frac{1}{H}\sum_{k=1}^{H}\frac{{\rm RplsC}_i(k-1,k)}{(1+r)^{k-1}} \quad (43)$$

where ${\rm RprsC}_i(k-1,k)$ and ${\rm RplsC}_i(k-1,k)$ represent the repair and replacement costs, respectively, of channel i in the kth year. From eqs 13 and 14, it is obvious that the expected numbers of repairs and replacements per year [i.e., ${\rm ENRpr}_i(m,n)$ and ${\rm ENRpl}_i(m,n)$] can be manipulated by adjusting the total number of purchased sensors m and the number of installed online sensors n.

On the other hand, because 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, we assume that the length of the inspection interval for each shutdown unit (τ_j) can be only an integer number of months. Specifically, the life-cycle cost associated with a shutdown unit can be written as

$$\mathrm{LCC}_j^{\mathrm{SD}} = \mathrm{PCV}_j + \frac{12}{\tau_j}H\overline{\mathrm{InspC}}_j + \frac{12}{\tau_j}(1 - \mathrm{e}^{-\lambda_j\tau_j/12})H\overline{\mathrm{RprlC}}_j \tag{44}$$

where PCV_j denotes the purchase cost of shutdown unit j and $\overline{\mathrm{InspC}}_j$ and $\overline{\mathrm{RprlC}}_j$ represent the average inspection and repair (replacement) costs, respectively. Notice that the average inspection and repair (replacement) costs can be defined as

$$\overline{\mathrm{InspC}}_j = \frac{1}{H}\sum_{k=1}^{H}\frac{\mathrm{InspC}_j(k-1,k)}{(1+r)^{k-1}} \tag{45}$$

$$\overline{\mathrm{RprlC}}_j = \frac{1}{H}\sum_{k=1}^{H}\frac{\mathrm{RprlC}_j(k-1,k)}{(1+r)^{k-1}} \tag{46}$$

where $\mathrm{InspC}_j(k-1,k)$ and $\mathrm{RprlC}_j(k-1,k)$ represent the inspection and repair (or replacement) costs, respectively, in the kth year.

6. Integer Program

As mentioned before, the expected expenditures associated with a protective system can be divided into three categories: (a) the purchase cost of the alarm subsystem and its expected repair and replacement expenditures, (b) the purchase and inspection costs of the 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 of these expenditures is used as the objective function.

Let us first consider the purchase and maintenance costs of the alarm subsystem. Because the exact alarm structure is unknown before the optimization problem is solved, the binary variable $w_{i,m,n,k}$ is employed in the mathematical programming model to characterize design specifications. More specifically, $w_{i,m,n,k} = 1$ indicates that the ith channel is employed and that, in this channel, there are m purchased sensors, n online sensors, and a k-out-of-n voting gate, whereas $w_{i,m,n,k} = 0$ means otherwise. Because at most one of the above options can be selected for every channel, the following inequality constraint must be used to stipulate such a requirement

$$\sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k} \le 1 \tag{47}$$

where Ω_i is the maximum allowable number of purchased sensors for the ith channel. It should be noted that this formulation accommodates the possibility of not incorporating the ith channel in the alarm logic, that is, $\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k} = 0$ for $m = 1, 2, ..., \Omega_i$. In addition, because it is sometimes desirable to ensure that at least one channel is included in the alarm subsystem, another inequality constraint can be added to the model

$$\sum_{i=1}^{M}\sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k} \ge 1 \tag{48}$$

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

$$C_{\mathrm{AL}}^{\mathrm{LC}} = \sum_{i=1}^{M}\sum_{m=1}^{\Omega_i}\sum_{n\le m}\Big(\sum_{k\le n} w_{i,m,n,k}\Big)(C_{i,m}^{\mathrm{PC}} + C_{i,m,n}^{\mathrm{Rpr}} + C_{i,m,n}^{\mathrm{Rpl}}) \tag{49}$$

In this equation, the three different types of costs can be determined with the equations

$$C_{i,m}^{\mathrm{PC}} = m\mathrm{PCS}_i \tag{50}$$

$$C_{i,m,n}^{\mathrm{Rpr}} = \mathrm{ENRpr}_i(m,n)H\overline{\mathrm{RprsC}}_i \tag{51}$$

$$C_{i,m,n}^{\mathrm{Rpl}} = \mathrm{ENRpl}_i(m,n)H\overline{\mathrm{RplsC}}_i \tag{52}$$

We next consider the purchase and maintenance costs associated with a shutdown subsystem. Because 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 the jth unit is selected for online implementation, that is

$$s_j = \begin{cases} 1 & \text{if the } j\text{th shutdown unit is selected for implementation} \\ 0 & \text{otherwise} \end{cases} \tag{53}$$

