I&EC research
Industrial & Engineering Chemistry Research

Article

pubs.acs.org/IECR

Model Based Approach To Identify Optimal System Structures and Maintenance Policies for Safety Interlocks with Time-Varying Failure Rates

Edwin Wibisono, Vincentius Surya Kurnia Adi, and Chuei-Tin Chang*

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

Supporting Information

ABSTRACT: In order to mitigate the detrimental outcomes of accidents in the modern chemical plants, it is a common practice to install safety interlocks on processes operated under hazardous conditions. A generic mathematical programming model has already been developed in the past for simultaneously stipulating the optimal interlock structure and the corresponding maintenance policies of a given process. This conventional formulation is improved in the present study by relaxing a constraining assumption, that is, the failure rate of every embedded component is constant. Instead of the exponential distribution, the more realistic Weibull distribution is incorporated in the modified model to characterize the time to failure of every embedded component. Consequently, this proposed practice could facilitate identification of more elaborate time-dependent inspection schedules and also alarm logics. Two examples are provided to demonstrate the feasibility and effectiveness of the proposed approach.

1. INTRODUCTION

In order to mitigate the detrimental outcomes of accidents in the modern chemical plants, it is a common practice to install safety interlock(s) on processes operated under hazardous conditions. Since faults and failures are random events, these protective mechanisms must function normally at all time. For the purpose of ensuring a desired level of availability, the interlock structure and its maintenance policy should be regarded as the key design specifications that must be stipulated properly.

In general, a comprehensive protective system is equipped with two basic functions: alarm and shutdown. The former is facilitated with online sensors. Based on their measurements, a predetermined Boolean logic can be applied to decide whether an alarm should be set off. The latter function can usually be accomplished with actuators, for example, solenoid valves or power switches. In response to the alarm decision, these devices can be activated to perform the required shutdown operation(s). Note that any hardware item may fail either safely (FS) or dangerously (FD). To reduce the chance of interlock malfunction, a common industrial practice is to introduce hardware redundancy at the component level. Note also that the unsafe process state can often be detected according to one or more critical variable. To facilitate reliable alarm generation, each of them may be monitored with a set of identical sensors (which as a whole is called an alarm "channel" in this paper). Similarly, there may be more than one way to stop a given operation, and for the purpose of ensuring safe shutdown, it may also be necessary to install repeated actuators. Tsai and Chang[1] proposed a statistics-based method to improve the overall reliability of any given sensor system for mass-flow network and to develop a systematic strategy to synthesize the corresponding alarm logic, while Chang et al.[2] generalized this approach to any process network. Also, Andrews and Barlett[3] tried to minimize system unavailability with a branch search logarithm.

The spare-supported corrective maintenance policy is adopted in the present study to upkeep the monitoring device(s) in every alarm channel. Specifically, it is assumed that, other than the sensor(s) installed online, spares may also be stored offline. The failed online sensor is immediately replaced with a spare and then repaired offline as quickly as possible. Therefore, the number of spares needed for every channel should be treated as an important design parameter. Lai and Chang[4] have carried out a preliminary study on the basis of this idea. On the other hand, since the shutdown units are not used during normal operations, their FD failures can only be revealed on demand. It is thus necessary to utilize a preventive maintenance strategy to lower the probability of catastrophic outcome(s) caused by these unobservable failures. Specifically, every shutdown device is required to be inspected at the designated time intervals. The failed unit must be repaired or replaced immediately after inspection, while the normal ones are allowed to stay online. Clearly, the inspection schedule is the most important consideration in drawing up the preventive maintenance plan. Vaurio[5] suggested that the inspection intervals must be determined to minimize the cost rate or accident rate. The same author later[6] incorporated the age replacement policy into the preventive maintenance scheme. Under this policy, every component is replaced after a fixed number of inspections and/or repairs, even it is still functional. Badia et al.[7] assumed that only the unrevealed failures may occur in the given system, and then developed a computational procedure to determine the cost-optimal inspection interval.

Received: September 3, 2013
Revised: February 5, 2014
Accepted: February 18, 2014
Published: February 18, 2014

ACS Publications © 2014 American Chemical Society

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

These authors[8] then expanded the scope of study to scenarios where both revealed and unrevealed failures are possible. Duarte and Craveiro[9] optimized the preventive maintenance strategy to achieve minimum total cost under the assumption that the repair rate is constant, and both failure rate and hazard rate are increasing over time. Okasha and Frangopol[10] proposed two optimization strategies for selecting maintenance actions and scheduling of structural components in terms of system reliability, redundancy, and life-cycle cost with multi-objective generic algorithm. Wang and Pham[11] introduced a multiobjective optimization embedded in the imperfect maintenance strategies for a single-unit system subject to two competing risks, that is, the aging failure and the immediate failure (random shocks). By maximizing the asymptotic availability and minimizing the cost rate, one can determine the number of inspections before replacement and the initial inspection interval. Kouedeu et al.[12] proposed a two-level hierarchical decision-making approach to compute the mean time to failure in the first level and to simultaneously optimize the production rate and the maintenance policies in the second level. Finally, Wang and Pham[13] thoroughly reviewed the state of the art in reliability and maintenance modeling, including repair maintenance, replacement policy, inspection policy and maintenance modeling for complex systems.

The aforementioned design and maintenance issues were traditionally addressed with an ad hoc approach, which could be both tedious and error prone. Several generic mathematical programming models have thus been developed in recent years for automating these tasks systematically. Liang and Chang[14] developed a mathematical programming model to simultaneously generate design specifications and maintenance policies for the *multilayer* interlocks, while Liao and Chang[15] later improved this model for the *multichannel* systems. In these published works, the failure rates were assumed to be constant mainly for the purposes of simplifying model formulation and reducing computation effort. This assumption is not always realistic. In fact, the failure rate of almost any hardware item inevitably increases with age and the corresponding availability level tends to drop faster over time. The use of a constant average value overestimates the true failure rate at the early stage of utilization, whereas underestimates in the long run. In addition, notice also that a constant failure rate implies that a working unit is always "as-good-as-new"; that is, the condition of this unit (in terms of failure rate) after inspection/repair is assumed to be the same as that of a brand new one. Since this inherent assumption is no longer applicable if the failure rates are time dependent, the alternative scenario of "as-bad-as-old" must be considered.

On the basis of the above considerations, the time-variant failure-rate models have been adopted in numerous recent studies for computing the component availabilities. Barlow and Hunter[16] suggested using the Weibull distribution under the assumption of minimal repair. An empirical equation was developed accordingly for determining the optimal replacement periods and the corresponding minimal maintenance cost. In a modified version, Park[17] proposed to perform an optimal number of minimal repairs before replacement. Brown and Proschan[18] developed a new model formulation to describe the time-varying failure rates according to the assumption of imperfect repair. The same authors[19] then improved this model to describe the imperfect maintenance policy, which features imperfect replacement, imperfect inspection period, and imperfect repair. Aven[20] also developed the optimal replacement strategy under minimal repair assumption, while Aven and Jensen[21] generalized the minimal repair model. Li and Shaked[22] proposed various preventive maintenance policies on the basis of imperfect repair models. Doyen and Gaudoin[23] derived the imperfect repair model to reduce failure intensity and virtual age. In other words, every repair action done on the failed unit is meant to reduce the failure rate of the system or lengthen the age of the system. Marlow and Tortorella[24] constructed the strong and weak minimal repair models, the revival process model, and the reliability model of a maintained system. Yevkin and Krivtsov[25] also studied various replacement policies under Kijima's general repair model with the underlying Weibull distribution function via two efficient methods.

The above survey clearly reveals that there is a strong incentive for the development of an improved mathematical programming model to minimize the expected life-cycle expenditure of any multilayer multichannel interlock, in which the time to failure of every component is assumed to follow the Weibull distribution. By solving this model, one can systematically determine the following design specifications: (1) the channel types and the corresponding alarm logic in the alarm subsystem, (2) the number of spare sensors stored offline, the number of redundant sensors installed online and the corresponding voting-gate structure in every channel, and (3) the number of redundant units in the shutdown subsystem and the inspection schedule of each unit.

2. SUPERSTRUCTURES FOR ALARM AND SHUTDOWN SUBSYSTEMS

Although the general structure of a single-layer interlock (see Figure 1) was described in Liao and Chang,[15] a brief description is still presented here for the sake of completeness.

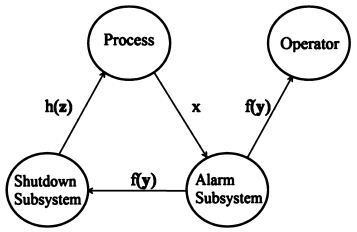

Figure 1. General structure of a protected system.