Again, because of the need to incorporate at least one shutdown unit, it is necessary to impose the constraint

$$\sum_{j=1}^{N} s_j \ge 1 \tag{54}$$

The total life-cycle cost of a shutdown subsystem can then be expressed with the aid of these binary variables as

$$C_{\mathrm{SD}}^{\mathrm{LC}} = \sum_{j=1}^{N} s_j\Big[\mathrm{PCV}_j + \frac{12}{\tau_j}H\overline{\mathrm{InspC}}_j + (1 - \mathrm{e}^{-\lambda_j\tau_j/12})\frac{12}{\tau_j}H\overline{\mathrm{RprlC}}_j\Big] \tag{55}$$

Finally, we consider the expected loss given in eq 37. 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_j. In other words, eqs 34 and 35 should be rewritten to account for the possibility of excluding one or more unit, that is

$$P_{\mathrm{FS}}^{\mathrm{SD}} = 1 - \prod_{j=1}^{N}(1 - \alpha_j s_j) \tag{56}$$

$$P_{\mathrm{FD}}^{\mathrm{SD}} = \prod_{j=1}^{N}\beta_j^{s_j} \tag{57}$$

From eqs 29, 30, and 37, it is clear that the function $g(\mathbf{y})$ must be reformulated in terms of the binary variables $w_{i,m,n,k}$. Specifically, eq 30 should be modified as

$$\Pr\{\mathbf{y}|\xi = 0\} = \prod_{i=1}^{M}\left[\begin{array}{l}\displaystyle\sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k}A_i^{y_i}(1 - A_i)^{1-y_i} + \\ \displaystyle(1 - y_i)(1 - \sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k})\end{array}\right]$$

$$\Pr\{\mathbf{y}|\xi = 1\} = \prod_{i=1}^{M}\left[\begin{array}{l}\displaystyle\sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k}B_i^{1-y_i}(1 - B_i)^{y_i} + \\ \displaystyle(1 - y_i)(1 - \sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k})\end{array}\right] \tag{58}$$

Table 1. Optimization Results for Example 1, Part 1: Multichannel Alarm Configuration

	case no.						
	1-1	1-2	1-3	1-4	1-5	1-6	1-7
initial budget (rcu)	10000	1800	1700	1600	850	750	650
objective value (rcu)	11742	11805	12027	13210	13240	14196	15123
purchase cost (rcu)	1850	1750	1650	900	800	700	600
maintenance cost (rcu)	1887	1865	1791	1609	1609	1608	1520
voting gate of channel 1	2oo2	2oo2	2oo2	–	–	–	–
number of spares in channel 1	1	1	1	–	–	–	–
voting gate of channel 2	3oo3	3oo3	2oo2	2oo2	2oo2	2oo2	1oo1
number of spares in channel 2	2	1	1	4	3	2	2
alarm logic $f(\mathbf{y})$	1oo2	1oo2	1oo2	1oo1	1oo1	1oo1	1oo1
inspection interval (months)	2	2	2	2	2	2	2
number of solenoid valves	2	2	2	2	2	2	2

Notice that, as mentioned previously regarding eqs 25 and 26, A_i varies with n and k, whereas B_i is a function of m, n, and k. It is important to note that the values of these parameters can be computed in advance before the optimization problem is solved. Notice also that the same term $(1 - y_i)(1 - \sum_{m=1}^{\Omega_i}\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k})$ appears in the expressions for both $\Pr\{\mathbf{y}|\xi = 0\}$ and $\Pr\{\mathbf{y}|\xi = 1\}$. These formulations are designed to provide correct probability values when the ith sensor is excluded from alarm logic ($\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k} = 0$ for $m = 1, 2, ..., \Omega_i$); that is, $\Pr\{y_i = 0|x = 0\} = 1$, $\Pr\{y_i = 0|x = 1\} = 1$, $\Pr\{y_i = 1|x = 0\} = 0$, and $\Pr\{y_i = 1|x = 1\} = 0$. In other words, this scenario can be viewed as having a fictitious online sensor that does not send any alarm signal under all circumstances. Substituting eq 58 into eq 29 yields a modified version of $g(\mathbf{y})$ in the expression for the total expected loss $L_{\mathrm{PT}}^{\mathrm{LC}}$.

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

$$\mathrm{obj} = C_{\mathrm{AL}}^{\mathrm{LC}} + C_{\mathrm{SD}}^{\mathrm{LC}} + L_{\mathrm{PT}}^{\mathrm{LC}} \tag{59}$$

In certain applications, there is also a need to impose an initial budget constraint, that is

$$\sum_{i=1}^{M}\sum_{m=1}^{\Omega_i}\left(\sum_{n\le m}\sum_{k\le n} w_{i,m,n,k}\right) m\mathrm{PCS}_i + \sum_{j=1}^{N} s_j\mathrm{PCV}_j \le C_{\mathrm{budget}} \tag{60}$$

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 $w_{i,m,n,k}$ and (b) the binary values of function $f(\mathbf{y})$ for all possible $\mathbf{y}$.