To facilitate construction of the modified model, a binary variable can be adopted to denote the condition of manufacturing process under consideration, that is,

$$\xi = \begin{cases} 1 & \text{if the process is in a specified unsafe state} \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

As mentioned before, the unsafe system state may be revealed in several different process conditions, such as the temperature, pressure and flow rate, etc. A binary vector, $\mathbf{x} = [x_1, x_2, \ldots x_M]^T$, is used in this study to characterize their actual values, that is

$$x_s = \begin{cases} 1 & \text{if the } s^{\text{th}} \text{ variable exceeds the specified safety limit} \\ 0 & \text{otherwise} \end{cases} \quad (2)$$

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

It is assumed that, for the purpose of measuring each variable online, there is one or more identical sensors configured in the corresponding alarm channel. All channel outputs also form another binary vector, $\mathbf{y} = [y_1, y_2, ..., y_M]^T$, and each indicates whether the unsafe state is verified, that is

$$y_i = \begin{cases} 1 & \text{if the } i^{\text{th}} \text{ channel detects the unsafe state} \\ 0 & \text{otherwise} \end{cases} \quad (3)$$

An alarm logic is applied based on all channel outputs and this logic can be expressed as a binary function $f(\mathbf{y})$, that is,

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

Sketches of the superstructures of an alarm subsystem and an alarm channel are shown in Figure 2. The shutdown decision

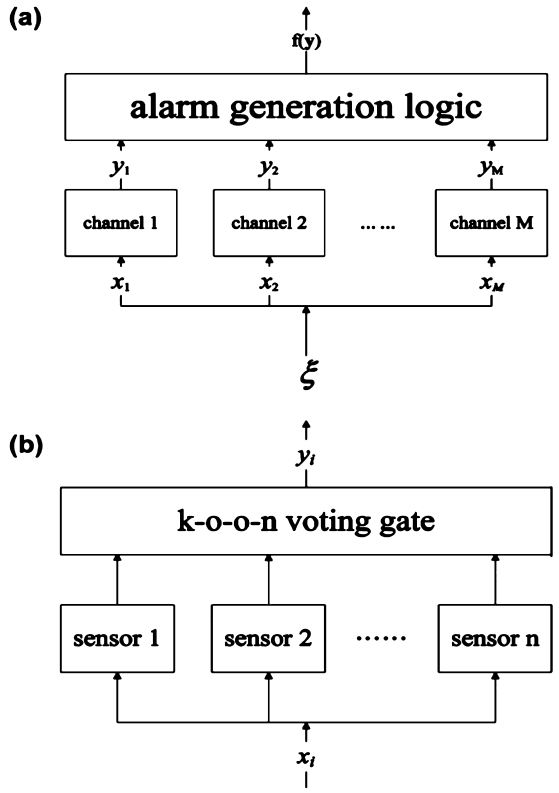

Figure 2. Superstructures of (a) alarm subsystem and (b) alarm channel with *k*-out-of-*n* voting gate.

can be either taken manually by operator(s) or automatically with a shutdown subsystem. For the sake of brevity, only the latter is considered in this study. To facilitate model formulation, an additional binary vector $\mathbf{z}$ is introduced to denote whether the designated operations are executed successfully. Its elements can be expressed as

$$z_j = \begin{cases} 1 & \text{if the } j^{\text{th}} \text{ unit completes the designated shutdown action} \\ 0 & \text{otherwise} \end{cases} \quad (5)$$

where $j = 1, 2, ..., N$. Another binary function can be defined to characterize the outcomes of all possible combinations of the actions taken by the units in shutdown subsystem, that is,

$$h(\mathbf{z}) = \begin{cases} 1 & \text{if the subsystem performs the shutdown operation successfully} \\ 0 & \text{otherwise} \end{cases} \quad (6)$$

In order to suppress the impacts of FD failures as much as possible, it is assumed that an OR logic is always adopted to configure the shutdown subsystem. This logic can thus be expressed explicitly as the following shutdown function and also in Figure 3.

$$h(\mathbf{z}) = 1 - \prod_{j=1}^{N} (1 - z_j) \quad (7)$$

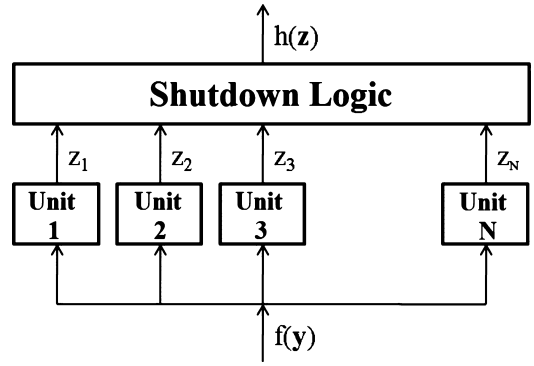

Figure 3. Superstructure of shutdown subsystem.

3. MAINTENANCE POLICIES OF CRITICAL COMPONENTS

Let us first review the candidate maintenance policies for critical components and also possible management measures to enhance interlock reliability (or availability). There are two types of maintenance policies that are relevant in the present study: the corrective and preventive policies.

Corrective Maintenance Policy. The corrective maintenance policies are designed specifically to handle the revealed failures which are unrecoverable. In particular, repair must be performed on a failed component to bring it back to the functioning state as quickly as possible. To ensure a high level of safety, the spare-supported program described in Liao and Chang[15] is adopted to maintain every alarm channel. In this study, the overall state of an alarm channel is represented with a special notation, as shown in Figure 4. In this figure, the

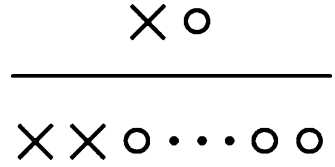

Figure 4. Example of the overall state of an alarm channel.

working sensors are denoted as "○", while " × " is used to denote the failed ones. The online sensor states are specified in the top row, whereas the bottom row reflects the states of spares. For illustration convenience, let us use *m* to denote the total number of sensors for the channel under consideration and *n* the number of online sensors in this channel.

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

The Markov diagram can be used to describe the state transition processes in a channel under the spare-supported corrective maintenance policies. Figure 5a shows an alarm channel with a single online sensor and $m - 1$ spares. Notice that there are $2m$ different nodes, each reflects a collective condition characterized with the notation defined above in Figure 4. Note also that every connecting arc is marked with the corresponding transition rate. In particular, λ, μ, and ε are used to denote failure rate, repair rate, and replacement rate, respectively. It is assumed in this study that a failure can only occur when at least one working sensor is online and state 0 represents the initial channel condition in which all sensors are normal. The proposed maintenance policies require that repair can only be carried out if all online sensors are functional and replacement is allowed if otherwise. Finally, it is clear that Figure 5a can be expanded to represent channels with more than one online sensor; for example, Figure 5b is for two online sensors ($n = 2$).

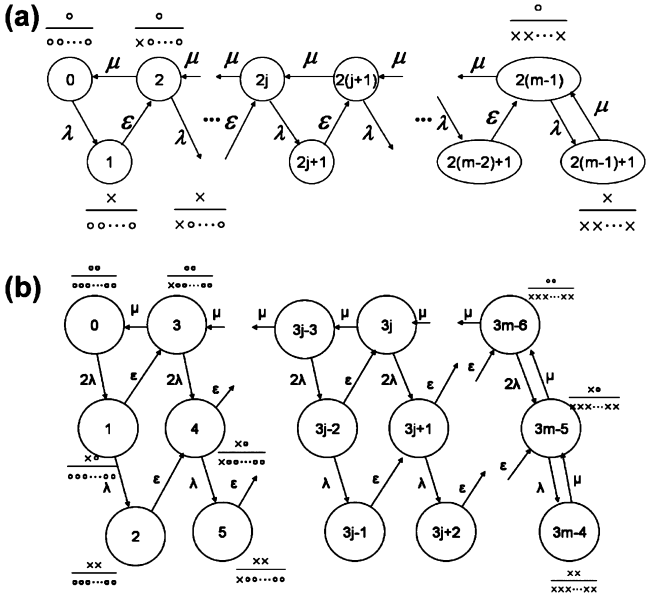

Figure 5. Markov diagrams of (a) a spare-supported corrective maintenance program for an alarm channel with $n = 1$, (b) a spare-supported corrective maintenance program for an alarm channel with $n = 2$.

For every node in the Markov diagram, a differential equation can be formulated to determine the probability of the corresponding state at any time. Let us consider a specific example when $m = 5$ and $n = 2$. It can be observed from Figure 6 that the nodes in this system can be grouped into seven blocks and the corresponding state equations in each block are of the same structure. Notice also that the failure rate $\lambda(t)$ is now time dependent, while the repair rate (μ) and replacement rate (ε) should both be regarded as constant model parameters. A complete list of all state equations for this example system can be found as follows:

Block 1

$$\frac{dP_0(t)}{dt} = \mu P_3(t) - 2\lambda(t)P_0(t) \tag{8}$$

Block 2

$$\frac{dP_3(t)}{dt} = \varepsilon P_1(t) + \mu P_6(t) - (2\lambda(t) + \mu)P_3(t) \tag{9}$$

$$\frac{dP_6(t)}{dt} = \varepsilon P_4(t) + \mu P_9(t) - (2\lambda(t) + \mu)P_6(t) \tag{10}$$

Block 3

$$\frac{dP_9(t)}{dt} = \varepsilon P_7(t) + \mu P_{10}(t) - (2\lambda(t) + \mu)P_9(t) \tag{11}$$

Block 4

$$\frac{dP_1(t)}{dt} = 2z(t)P_0(t) - (\lambda(t) + \varepsilon)P_1(t) \tag{12}$$

Block 5

$$\frac{dP_4(t)}{dt} = \varepsilon P_2(t) + 2\lambda(t)P_3(t) - (\lambda(t) + \varepsilon)P_4(t) \tag{13}$$

$$\frac{dP_7(t)}{dt} = \varepsilon P_5(t) + 2\lambda(t)P_6(t) - (\lambda(t) + \varepsilon)P_7(t) \tag{14}$$

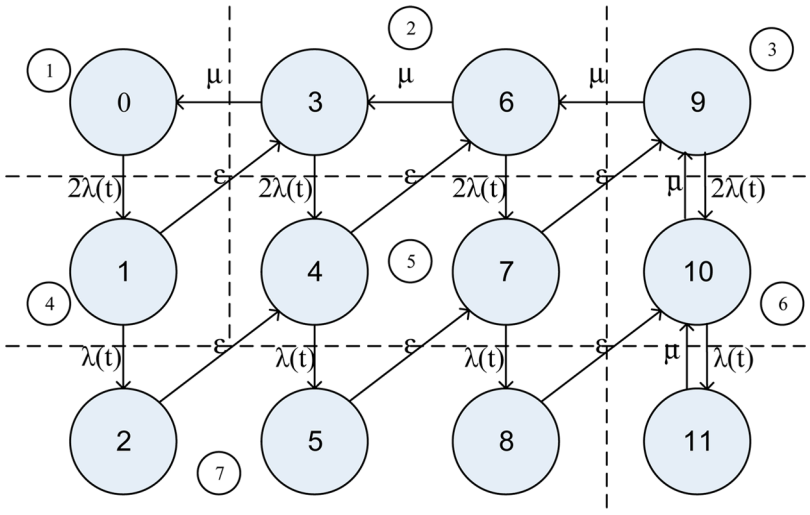

Figure 6. Markov diagram of spare-supported corrective maintenance program for an alarm channel ($m = 5$, $n = 2$).

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

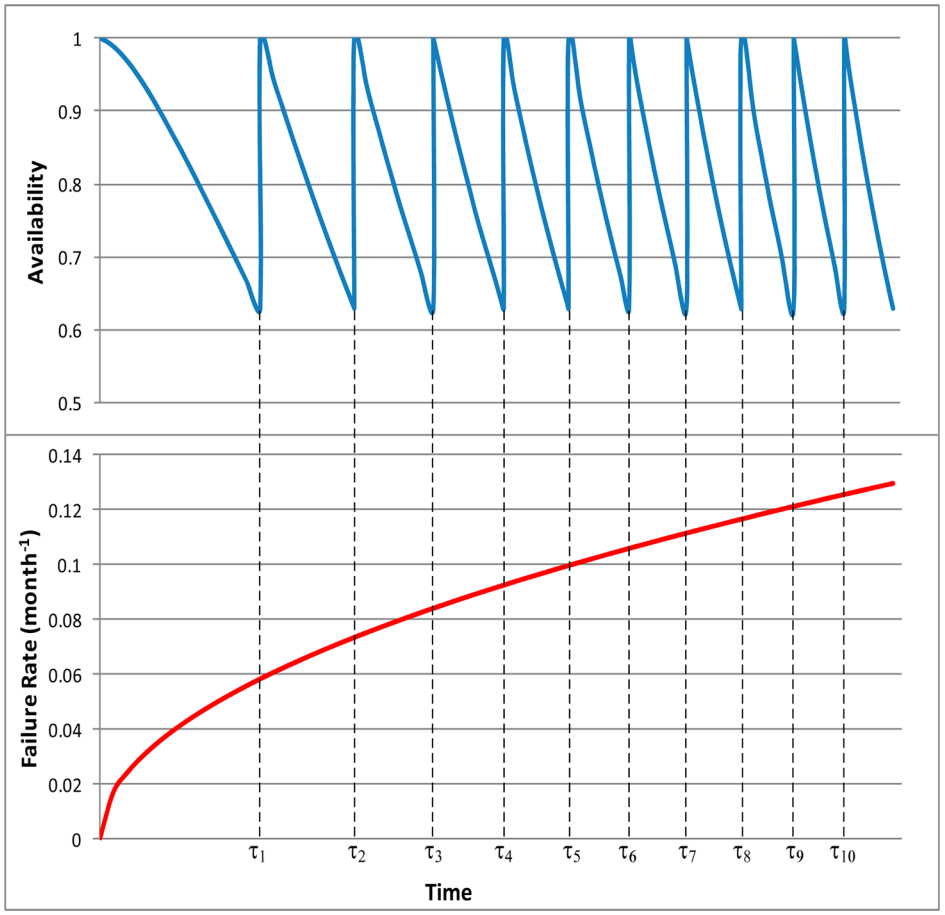

Figure 7. Typical time profiles of availability and failure rate of a passive component under preventive maintenance.

Block 6

$$\frac{dP_{10}(t)}{dt} = \varepsilon P_8(t) + 2\lambda(t)P_9(t) + \mu P_{11}(t) - (\mu + \lambda(t))P_{10}(t) \quad (15)$$

Block 7

$$\frac{dP_2(t)}{dt} = \lambda(t)P_1(t) - \varepsilon P_2(t) \quad (16)$$

$$\frac{dP_5(t)}{dt} = \lambda(t)P_4(t) - \varepsilon P_5(t) \quad (17)$$

$$\frac{dP_8(t)}{dt} = \lambda(t)P_7(t) - \varepsilon P_8(t) \quad (18)$$

where $P_k(t)$ denotes the probability of state k at time t and k = 0,1,2,...,11.

To facilitate integration of eqs 8−18, the time to failure of every hardware component is assumed to follow Weibull distribution;[26] that is, the probability that the component fails within the time interval $(0,t]$ can be expressed as the following cumulative distribution function $F(t)$

$$F(t) = \Pr\{T^C \le t\} = \begin{cases} 1 - e^{-(\theta t)^\alpha} & \text{if } t > 0 \\ 0 & \text{otherwise} \end{cases} \quad (19)$$

where T^C denotes the random variable representing the time to falure of a component, and θ and α denote the scale and shape parameters, respectively. The corresponding failure rate can be obtained by differentiating $F(t)$ with respect to t and then dividing the result by $1 - F(t)$, that is, $\lambda(t) = \alpha\theta(\theta t)^{\alpha-1}$. Note that, when $\alpha = 1$, the failure rate is constant and the Weibull distribution reduces to the exponential distribution. The failure rate is increasing with time if $\alpha > 1$, while decreasing if $0 < \alpha < 1$.

Since all online and spare sensors used for the given channel are assumed to be working initially, that is, $P_0(0) = 1$, and the sum of all probabilities at any instance equals unity, that is, $\sum_{k=0}^{11} P_k(t) = 1$, the time profiles of all state probabilities can be made available by numerically integrating eqs 8−18 and the average availability of this channel can then be computed according to the following formula:

$$\overline{\mathrm{Av}}^{\mathrm{Corr}}(m, n, k) = \frac{1}{H}\int_0^H \left[\sum_{j=0}^{m-n}\sum_{i=0}^{n-k} P_{j(n+1)+i}(t)\right] dt \quad (20)$$

where H is the total length of time horizon. Note that, since the hardware configuration cannot be changed during operation, only a single time-averaged availability is needed to produce the corresponding design specifications. However, since the alarm structure is not given a priori, the numerical value of average availability for every possible combination of m, n, and k must be computed in advance and an optimal one can be identified after solving the proposed optimization problem.

Finally, note that the expected numbers of repairs and replacements of the sensors can be approximated with the following two formulas respectively:[27]

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

$$\mathrm{ENRpr}(m, n) \approx \mu \int_0^H \left(\sum_{j=1}^{m-n} P_{j(n+1)}(t) + \sum_{i=1}^{n} P_{(m-n)(n+1)+i}(t) \right) \mathrm{d}t \tag{21}$$

$$\mathrm{ENRpl}(m, n) \approx \varepsilon \int_0^H \left(\sum_{j=0}^{m-n-1} \sum_{i=1}^{n} P_{j(n+1)+i}(t) \right) \mathrm{d}t \tag{22}$$

Preventive Maintenance Policy. The passive components in shutdown subsystem, such as the solenoid valves, the safety valves, and the rupture discs, are operated only after the unsafe state is detected, while in the normal operation these components are left idle. Therefore, the FD failures of these components generally cannot be observed online, and such failures are referred to as the *unrevealed* or *hidden* failures. A proper preventive maintenance policy must therefore be put in place to keep the availability of the shutdown subsystem above an acceptable level. In this study, the maintenance tasks are restricted to those associated with the periodic inspections, repairs, and replacements of passive components. The proposed strategy is summarized as follows:

(i) A failed unit should be repaired immediately after inspection so as to bring back the working state; that is, its availability is supposed to be raised to the value of one at that instance. It is further assumed that inspection and repair can be completed almost instantaneously.