7. Examples

The feasibility and effectiveness of the proposed sequential design strategy are demonstrated here with case studies. In all examples described in this section, it is assumed that (1) the operating life of every protected process (H) is 5 years, (2) the probability of the unsafe system state (p) in each year is constant at 0.2, and (3) the interest rate (r) is 6% per year. It should also be noted that these examples are used solely to highlight various features of the proposed design and maintenance strategies. To this end, all cost data are presented in terms of the relative cost unit (rcu), and these values are chosen primarily for the purpose of facilitating proper tradeoffs. Finally, it should be noted that all integer program (IP) models in the following examples were solved with the solver BARON in the GAMS environment on a Pentium 4 3.00 GHz PC.

7.1. Example 1. Consider a fictitious exothermic continuous stirred-tank reactor (CSTR). It is assumed in this example that a larger-than-normal throughput could drive the system temperature to a sufficiently high level that, in turn, could cause the reaction to run away. To protect the reactor against catastrophic consequences, the reactor temperature and feed flow rate are both measured online in two separate alarm channels (i.e., $M = 2$). The outputs of these channels are then used as the basis for actuating the solenoid valve(s) on the inlet pipeline according to a predetermined logic. The life-cycle cost parameters adopted in this example for the FS and FD system failures are $C_{\mathrm{a}}^{\mathrm{LC}} = 4.4651 \times 10^4$ rcu and $C_{\mathrm{b}}^{\mathrm{LC}} = 4.4651 \times 10^6$ rcu, respectively.

We first assume that there are at most six online sensors for use in each alarm channel and that each can be supported by at most 20 spares, that is, $\Omega_i = 26$ and $i = 1, 2$. The maintenance and cost parameters of the flow sensors ($i = 1$) are as follows

$$\lambda_1 = 0.3\ \mathrm{year}^{-1}, \quad \mu_1 = 6.0\ \mathrm{year}^{-1},$$
$$\varepsilon_1 = 365\ \mathrm{year}^{-1}, \quad a_1 = 0.1, \quad \mathrm{PCS}_1 = 350\ \mathrm{rcu},$$
$$\overline{\mathrm{RprsC}}_1 = 44.7\ \mathrm{rcu}, \quad \overline{\mathrm{RplsC}}_1 = 22.3\ \mathrm{rcu}$$

The corresponding parameters of the temperature sensors ($i = 2$) are chosen to be

$$\lambda_2 = 0.5\ \mathrm{year}^{-1}, \quad \mu_2 = 8.0\ \mathrm{year}^{-1},$$
$$\varepsilon_2 = 365\ \mathrm{year}^{-1}, \quad a_2 = 0.15, \quad \mathrm{PCS}_2 = 100\ \mathrm{rcu},$$
$$\overline{\mathrm{RprsC}}_2 = 17.9\ \mathrm{rcu}, \quad \overline{\mathrm{RplsC}}_2 = 17.9\ \mathrm{rcu}$$

On the other hand, it is assumed that there are at most five solenoid valves available for shutdown operation, that is, $N = 5$. There is only one valve type and its specifications are

$$\lambda_j = 0.35\ \mathrm{year}^{-1}, \quad \alpha_j = 0.1, \quad \mathrm{PCV}_j = 150\ \mathrm{rcu},$$
$$\overline{\mathrm{InspC}}_j = 26.8\ \mathrm{rcu}, \quad \overline{\mathrm{RprlC}}_j = 22.3\ \mathrm{rcu}$$

where $j = 1, ..., 5$.

Seven optimization runs were carried out according to different levels of initial budget, and the results are summarized in Table 1. Notice that the abbreviations 3oo3, 2oo2, 1oo2, and 1oo1 are used in this table to represent the logic gates 3 out of 3, 2 out of 2, 1 out of 2, and 1 out of 1, respectively. It can be observed that the objective value can generally be reduced by relaxing the budget constraint. The minimum expected life-cycle expenditure is achieved if a sufficient initial budget can be allocated to purchase the critical components in the protective system; see case 1-1. Notice that, in this case, the total number of temperature sensors is larger than the total number of flow sensors. This is mainly due to the fact that the former is cheaper. Although the temperature sensors are less reliable with higher failure rates, the availability of the temperature alarm channel can be enhanced basically with more components. Notice also