(ii) It is also assumed that the repair is done minimally so that the failed unit is restored to the aged normal condition; that is, it is "as-bad-as-old." More specifically, the *failure rate* of the repaired unit should be exactly the same as that of a continuously functioning (and aging) unit at the time of inspection.

(iii) If an inspected unit is in a functioning state, it should be left online. Since the normal condition is *confirmed* (with 100% certainty) by inspection, the corresponding availability should be brought back to one. However, the failure rate should be unaffected since the same functional unit stays continuously online before and after the inspection.

Figure 7 shows the typical time profiles of both availability and failure rate of a passive component under preventive maintenance. The corresponding Markov model for the time period between consecutive inspections can be found in Figure 8. Notice that nodes N and F represent the normal and failed states of a shutdown unit respectively. Their probabilities, that is, $P_N(t)$ and $P_F(t)$, can be determined with the following equations:

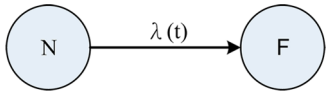

Figure 8. Markov diagram for a passive component.

$$\frac{\mathrm{d}P_F(t)}{\mathrm{d}t} = \lambda(t)P_N(t) \tag{23}$$

$$P_N(t) + P_F(t) = 1 \tag{24}$$

By introducing the mathematical expression for failure rate $\lambda(t)$ of the Weibull distribution and then solving eqs 23 and 24, one can derive a formula for computing the availability of a shutdown unit at any time between two consecutive inspections:

$$\mathrm{Av}^{\mathrm{Prev}}(t) = P_N(t) = \mathrm{e}^{(\tau_p)^\alpha - (t)^\alpha}; \quad \tau_p \le t \le \tau_{p+1} \tag{25}$$

where τ_p denotes the time at the p^{th} inspection and p = 0, 1, 2, ..., I. Notice that τ_0 = 0,

$$\tau_1 < \tau_2 < \cdots < \tau_I < H \tag{26}$$

and $\tau_{I+1} \ge H$, where H and I respectively represent the system lifetime (which is a given constant) and the total number of inspections (which is a design variable).

To simplify model formulation, let us further assume that the maintenance schedule can be adjusted so as to make the availabilities at the instances just before inspections identical:

$$\mathrm{Av}^{\mathrm{prev}}(\tau_1) = \mathrm{Av}^{\mathrm{prev}}(\tau_2) = \cdots = \mathrm{Av}^{\mathrm{prev}}(\tau_I) \tag{27}$$

From eqs 25−27, one can deduce that the time for conducting the p^{th} inspection should be

$$\tau_p = (p)^{1/\alpha}\tau_1 \tag{28}$$

Also, based on the additional assumption that the availability within each inspection interval can be closely approximated with a linear function of time, the average availability of every shutdown unit can be estimated by

$$\overline{\mathrm{Av}}^{\mathrm{Prev}} \cong \frac{1}{2}(1 + \mathrm{e}^{-(\theta\tau_1)^\alpha}) \tag{29}$$

The proposed mathematical programming model is further simplified in this study to facilitate identification of a proper τ_1 and the corresponding inspection schedule on the basis of eq 28. Specifically, the total number of inspections (i.e., I) is treated as a decision parameter in the optimization problem. By imposing two extra constraints, that is, $\tau_{I+1} = H$ and $\mathrm{Av}^{\mathrm{prev}}(\tau_I) = \mathrm{Av}^{\mathrm{prev}}(\tau_{I+1})$, one can then utilize the following formula for computing τ_1 according to any selected I:

$$\tau_1 = \frac{H}{(I+1)^{1/\alpha}} \tag{30}$$

4. EXPECTED LIFE-CYCLE LOSS

Let us assume that the protected process is operated under the normal conditions (ξ = 0) *initially* and may enter the unsafe sate (ξ = 1) at any later time. To be specific, let us further use p to denote the probability that this state transition action takes place at an instance in the intended operation life, that is,

$$p = \Pr\{T^S \le H\} \tag{31}$$

where T^S is a random variable that denotes the state transition time.

If a k_i -out-of-n_i voting gate is used in the i^{th} alarm channel to confirm this unsafe state, the conditional probabilities associated with the FS and FD failures (denoted respectively as A_i and B_i) can be calculated with following formulas:

$$A_i = 1 - (1 - a_i^{k_i})^{n_i!/k_i!} \tag{32}$$

$$B_i = 1 - \overline{\mathrm{Av}}_i^{\mathrm{Corr}} \tag{33}$$

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

where, a_i is the *constant* FS probability of a single sensor in the i^{th} channel, and $\overline{Av}_i^{Corr}$ is the average availability of the i^{th} alarm channel evaluated on the basis of eq 20. If the outputs of the alarm channels are statistically independent, the conditional probabilities of FS and FD failures of the entire alarm subsystem can be expressed respectively as[27]

$$P_{FS}^{AL} = \sum_{\mathbf{y}} f(\mathbf{y}) \Pr\{\mathbf{y}|\xi = 0\} \tag{34}$$

$$P_{FD}^{AL} = \sum_{\mathbf{y}} [1 - f(\mathbf{y})] \Pr\{\mathbf{y}|\xi = 1\} \tag{35}$$

where

$$\Pr\{\mathbf{y}|\xi = 0\} = \prod_{i=1}^{M} [A_i^{y_i}(1 - A_i)^{1-y_i}] \tag{36}$$

$$\Pr\{\mathbf{y}|\xi = 1\} = \prod_{i=1}^{M} [B_i^{1-y_i}(1 - B_i)^{y_i}] \tag{37}$$

The above formulation can be further generalized by incorporating additional possibilities of FS and FD failures in the shutdown subsystem (see Figure 9). Scenarios 2 and 4 can

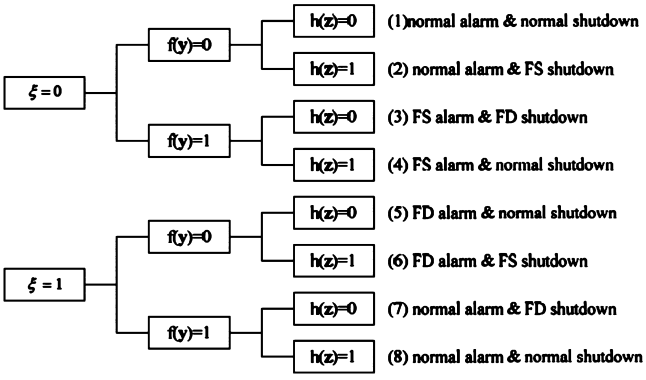

Figure 9. All possible scenarios of a protective system.

be classified as FS interlock failures, whereas scenarios 5 and 7 are the corresponding FD failures. The probabilities of both subsystems fail simultaneously (i.e., scenarios 3 and 6) are assumed to be very low and can be ignored.

Because an OR logic is always adopted in shutdown configuration, the corresponding conditional probabilities of FS and FD failures can be expressed as

$$P_{FS}^{SD} = \Pr\{h(\mathbf{z}) = 1|f(\mathbf{y}) = 0\} = 1 - \prod_{j=1}^{N} (1 - \alpha_j) \tag{38}$$

$$P_{FD}^{SD} = \Pr\{h(\mathbf{z}) = 0|f(\mathbf{y}) = 1\} = \prod_{j=1}^{N} \beta_j \tag{39}$$

where α_j and β_j represent the conditional probabilities of FS and FD failures, respectively, of the j^{th} shutdown unit. In this study, α_j is regarded as a given constant parameter, while

$$\beta_j = 1 - \overline{Av}_J^{Prev} \tag{40}$$

and $\overline{Av}_J^{Prev}$ is the average availability of the j^{th} shutdown unit, which can be evaluated according to eq 29. On the basis of the aforementioned conditional probabilities, a compact expression of the expected loss of interlock can be derived:[27]

$$L_{PT,1}^{LC} = (1 - P_{FS}^{SD})C_b p + P_{FS}^{SD} C_a (1 - p) - (1 - P_{FS}^{SD} - P_{FD}^{SD}) \sum_{\mathbf{y}} f(\mathbf{y}) g(\mathbf{y}) \tag{41}$$

where

$$g(\mathbf{y}) = C_b p \Pr\{\mathbf{y}|\xi = 1\} - C_a (1 - p) \Pr\{\mathbf{y}|\xi = 0\} \tag{42}$$

In this equation, C_a and C_b denote the financial losses incurred from the FS and FD interlock failures, respectively.

5. TOTAL LIFE-CYCLE COSTS

Since the spare-supported corrective maintenance policy is employed in this study to enhance the availability of every sensor channel, the related costs can be attributed to those used for the purchase, repair, and replacement of sensors. Specifically, the total life-cycle cost of alarm channel i can be expressed as

$$LCC_i^{AL} = m \times PCS_i + ENRpr_i(m, n) \times RprsC_i + ENRpl_i(m, n) \times RplsC_i \tag{43}$$

where PCS_i denotes the purchase cost of one sensor in channel i; $RprsC_i$ and $RplsC_i$ respectively denote the repair and replacement costs. Notice that the expected number of repair and replacement, that is, $ENRpr_i(m,n)$ and $ENRpl_i(m,n)$, can be computed according to eqs 21 and 22.

On the other hand, because the preventive maintenance strategy is used to upkeep the shutdown subsystem, the corresponding total life-cycle cost should include the purchase, inspection and repair costs. Let us use the symbol $\tau_{j,p}$ to represent the instance when the p^{th} inspection is performed on shutdown unit j. The life-cycle cost associated with this unit can thus be expressed as

$$LCC_j^{SD} = PCV_j + I_j \times InspC_j + RprC_j \times \sum_{p=1}^{I_j} \{1 - \exp[(\theta_j \tau_{j,p-1})^{\alpha_j} - (\theta_j \tau_{j,p})^{\alpha_j}]\} \tag{44}$$

where PCV_j denotes the purchase cost of unit j; $InspC_j$ and $RprC_j$ respectively represent the corresponding inspection and repair costs; I_j is the number of inspections performed on unit j.

6. STRUCTURE REPRESENTATION

Since the exact alarm structure is unknown before solving the optimization problem, a set of binary variables must be introduced in the mathematical programming model to enumerate all possible alarm configurations in the superstructure,[15] that is,

$$w_{i,m,n,k} = \begin{cases} 1 & \text{if } i^{th} \text{ channel with } m \text{ purchased sensors, } n \text{ online sensors, and } k\text{-out-of-}n \text{ voting gate is selected for implementation} \\ 0 & \text{otherwise} \end{cases} \tag{45}$$

To ensure reasonable solutions, the following inequality constraints must also be imposed:

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

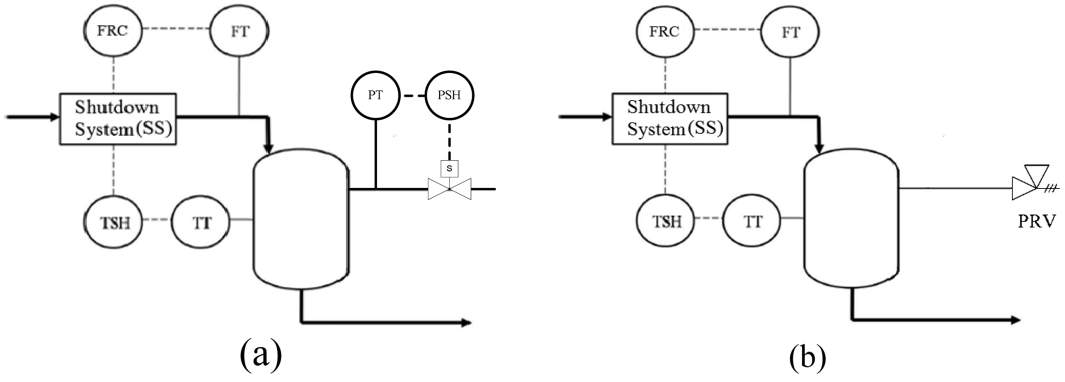

Figure 10. Two alternative protective schemes used on a fictitious CSTR reactor: (a) scheme A; (b) scheme B.

$$\sum_{m=1}^{\Omega_i} \sum_{n\le m} \sum_{k\le n} w_{i,m,n,k} \le 1 \tag{46}$$

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

where M is the maximum number of channels incorporated in the alarm subsystem, and Ω_i is the maximum allowable number of purchased sensors for the i^{th} channel. The total life-cycle cost of the alarm subsystem can thus be expressed in a general form as

$$C_{\text{AL}}^{\text{LC}} = \sum_{i=1}^{M} \text{LCC}_i^{\text{AL}} \left(\sum_{m=1}^{\Omega_i} \sum_{n\le m} \sum_{k\le n} w_{i,m,n,k} \right) \tag{48}$$

where LCC_i^{AL} can be determined according to eq 43.

Because the total number of shutdown units is also unknown, another binary variable is adopted to determine whether the j^{th} unit in shutdown superstructure is selected for online implementation, that is,

$$s_j = \begin{cases} 1 & \text{if the } j^{\text{th}} \text{ shutdown unit is selected} \\ 0 & \text{otherwise} \end{cases} \tag{49}$$

A similar inequality constraint must be imposed on these binary variables, that is,

$$\sum_{j=1}^{N} s_j \ge 1 \tag{50}$$

The total life-cycle cost for a shutdown subsystem can thus be calculated accordingly as

$$C_{\text{SD}}^{\text{LC}} = \sum_{j=1}^{N} s_j \times \text{LCC}_j^{\text{SD}} \tag{51}$$

where LCC_j^{SD} is expressed in eq 44.

Finally, note that eqs 32−42 are used to compute the expected life-cycle loss associated with a *given* interlock structure. If an optimal system configuration is to be identified from superstructures, then these equations must be modified with the aforementioned binary variables. Specifically, eqs 36 and 37 should be replaced with

$$\Pr\{\mathbf{y}|\xi = 0\} = \prod_{i=1}^{M} \left[\sum_{m=1}^{\Omega_i} \sum_{n\le m} \sum_{k\le n} w_{i,m,n,k} [A_i^{y_i}(1 - A_i)^{1-y_i}] + (1 - y_i)\left(1 - \sum_{m=1}^{\Omega_i} \sum_{n\le m} \sum_{k\le n} w_{i,m,n,k}\right) \right] \tag{52}$$

$$\Pr\{\mathbf{y}|\xi = 1\} = \prod_{i=1}^{M} \left[\sum_{m=1}^{\Omega_i} \sum_{n\le m} \sum_{k\le n} w_{i,m,n,k} [B_i^{1-y_i}(1 - B_i)^{y_i}] + (1 - y_i)\left(1 - \sum_{m=1}^{\Omega_i} \sum_{n\le m} \sum_{k\le n} w_{i,m,n,k}\right) \right] \tag{53}$$

while eqs 38 and 39 should be replaced with

$$P_{\text{FS}}^{\text{SD}} = 1 - \prod_{j=1}^{N} (1 - \alpha_j s_j) \tag{54}$$

$$P_{\text{FD}}^{\text{SD}} = \prod_{j=1}^{N} \beta_j^{s_j} \tag{55}$$

7. MULTILAYER DESIGNS

The aforementioned generic formulas for computing the total life-cycle costs of alarm and shutdown subsystems in a single-layer interlock can be directly extended to produce the corresponding cost estimates for any multilayer design, while an additional event tree analysis must be performed to facilitate calculation of the corresponding expected life-cycle loss. To illustrate the latter approach, let us consider the specific examples presented in Figure 10, that is, the two alternative two-layer interlocks (scheme A and scheme B) installed on a fictitious CSTR reactor. The lower-layer configurations of both schemes are essentially the same, that is, a two-channel alarm subsystem connected to a shutdown subsystem that cuts off the reactor feed on demand. An interlock FD failure in this layer inevitably causes excessive flow, high temperature, or a combination of both. As a result, the reactor pressure could be driven to a dangerously high level. To prevent the catastrophic outcomes of a runaway reaction and/or explosion, a relief mechanism must also be put in place as an upper-layer interlock for venting the reactor contents at a set pressure. The pressure-relief system in scheme A consists of a pressure sensor/transmitter (PT), a switch (PSH), and a solenoid valve (PRV), while the alternative (scheme B) is simply a safety valve or rupture disc.

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

For the sake of illustration clarity, let us introduce the following two binary variables to characterize the process states:

$$x^{FT} = \begin{cases} 1 & \text{if the inlet flow or reactor temperature exceeds the designated limit} \\ 0 & \text{otherwise} \end{cases} \quad (56)$$

$$x^{P} = \begin{cases} 1 & \text{if the reactor pressure exceeds the designated limit} \\ 0 & \text{otherwise} \end{cases} \quad (57)$$

Since the lower-layer interlock is triggered when the temperature or flow measurements go beyond the acceptable limits, all possible scenarios can be described with two event trees (see Figure 11). The branch labels FS^{FT} and FS^{P} in the first tree

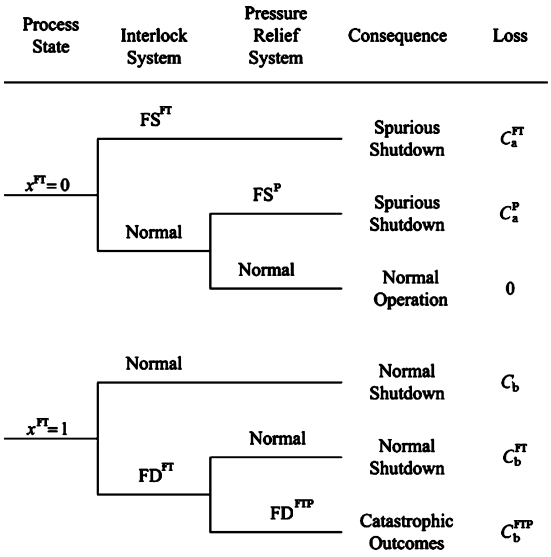

Figure 11. Event trees for a CSTR with two protection layers.

represent the fail-safe failures of the lower and upper protection layers respectively, while FD^{FT} and FD^{FTP} in the second tree denote the fail-dangerous failures of the corresponding interlocks. It should be noted that the financial losses of all possible scenarios are listed in the last column in Figure 11 and, in general, $C_a^{FT} < C_a^{P} < C_b^{FT} < C_b^{FTP}$. Finally, note that the inherent cost of normal shutdown operation in the lower layer, that is, C_b, is not considered in this study since no failures are involved in this situation.