Table 2. Optimization Results for Example 1, Part 2: Single-Channel Alarm Configuration with Flow Sensors

	case no.				
	1-8	1-9	1-10	1-11	1-12
initial budget (rcu)	10000	1950	1600	1250	900
objective value (rcu)	12993	13222	13967	15216	24461
purchase cost (rcu)	2050	1700	1350	1000	850
maintenance cost (rcu)	1632	1631	1531	1529	1484
alarm logic *f*(**y**)	2oo2	2oo2	1oo1	1oo1	1oo1
number of spares	3	2	2	1	1
inspection interval (months)	2	2	2	2	1
number of solenoid valves	2	2	2	2	1

Table 3. Optimization Results for Example 1, Part 3: Single-Channel Alarm Configuration with Temperature Sensors

	case no.				
	1-13	1-14	1-15	1-16	1-17
initial budget (rcu)	10000	850	750	650	550
objective value (rcu)	13210	13240	14196	15123	17441
purchase cost (rcu)	900	800	700	600	500
maintenance cost (rcu)	1609	1609	1608	1072	1517
alarm logic *f*(**y**)	2oo2	2oo2	2oo2	1oo1	1oo1
number of spares	4	3	2	2	1
inspection interval (months)	2	2	2	2	2
number of solenoid valves	2	2	2	2	2

that the optimal purchase cost is actually much lower than the initial budget in case 1-1. This result implies that 1850 rcu is also the true optimum without setting any maximum allowable cost limit. If the initial budget is reduced to a lower-than-optimum level, then obviously, a different collection of components must be selected to satisfy the more stringent budget constraint. The resulting structural changes can be summarized as follows:

(i) If $C_{\text{budget}} = 1800$ rcu, the number of spares for temperature sensor must be reduced from 2 to 1.

(ii) If $C_{\text{budget}} = 1700$ rcu, the voting gate of channel 2 must be simplified from 3oo3 to 2oo2.

(iii) If $C_{\text{budget}} = 1600$ rcu or lower, the flow alarm channel should be removed. There is only a single temperature alarm channel left in the protective system.

To demonstrate the advantage(s) of multichannel alarm strategy, the proposed model was solved again to generate single-channel structures ($M = 1$) with flow or temperature sensors. The corresponding optimization results can be found in Tables 2 and 3, respectively. Notice that, in this example, a flow sensor is more reliable but has a higher cost. Consequently, if the initial budget is large enough, the flow-based protective system is superior to that equipped with temperature sensors (see cases 1-8 and 1-13). However, as the budget limit is tightened to no more than 2000 rcu, the latter system starts to outperform the former (see cases 1-9 and 1-13). It can also be observed from Tables 1−3 that, given a sufficient budget, the multichannel alarm structure is better suited for maintaining a lower level of expected life-cycle expenditure.

7.2. Example 2. The refrigeration unit considered in this example is taken from Liptak.[11] A simplified P&ID is shown in Figure 9, and the detailed process description can be found in Appendix II. Operational safety in this system is guaranteed by a number of interlocks. One of them stops the compressor if any of the following six conditions occurs while the compressor is running:

(1) Refrigerated water flow is low, measure by FSL-3.

(2) Compressor discharge pressure (and, therefore, pressure in the condenser) is high, 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, detected by TSH-5.

(6) Lubricating oil pressure is low (not shown in Figure 9).

The proposed design and maintenance strategies were applied to this interlocking system with assumed parameters. For illustration convenience, the last alarm variable, namely, the pressure of lubricating oil, is neglected in the present study, and thus, $M = 5$. We assume that the life-cycle cost parameters for the FS and FD system failures can be estimated to be $C_{\text{a}}^{\text{LC}} = 4.4651 \times 10^4$ rcu and $C_{\text{b}}^{\text{LC}} = 4.4651 \times 10^7$ rcu, respectively, and also that there are at most six online sensors for use in every alarm channel and that each channel is supported by at most 20 spares, that is, $\Omega_i = 26$ and $i = 1, ..., 5$. The chosen maintenance and cost parameters of the sensors in different alarm channels can be found in Table 4. Finally, it is assumed that there are at most five shutdown units, that is, $N = 5$. Their specifications are

$$\lambda_j = 0.4\ \text{year}^{-1}, \quad \alpha_j = 0.1, \quad \text{PCV}_j = 200\ \text{rcu},$$
$$\overline{\text{InspC}}_j = 13.4\ \text{rcu}, \quad \overline{\text{RprlC}}_j = 22.3\ \text{rcu}$$

where $j = 1, ..., 5$.