The expected life-cycle loss of operating any of the two protective systems in Figure 10 can be expressed in a general form according to the two event trees given in Figure 11. In particular

$$L_{PT,2}^{LC} = C_a^{FT}(1 - p^{FT})\Pr\{FS^{FT}\} + C_a^{P}(1 - p^{FT}) \times (1 - \Pr\{FS^{FT}\})\Pr\{FS^{P}\} + C_b^{FT}p^{FT}\Pr\{FD^{FT}\} \times (1 - \Pr\{FD^{P}\}) + C_b^{FTP}p^{FT}\Pr\{FD^{FT}\}\Pr\{FD^{P}\} \quad (58)$$

where $p^{FT} = \Pr\{T^{FT} \leq H\}$ and T^{FT} denotes the instance when the transition from $x^{FT} = 0$ to $x^{FT} = 1$ occurs. It should also be noted that the product $p^{FT}\Pr\{FD^{FT}\}$ in the fourth term can be expressed as

$$p^{FT}\Pr\{FD^{FT}\} \cong \Pr\{T^{P} \leq H\} = p^{P} \quad (59)$$

where T^{P} denotes the instance when the transition from $x^{P} = 0$ to $x^{P} = 1$ takes place.

For scheme A, the conditional probabilities of FS and FD failures in eq 58 can be expressed as[15]

$$\Pr\{FS^{FT}\} = P_{FS}^{SD^{FT}} + (1 - P_{FS}^{SD^{FT}} - P_{FD}^{SD^{FT}}) \times \sum_{\mathbf{y}^{FT}} f^{FT}(\mathbf{y}^{FT})\Pr\{\mathbf{y}^{FT}|x^{FT} = 0\} \quad (60)$$

$$\Pr\{FD^{FT}\} = (1 - P_{FS}^{SD^{FT}}) - (1 - P_{FS}^{SD^{FT}} - P_{FD}^{SD^{FT}}) \times \sum_{\mathbf{y}^{FT}} f^{FT}(\mathbf{y}^{FT})\Pr\{\mathbf{y}^{FT}|x^{FT} = 1\} \quad (61)$$

$$\Pr\{FS^{P}\} = P_{FS}^{SD^{P}} + (1 - P_{FS}^{SD^{P}} - P_{FD}^{SD^{P}}) \times \sum_{\mathbf{y}^{P}} f^{P}(\mathbf{y}^{P})\Pr\{\mathbf{y}^{P}|x^{P} = 0\} \quad (62)$$

$$\Pr\{FD^{P}\} = (1 - P_{FS}^{SD^{P}}) - (1 - P_{FS}^{SD^{P}} - P_{FD}^{SD^{P}}) \times \sum_{\mathbf{y}^{P}} f^{P}(\mathbf{y}^{P})\Pr\{\mathbf{y}^{P}|x^{P} = 1\} \quad (63)$$

where $\mathbf{y}^{FT}$ and $\mathbf{y}^{P}$ denote respectively the outputs of flow/temperature and pressure channels; $f^{FT}(\bullet)$ and $f^{P}(\bullet)$ represent the alarm functions in the lower and upper layers respectively and $h^{FT}(\bullet)$ and $h^{P}(\bullet)$ are the corresponding shutdown functions. In the above equations, $P_{FS}^{SD^{FT}}$ and $P_{FS}^{SD^{P}}$ respectively represent the conditional probabilities of FS failures of the shutdown subsystem in the lower- and upper-layer interlocks, while $P_{FD}^{SD^{FT}}$ and $P_{FS}^{SD^{P}}$ denote the conditional probabilities of corresponding FD failures. These probabilities can be computed according to eqs 54 and 55. Finally, the other conditional probabilities in eqs 60−63 can be expressed by placing the superscripts η (= FT or P) into eqs 52 and 53:

$$\Pr\{\mathbf{y}^{\eta}|x^{\eta} = 0\} = \prod_{i=1}^{M^{\eta}}\Big[\sum_{m=1}^{\Omega_i^{\eta}}\sum_{n\leq m}\sum_{k\leq n} w_{i,m,n,k}^{\eta}(A_i^{\eta})^{y_i^{\eta}}(1 - A_i^{\eta})^{1-y_i^{\eta}} + (1 - y_i^{\eta})\Big(1 - \sum_{m=1}^{\Omega_i^{\eta}}\sum_{n\leq m}\sum_{k\leq n} w_{i,m,n,k}^{\eta}\Big)\Big] \quad (64)$$

$$\Pr\{\mathbf{y}^{\eta}|x^{\eta} = 1\} = \prod_{i=1}^{\Omega_i^{\eta}}\Big[\sum_{m=1}^{\Omega^{\eta}}\sum_{n\leq m}\sum_{k\leq n} w_{i,m,n,k}^{\eta}(B_i^{\eta})^{1-y_i^{\eta}}(1 - B_i^{\eta})^{y_i^{\eta}} + (1 - y_i^{\eta})\Big(1 - \sum_{m=1}^{\Omega^{\eta}}\sum_{n\leq m}\sum_{k\leq n} w_{i,m,n,k}^{\eta}\Big)\Big] \quad (65)$$

Note that, in the case of scheme B, all aforementioned formulations in this section are still valid except eqs 62 and 63. Since no pressure sensors are needed, the conditional probabilities of FS and FD failures in the upper protection layer should be represented as[15]

$$\Pr\{FS^{P}\} = P_{FS}^{SD} = 1 - \prod_{j=1}^{N}(1 - \alpha'_j s_j) \quad (66)$$

$$\Pr\{FD^{P}\} = P_{FD}^{SD} = \prod_{j=1}^{N}\beta'_j{}^{s_j} \quad (67)$$

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

where α'_j and β'_j represent the conditional probabilities of the FS and FD failures of the j^{th} shutdown unit in the pressure-relief system.

8. OBJECTIVE FUNCTIONS

The total expected life-cycle expenditure is used in the present study as the objective function for generating the optimal interlock configuration and maintenance policies. In the case of single-layer designs, this function should be written as

$$\text{obj}_1 = C_{AL}^{LC} + C_{SD}^{LC} + L_{PT,1}^{LC} \tag{68}$$

The total life-cycle costs of alarm and shutdown subsystems (C_{AL}^{LC} and C_{SD}^{LC}) can be computed with the explicit formulas given in eqs 48 and 51, respectively, while the expected life-cycle loss ($L_{PT,1}^{LC}$) should be determined according to eqs 32−35, 40−42, and 52−55. Notice also that there may be a need to impose an initial budget constraint in certain applications, that is,

$$C_{AL}^{PC} + C_{SD}^{PC} \le C_{budget} \tag{69}$$

where the budget limit C_{budget} is a model parameter and C_{AL}^{PC} and C_{SD}^{PC} denote the purchase costs of sensors and shutdown units, respectively.

As for the two specific two-layer interlocks described in Figure 10, their design objectives can be expressed respectively as

$$\text{obj}_{2A} = (C_{AL,FT}^{LC} + C_{SD,FT}^{LC}) + (C_{AL,P}^{LC} + C_{SD,P}^{LC}) + L_{PT,2A}^{LC} \tag{70}$$

$$\text{obj}_{2B} = (C_{AL,FT}^{LC} + C_{SD,FT}^{LC}) + C_{SD,P}^{LC} + L_{PT,2B}^{LC} \tag{71}$$

where $C_{AL,FT}^{LC}$ and $C_{SD,FT}^{LC}$ respectively denote the life-cycle costs of alarm and shutdown subsystems in the lower-layer interlock and $C_{AL,P}^{LC}$ and $C_{SD,P}^{LC}$ represent the corresponding life-cycle costs in the upper layer; $L_{PT,2A}^{LC}$ and $L_{PT,2B}^{LC}$ denote the expected life-cycle losses of scheme A and scheme B respectively. Finally, the following budget constraints may also be necessary:

$$(C_{AL,FT}^{PC} + C_{SD,FT}^{PC}) + (C_{AL,P}^{PC} + C_{SD,P}^{PC}) \le C_{budget}^{2A} \tag{72}$$

$$(C_{AL,FT}^{PC} + C_{SD,FT}^{PC}) + C_{SD,P}^{PC} \le C_{budget}^{2B} \tag{73}$$

where $C_{AL,FT}^{PC}$ and $C_{SD,FT}^{PC}$ respectively denote the total purchase costs of alarm and shutdown subsystems in the lower-layer interlock; $C_{AL,P}^{PC}$ and $C_{SD,P}^{PC}$ respectively denote the total purchase costs of alarm and shutdown subsystems in the upper layer; C_{budget}^{2A} and C_{budget}^{2B} are the model parameters used to represent the budget limits for scheme A and scheme B, respectively.