Two optimization runs were performed to generate better design specifications and maintenance programs under different budget constraints. The results are summarized in Table 5. The corresponding alarm-generation logic can be found in Figures 10 and 11. Notice that these logic systems can also be expressed as the following alarm functions:

Case 2-1

$$f(\mathbf{y}) = 1 - \{1 - [y_2(1 - (1 - y_3)(1 - y_4)(1 - y_5))]\} \times \{1 - [y_1(1 - (1 - y_3y_4)(1 - y_3y_5)(1 - y_4y_5))]\} \times \{1 - y_3y_4y_5\}$$

Case 2-2

$$f(\mathbf{y}) = 1 - [1 - (y_1y_2)] \times \{1 - [y_2(1 - y_3)(1 - y_4)(1 - y_5)]\} \times \{1 - [(1 - y_3y_4)(1 - y_3y_5)(1 - y_4y_5)]\}$$

It can be observed from Table 5 that, if the initial budget is sufficient, a larger number of spares can often be selected in each channel to improve availability; see case 2-1. Notice also that, in the same protective system design, the numbers of spares in different channels are usually not identical. By and large, these numbers should increase with the corresponding failure rates, and they can also be affected by other design parameters, such as the repair rate, replacements rate, and purchase and maintenance costs. Notice also that the 1-out-of-1 voting gate is used in every alarm channel in all cases. Consequently, the FD failure probability of a single channel is relatively high, but the FS failure probability should be low. This is not a problem because a large number (five) of channels is used in the present system. The resulting FD failure probability of the

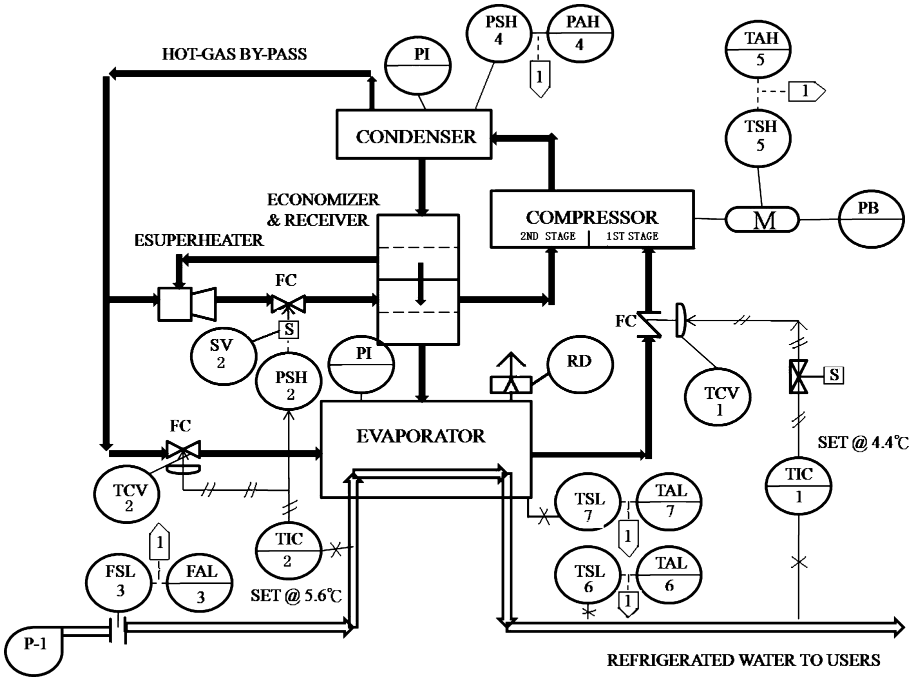

Figure 9. Piping and instrumentation diagram (P&ID) of a typical refrigeration unit.

Table 4. Sensor Parameters Used in Example 2

	channel no.				
	1	2	3	4	5
failure rate, μ_i (year $^{-1}$)	2.5	0.3	1.5	1.8	2
repair rate, μ_i (year $^{-1}$)	3	3	3	3.5	4
replacement rate, ε_i (year $^{-1}$)	365	365	365	365	365
purchase cost, PCS_i (rcu)	100	250	100	80	60
average repair cost, RprsC_i (rcu)	8.93	17.86	8.93	6.25	4.47
average replacement cost, RplsC_i (rcu)	8.93	8.93	4.47	4.47	4.47
probability of sensor FS failure, a_i	0.15	0.1	0.1	0.1	0.1

Table 5. Optimization Results for Example 2

	case no.	
	2-1	2-2
initial budget (rcu)	10000	1800
objective value (rcu)	15516	16547
purchase cost (rcu)	2410	1780
maintenance cost (rcu)	3211	3191
voting gate of channel 1	1oo1	1oo1
number of spares in channel 1	1	1
voting gate of channel 2	1oo1	1oo1
number of spares in channel 2	2	1
voting gate of channel 3	1oo1	1oo1
number of spares in channel 3	3	2
voting gate of channel 4	1oo1	1oo1
number of spares in channel 4	4	2
voting gate of channel 5	1oo1	1oo1
number of spares in channel 5	5	3
inspection interval (month)	1	1
number of shutdown units	2	2

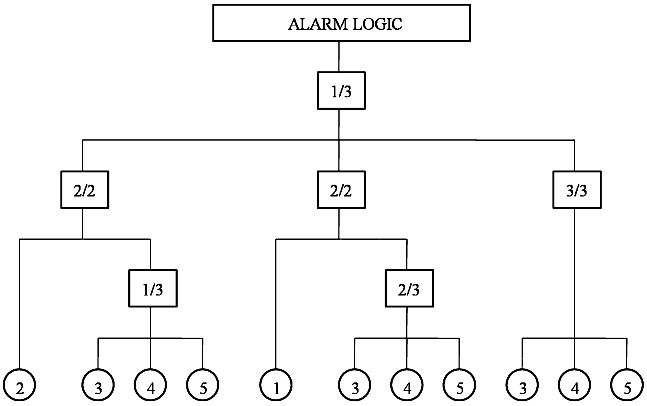

Figure 10. Optimal alarm-generation logic in case 2-1.

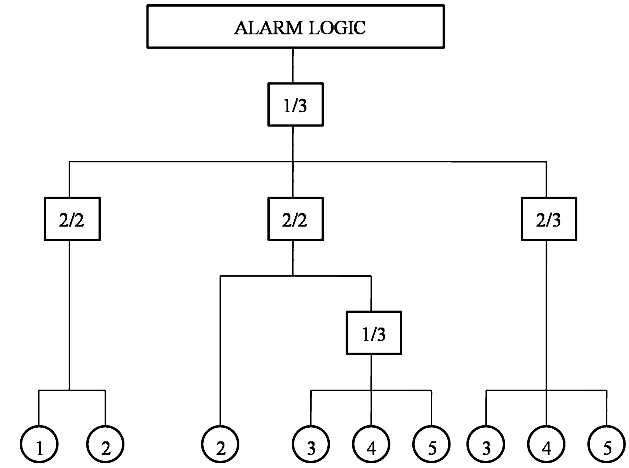

Figure 11. Optimal alarm-generation logic in case 2-2.

entire protective system can be reduced to an ideal level with the proposed optimal alarm-generation logic.

As for the alarm-generation structures described in Figures 10 and 11, it can be observed that the alarm channels can be generally divided into two groups, namely, {1, 2} and {3, 4, 5}. Let us first take a closer look at the alarm logic for case 2-1. From Figure 10, it is clear that there are three combinations that could result in an alarm and that all three involve channels 3, 4, and 5. A system alarm calls for the detection of a dangerous state in one of these three channels if channel 2 simultaneously confirms the unsafe condition, whereas the combination of a

2-out-of-3 selection among these channels plus channel 1 can also set off the alarm. This arrangement is clearly due to the fact that the sensors in channel 2 are relatively more reliable (with smaller failure rates) than those in channel 1 (see Table 4). Finally, if all three aforementioned channels detect the dangerous state, then an alarm can be generated directly without considering channels 1 and 2. Notice that the initial capital expenditure can be reduced by using fewer spares and, also, modifying the alarm-generation logic. The optimal alarm-generation logic in Figure 11 (for case 2-2) can be identified with a significantly lower budget level at 1800 rcu.

8. Conclusions

To mitigate the catastrophic outcomes caused by accidents in chemical plants, it is a common practice to install protective systems on processing units operated under hazardous conditions. Because hardware failures are basically random but unavoidable, the system availability is highly dependent on the protective scheme and also the maintenance program. The aim of this study was to improve and generalize the current practice for generating the design specifications and the inspection, repair, and replacement policies for multichannel protective systems. By solving the proposed mathematical programming model, it is possible to determine (1) the number of online sensors and the corresponding voting gate in each alarm channel, (2) the multichannel alarm-generation logic, (3) the number of valves and the corresponding shutdown configuration, and (4) the needed maintenance policies for all critical components. In addition, because the sensors and valves in the protective systems are assumed to be maintained with the appropriate corrective and preventive strategies, the optimal number of spare sensors stored off-line and the best inspection interval for each valve can also be identified in the optimal solution of the proposed model.

From the extensive case studies carried out in this study, it can be observed that the proposed design procedure is feasible and effective. Furthermore, the mathematical programming approach is obviously more efficient than the traditional ad hoc approach in configuring the protective systems and stipulating the corresponding maintenance procedures. It can also be concluded that, given a sufficient budget, the expected life-cycle expenditure of a multichannel protective system can be lowered to a desired level that is not achievable with any single-channel system.