9. CASE STUDIES

The feasibility and effectiveness of the proposed strategy are demonstrated in this paper with case studies. It is assumed that the operating life (H) is 5 years in all cases and the probability of the initial unsafe state is 0.2. All cost data are represented in terms of the so-called *relative cost unit* (rcu), and these values are chosen primarily to facilitate proper trade-offs in the optimization problems. The mixed integer nonlinear program (MINLP) in the following examples were solved with the solver BARON in the GAMS environment on a Pentium 4 3.00 GHz PC.

Case 1: The Single-Layer Interlocks for a CSTR Reactor. Since the lower protection layers installed on the two CSTR reactors in Figure 10 are identical, let us consider just one of them and, for illustration convenience, ignore the upper layers in the present example. The financial losses incurred from the FS and FD interlock failures are assumed to be $C_a = 1 \times 10^4$ rcu and $C_b = 1 \times 10^7$ rcu, respectively. The model parameters of flow and temperature sensors and solenoid valves can be found in Table 1.

Table 1. Model Parameters of Sensors and Valves in the CSTR Interlock

model param.		flow sensor	temp. sensor	solenoid valve
failure rate param.	shape param., α	1.3	1.7	1.6
	scale param. (1/month), θ	0.04	0.07	0.06
repair rate (1/month), μ		0.6	0.8	
replace rate (1/month), ε		30	30	
purchase cost (rcu), PC		350	100	200
repair cost (rcu), RrC		5	2	3
replacement cost (rcu), RplC		3	2	
inspection cost (rcu), InspC				20
probability of FS failure, $a_{i,m}$		0.1	0.15	
probability of FS failure, $\alpha_{i,m}$				0.1

As mentioned before, the initial unsafe state is detected with flow and temperature channels ($M = 2$). Let us assume that there are at most four online sensors used in every channel and that each is supported with at most 10 spares (i.e., $\Omega_i = 14$; $i = 1, 2$). Based on these assumptions and eqs 8−20, the average channel availabilities can be computed for all possible combinations of m, n, and k. For the sake of completeness, their numerical values are provided in the Supporting Information. On the other hand, it is assumed that at most 5 solenoid valves can be employed in the shutdown subsystem and at most 24 inspections can be performed over the entire operation life. It should be noted that the aforementioned upper bounds are adopted only for the purpose of facilitating convergence. Without these limits, the iterative computation process may be extremely inefficient.

By solving the corresponding MINLP model, the optimal design specifications and maintenance policies can be obtained and these optimization results are presented in Table 2. From row 2 to row 6 in Table 2, it can be observed that the lowest objective value can be reached with a relatively large budget, that is, $C_{budget} \ge 2350$. This is due to the fact that, in this particular example, the FD failures exert an overwhelming impact on the expected life-cycle loss. Removing the critical components in a protective system inevitably results in a significant increase in the probability of FD failures. Thus, if the budget is enough (e.g., run 1−1), it is preferable to introduce a high level of hardware redundancy into the interlock.

Row 7 to row 11 in Table 2 show that, although the flow sensors are more reliable, fewer of them are required in most cases. This is probably due to the fact that a temperature sensor costs lower. As the budget gradually decreases (see run 1−2, run 1−3, and run 1−4), the required cutbacks are realized by reducing the number of temperature sensors without causing significant deterioration in the system reliability. Decreasing the initial budget from 1950 rcu (run 1−4) to 1850 rcu (run 1−5) results in an alarm reconfiguration; that is, the more expensive flow measurements are abandoned altogether, and consequently, the two-channel scheme is replaced with a single

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

Table 2. Budget Constrained Optimal Interlock Structures and Their Maintenance Programs for a CSTR Reactor—One Protection Layer and Two Alarm Channels

run		1−1	1−2	1−3	1−4	1−5	1−6	1−7	1−8	1−9
initial budget (rcu)			2350	2250	1950	1850	1700	1000	800	600
objective (rcu)		8711.4	8712.6	8735.4	9416.5	11018.8	11337.8	11666.7	15072.6	45127.9
total PC (rcu)		2400	2300	2000	1900	1800	1200	1000	800	600
total Rc (rcu)		1795.5	1793.8	1753.6	2556.9	1773.1	1725.4	2034.3	1535.1	1035.8
total loss (rcu)		4515.9	4618.8	4981.7	4959.6	7445.7	8412.4	8632.4	12737.5	43492.0
voting gate	flow	1oo1	1oo1	1oo1	1oo1					
	temp.	2oo2	2oo2	1oo1	1oo1	1oo2	1oo1	1oo1	1oo1	1oo1
spares	flow	1	1	1	1					
	temp.	5	4	2	1	6	1	1	1	1
alarm logic		1oo2	1oo2	1oo2	1oo2	1oo1	1oo1	1oo1	1oo1	1oo1
no. valves		5	5	5	5	5	5	4	3	2
first inspection, τ_1 (month)		10.21	10.21	10.21	10.21	10.21	10.21	8.03	8.03	8.03
no. inspections		16	16	16	16	16	16	24	24	24

Table 3. Budget Constrained Optimal Interlock Structures and Their Maintenance Programs for a CSTR Reactor—One Protection Layer and One Temperature Channel

run	1−10	1−11	1−12	1−13	1−14	1−15	1−16	1−17	1−18
initial budget (rcu)		2150	2050	1950	1850	1750	1000	800	600
objective (rcu)	9300.8	9384.9	9612.0	10096	11018.8	11337.7	11666.7	15072.6	45127.9
total PC (rcu)	2200	2100	2000	1900	1800	1200	1000	800	600
total Rc (rcu)	1774.2	1774.1	1774.0	1773.7	1773.1	1725.4	2034.3	1535.1	1035.8
total loss (rcu)	5326.6	5510.7	5838.1	6422.3	7445.7	8412.3	8632.4	12737.5	43492.0
voting gate	1oo2	1oo2	1oo2	1oo2	1oo2	1oo1	1oo1	1oo1	1oo1
spares	10	9	8	7	6	1	1	1	1
no. valves	5	5	5	5	5	5	4	3	2
first inspection, τ_1 (month)	10.21	10.21	10.21	10.21	10.21	10.21	8.03	8.03	8.03
no. inspections	16	16	16	16	16	16	24	24	24

Table 4. Budget Constrained Optimal Interlock Structures and Their Maintenance Programs for a CSTR Reactor—One Protection Layer and One Flow Channel

run	1−19	1−20	1−21	1−22	1−23	1−24	1−25
initial budget (rcu)		2700	2300	2000	1500	1300	1200
objective (rcu)	9169.5	9206.5	10662.6	11823.7	12152.6	15558.6	45613.8
total PC (rcu)	2750	2400	2050	1700	1500	1300	1100
total Rc (rcu)	1736.2	1735.7	1712.2	1711.3	2020.2	1521.0	1021.8
total loss (rcu)	4683.3	5070.8	6900.4	8412.4	8632.4	12737.5	43492.0
voting gate	1oo2	1oo2	1oo1	1oo1	1oo1	1oo1	1oo1
spares	3	2	2	1	1	1	1
no. valves	5	5	5	5	4	3	2
first inspection, τ_1 (month)	10.21	10.21	10.21	10.21	8.03	8.03	8.03
no. inspections	16	16	16	16	24	24	24

temperature channel. Since eliminating an alarm channel inevitably causes an increase in the probability of FD interlock failures, a larger number of temperature sensors (2 online and 6 offline) is adopted in run 1−5 to offset its effects. To facilitate the more stringent budget constraints in runs 1−6 to 1−9, it is necessary to further lower both the numbers of online and spare sensors to 1 and then reduce the number of solenoid valves to 2.

The shutdown configuration and the corresponding inspection schedule are outlined in rows 12−14 in Table 2. The optimal numbers of solenoid valves and their inspections appears to be insensitive to the initial budget cut until when C_{budget} reaches 1700 rcu. In runs 1−7, 1−8, and 1−9, it becomes necessary to carry out inspections as often as possible so as to compensate for the extra financial loss caused by installing fewer valves. Finally, notice that the best inspection intervals can be determined by substituting the optimal value of τ_1 into eq 28. It should also be noted that the interval lengths produced with the existing method[15] should be all identical in this case.