Nomenclature

A_i = conditional probability of FS failure of the ith alarm channel

$\overline{\mathrm{Av}(t)}$ = availability function

$\overline{\mathrm{Av}}$ = average availability

$\overline{\mathrm{Av}}^{\mathrm{Corr}}$ = average availability of an alarm channel maintained by a corrective strategy

$\overline{\mathrm{Av}}^{\mathrm{Prev}}$ = average availability of a shutdown unit maintained by a preventive strategy

a_i = FS probability of a single sensor in the ith channel

B_i = conditional probability of FD failure of the ith alarm channel

C_{a} = financial loss incurred from FS failure of the protective system

$C_{\mathrm{a}}(k-1,k)$ = cost of FS failure of the protective system in the kth year

$C_{\mathrm{a}}^{\mathrm{LC}}$ = life-cycle cost parameter defined in eq 39

$C_{\mathrm{AL}}^{\mathrm{LC}}$ = total life-cycle cost of alarm subsystem

C_{b} = financial loss incurred from FD failure of the protective system

$C_{\mathrm{b}}(k-1,k)$ = cost of FD failure of the protective system in the kth year

$C_{\mathrm{b}}^{\mathrm{LC}}$ = life-cycle cost parameter defined in eq 40

C_{budget} = budget limit for initial investment

$C_{\mathrm{SD}}^{\mathrm{LC}}$ = total life-cycle cost of shutdown subsystem

$\mathrm{ENRpl}_i(m,n)$ = expected number of replacements for channel i in a year

$\mathrm{ENRpr}[t_1,t_2]$ = expected number of repairs in time interval $[t_1,t_2]$

$\mathrm{ENRpr}_i(m,n)$ = expected number of repairs for channel i in a year

$f(\mathbf{y})$ = alarm function $[f(\mathbf{y}) \in \{0,1\}]$

H = operating life of protective system

$h(\mathbf{z})$ = shutdown function $[h(\mathbf{z}) \in \{0,1\}]$

$\overline{\mathrm{InspC}}_j$ = average inspection cost of shutdown unit j

$\mathrm{InspC}_j(k-1,k)$ = inspection cost of shutdown unit j in the kth year

L_{AL} = expected yearly loss due to FS and FD alarm failures

L_{PT} = expected yearly loss due to FS and FD failures of the protective system

$L_{\mathrm{PT}}^{\mathrm{LC}}$ = overall life-cycle loss of a protective system

$L_{\mathrm{PT}}(k-1,k)$ = expected loss of a protective system in the kth year

$\mathrm{LCC}_i^{\mathrm{AL}}$ = life-cycle cost of alarm channel i

$\mathrm{LCC}_j^{\mathrm{SD}}$ = life-cycle cost of shutdown unit j

M = total number of possible alarm channels

m = number of sensors purchased for an alarm channel

N = total number of possible shutdown units

n = number of sensors installed online in an alarm channel

n_{ol} = number of functional online sensors in an alarm channel

p = average probability of a given unsafe process state in one year

$P_{\mathrm{FD}}^{\mathrm{AL}}$ = conditional probability of FD failure of the alarm subsystem

$P_{\mathrm{FD}}^{\mathrm{SD}}$ = conditional probability of FD failure of the shutdown subsystem

$P_{\mathrm{FS}}^{\mathrm{AL}}$ = conditional probability of FS failure of the alarm subsystem

$P_{\mathrm{FS}}^{\mathrm{SD}}$ = conditional probability of FS failure of the shutdown subsystem

P_k = steady-state probability of the system at node k

PCS_i = purchase cost of one sensor in channel i

PCV_j = purchase cost of shutdown unit j

r = interest rate

$\overline{\mathrm{RplsC}}_i$ = average replacement cost of channel i

$\mathrm{RplsC}_i(k-1,k)$ = replacement cost of channel i in the kth year

$\overline{\mathrm{RprlC}}_j$ = average repair/replacement of shutdown unit j

$\mathrm{RprlC}_j(k-1,k)$ = repair/replacement of shutdown unit j in the kth year

$\overline{\mathrm{RprsC}}_i$ = average repair cost of channel i

$\mathrm{RprsC}_i(k-1,k)$ = repair cost of channel i in the kth year

s_j = binary variable adopted to represent whether the jth unit is selected for online implementation

$w_{i,m,n,k}$ = binary variable used to denote whether the ith channel is used and that, in this channel, there are m purchased sensors, n online sensors, and a k-out-of-n voting gate

x_i = binary variable used to denote whether the ith process variable exceeds the specified safety limit

y_i = binary variable used to denote whether an unsafe state is detected in the ith alarm channel

z_j = binary variable used to denote whether the jth shutdown unit completes the designated operation

Greek Letters

α_j = conditional probability of FS failure of the jth shutdown unit

β_j = conditional probability of FD failure of the jth shutdown unit

ε_i = replacement rate of a sensor in alarm channel i

λ_i = failure rate of a sensor in alarm channel i

λ_j = failure rate of shutdown unit j

μ_i = repair rate of a sensor in alarm channel i

ξ = binary variable used to denote whether a particular unsafe process state is present

τ_j = length of inspection interval for shutdown unit j
Ω_i = maximum allowable number of purchased sensors for the ith channel

Appendix I: Steady-State Probabilities of Channel States under a Spare-Supported Corrective Maintenance Program

Block 1

$$P_{j+1} = \frac{j\lambda}{\mu}p_0, \quad j = 1, 2, ..., n$$

Block 2

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

Block 3

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

Block 4

$$P_i = P_0\lambda^i \prod_{k=1}^{i} \frac{j + 1 - k}{\varepsilon + (j - k)\lambda}, \quad j = 1, 2, ..., n; i = 1, 2, ..., j - 1$$

Block 5

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

Block 6

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

Block 7

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

Appendix II: Process Description of the Refrigeration Unit in Example 2

The refrigeration unit in Figure 9 provides chilled water at 40 °F (4.4 °C) through the circulating header system of an industrial plant. The flow rate is fairly constant, and therefore, process load changes are reflected by the temperature of the returning refrigerated water. Under normal load conditions, this return water temperature is 51 °F (10.6 °C). As the process load decreases, the return water temperature drops correspondingly. With the reduced load on the evaporator, TIC-1 gradually closes the suction damper or the prerotation vane of the compressor. By throttling the suction vane, a 10:1 turndown ratio can be accomplished. If the load drops below this ratio, the hot-gas bypass system has to be activated.

The hot-gas bypass is automatically controlled by TIC-2. Its purpose is to keep the constant-speed compressor out of surge: When the load drops to levels sufficiently low to approach surge, this bypass valve is opened. If the chilled-water flow rate is constant, the difference between the chilled-water supply and return temperatures is an indication of the load. If full load corresponds to a 15 °F (8.3 °C) difference on the chilled-water side of the evaporator and the chilled-water supply temperature is controlled by TIC-1 at 40 °F (4.4 °C), then the return water temperature detected by TIC-2 is also an indication of load.

If surge occurs at 10% load, this would correspond to a return water temperature of 41.5 °F (5.3 °C). To stay safely away from surge, TIC-2 in Figure 9 is set at 42 °F (5.6 °C), corresponding to an approximately 13% load. When the temperature drops to 42 °F (5.6 °C), this valve starts to open, and its opening can be proportional to the load detected. This means that the valve is fully closed at 42 °F (5.6 °C), fully open at 40 °F (4.4 °C), and throttled in between. This throttling action is accomplished by a plain proportional controller that has a 2 °F throttling range, which, on a span of 0−100 °F, corresponds to a proportional band of 2% or a gain of 50.

The economizer shown in Figure 9 can increase the efficiency of operation by 5−10%. This is achieved through reductions in space requirements, savings on compressor power consumption, reductions of condenser and evaporator surfaces, and other effects. The economizer shown in Figure 9 is a two-stage expansion valve with condensate collection chambers. When the load is above 10%, the hot-gas bypass system is inactive. Condensate is collected in the upper chamber of the economizer, and it is drained under float level control, driven by the condenser pressure. The pressure in the lower chamber floats off the second stage of the compressor, and it, too, is drained into the evaporator under float level control, driven by the pressure of the compressor second stage. Economy is achieved as a result of the vaporization in the lower chamber by precooling the liquid that enters the evaporator and, at the same time, desuperheating the vapors that are sent to the compressor second stage. When the load is below 10%, the hot-gas bypass is in operation, and solenoid valve SV-2, which is actuated by high-pressure switch PSH-2, opens. Some of the hot gas goes through the evaporator and is cooled by contact with the liquid refrigerant, and some of the hot gas flows through the open solenoid. This second portion is desuperheated by the injection of liquid refrigerant upstream of the solenoid, which protects against overheating of the compressor.

Literature Cited

(1) Liang, K. H.; Chang, C. T. A Simultaneous Optimization Approach To Generate Design Specifications and Maintenance Policies for the Multilayer Protective Systems in Chemical Processes. *Ind. Eng. Chem. Res.* **2008**, *47*, 5543.

(2) Tsai, C. S.; Chang, C. T. A Statistics Based Approach to Enhancing Safety and Reliability of the Batch-Reactor Charging Operation. *Comput. Chem. Eng.* **1996**, *20*, S647.

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

(4) 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.

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

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

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

(8) 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.

(9) 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.

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

(11) Liptak, B. G. *Optimization of Unit Operations*; Chilton Book Co.: Radnor, PA, 1987.

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

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

(14) Henley, E. J.; Kumamoto, H. *Designing for Reliability and Safety Control*; Prentice Hall: Upper Saddle River, NJ, 1985.

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

Received for review November 16, 2009
Revised manuscript received July 29, 2010
Accepted September 19, 2010

IE901818E