Additional optimization results obtained with the single-channel superstructures are presented in Tables 3 and 4. The former shows the interlock designs with only temperature sensors, while the latter provides those with flow sensors. By comparing runs 1−1, 1−10, and 1−19, it can be observed that the objective value achieved with a two-channel alarm subsystem is lower than those with the single-channel ones. As mentioned before, a flow sensor is more reliable but more expensive than a temperature sensor. These features are clearly reflected in the results obtained in run 1−10 and run 1−19. The expected loss of a standalone flow channel is far less than that of a standalone temperature channel, while the purchase

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

cost of the former is larger than that of latter. Thus, it is quite reasonable to achieve a better trade-off with the two-channel alarm. Note especially that the expected life-cycle loss in run 1−1 is the lowest among all 25 runs.

Case 2: The Two-Layer Interlocks for a CSTR Reactor. Let us next examine the two-layer scheme B in Figure 10 and assume that the financial losses resulting from all failure-induced scenarios in Figure 11 can be estimated, that is, $C_a^{FT} = 1 \times 10^4$ rcu, $C_b^{FT} = 1 \times 10^5$ rcu, $C_a^{P} = 5 \times 10^4$ rcu, and $C_b^{FTP} = 1 \times 10^7$ rcu. Note that the value of C_a^{FT} in this case is chosen to be the same as the financial loss due to a FS interlock failure in Case 1 since these two scenarios are essentially equivalent. Similarly, C_b^{FTP} is set to be the loss of a FD interlock failure in Case 1. All model parameters of the components in the first layer can be found in Table 1. As for the second layer, it is assumed that there are at most 5 relief valves and at most 24 inspections can be performed. The model parameters for the pressure relief calves are listed in Table 5.

Table 5. Model Parameters of Pressure-Relief Valves in CSTR Interlock

specification param.		value
failure rate param.	shape param., α	1.5
	scale param. (1/month), θ	0.05
purchase cost (rcu), TripPC		200
repair cost (rcu), TripRrC		3
inspection cost (rcu), InspC		20
probability of FS failure, $\alpha_{i,m}$		0.1

The corresponding optimization results are presented in Table 6. A number of interesting features can be identified:

- Note that the alarm subsystem in the first layer only employs a single temperature channel. This is probably because the two-layer structure is too reliable to justify the use of more than one alarm channel, and thus, the cheaper one is chosen despite its low reliability.
- It can be seen from runs 2−1 to 2−7 that the pressure-relief valves (PRVs) adopted in the second layer are more than the solenoid valves in the first layer. This is due to the fact that the failure rate of a PRV is lower than that of a solenoid valve. However, when the initial budget drops below 1400 rcu (i.e., run 2−8 and run 2−9), the cheaper solenoid valves are preferred over the pressure-relief valves.
- Notice from run 2−1 to run 2−7 that the solenoid valves are required to be inspected 24 times (which is the upper bound). This is due to that fact that relatively few (i.e., only two) solenoid valves are adopted. On the other hand, the inspection number for the second layer varies with the number of installed relief valves, 11 inspections for 5 PRVs, 16 or 17 for 4 PRVs, and the maximum level of 24 inspections in the case of 3 PRVs. Since fewer PRVs naturally bring down the subsystem availability, inspections should therefore be performed more frequently to compensate the unfavorable effects. This pattern changes when the initial budget is lower than 1400 rcu (i.e., run 2−8 and run 2−9). Both types of valves require similar inspection frequencies which increase as the budget decreases.
- By comparing the best two-layer design (run 2−1) with its single-layer counterpart (run 1−1), it can be observed that the former is clearly a better choice. Given the same budget, the minimum objective value of the former design is lower than that of the latter. By applying the two-layer strategy, the probability of FD failures can be reduced significantly as the second layer acts as a stand-by protector in case the first-layer defense fails dangerously. More specifically, since the FD probability of the entire system equals the product the FD probabilities of individual layers, the multilayer configuration usually outperforms the single-layer counterpart.

Case 3: The Single-Layer Two-Channel Interlocks for a Fan. Let us next consider the interlock-protected fan system given in Figure 12.[28] The power supply to fan is switched off when either a high pressure is developed on the discharge side or a high vacuum on the suction side. Two pressure channels (PSH 02 and PSL 03) are installed to detect these two abnormal conditions respectively, and both are connected to switch #1 to stop the fan. Notice that triggering this switch also closes the discharge damper XCD 06 simultaneously so as to prevent reverse flow. It is assumed that the financial losses from

Table 6. Budget Constrained Optimal Interlock Structures and Their Maintenance Programs for a CSTR Reactor—Two Protection Layers and Two Alarm Channels

run		2−1	2−2	2−3	2−4	2−5	2−6	2−7	2−8	2−9
initial budget (rcu)			2500	2400	2200	2100	1850	1650	1400	1200
objective (rcu)		7975.3	7991.5	8030.0	8041.7	8043.4	8156.0	8623.7	11272.7	11558.3
total PC (rcu)		2550	2450	2300	2150	2000	1800	1650	1250	1050
total Rc (rcu)		2289.8	2184.5	2459.9	2255.2	2509.1	2419.5	2571.9	1623.2	1932.4
total loss (rcu)		3135.6	3357.0	3270.2	3636.5	3534.3	3936.5	4401.7	8399.4	8575.9
voting gate	flow									
	temp.	3oo3	3oo3	3oo3	2oo2	2oo2	2oo2	2oo2	1oo1	1oo1
spares	flow									
	temp.	6	5	6	3	4	2	3	1	1
alarm logic		1oo1	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1
no. valves	solenoid	2	2	2	2	2	2	2	4	3
	PRV	5	5	4	5	4	4	3	1	1
first inspection, τ_1 (month)	solenoid	8.03	8.03	8.03	8.03	8.03	8.03	8.03	10.61	8.23
	PRV	11.45	12.13	9.08	11.45	8.74	8.08	7.02	9.45	7.42
no. inspections	solenoid	24	24	24	24	24	24	24	15	23
	PRV	11	10	16	11	17	16	24	15	22

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

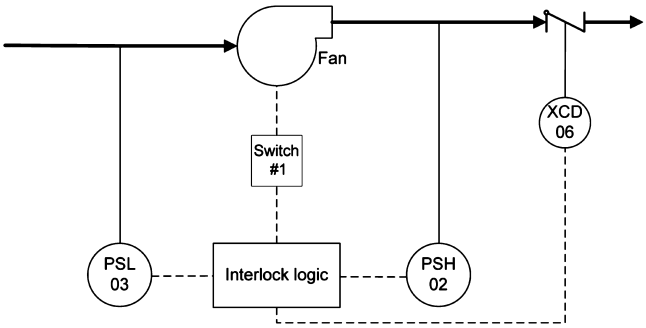

Figure 12. Interlock-protected fan system.

the FS and FD interlock failures can be estimated to be $C_a = 1 \times 10^4$ rcu and $C_b = 1 \times 10^7$ rcu, respectively.

It is also assumed that there are at most four online sensors for use in each alarm channel and that every channel is supported with at most 10 spare sensors ($\Omega_i = 14$; $i = 1, 2$). On the other hand, notice that there are actually two channels in the shutdown subsystem and the required emergency operations must both be performed successfully after an alarm is issued. In this example, it is assumed that at most 7 units can be installed in each channel and at most 99 inspections performed. From the above descriptions concerning the shutdown subsystem, it is clear that an AND logic should be applied between channels while an OR logic should be employed within the same channel. Therefore, eqs 54 and 55 must be modified accordingly:

$$P_{FS}^{SD} = \prod_{\sigma}\left[1 - \prod_{j=1}^{N}(1 - \alpha_j^{\sigma} s_j^{\sigma})\right] \tag{74}$$

$$P_{FD}^{SD} = 1 - \prod_{\sigma}\left[1 - \prod_{j=1}^{N}\beta_j^{\sigma^{s_j^{\sigma}}}\right] \tag{75}$$

where α_j^{σ} and β_j^{σ} respectively represent the FS and FD probabilities of the j^{th} unit in channel σ, s_j^{σ} is a binary variable used to reflect whether the j^{th} unit in channel σ is present; σ is a channel label, that is, switch or damper. The model parameters for the sensors and shutdown units in the fan interlock are shown in Table 7.

The corresponding optimization results are shown in Table 8. As expected, the lowest objective value is reached when the system is provided with the largest initial budget (run 3−1).

Table 7. Model Parameters for Pressure Sensors, Switches, and Dampers in Fan Interlock

specification param.		PSL 03	PSH 02	switch	damper
failure rate param.	shape param., α	1.3	1.7	1.5	1.4
	scale param. (1/month), θ	0.04	0.07	0.05	0.05
repair rate (1/month), μ		0.6	0.8		
replace rate (1/month), ε		30	30		
purchase cost (rcu), PC		350	100	200	250
repair cost (rcu), RrC		5	2	3	4
replacement cost (rcu), RplC		3	2		
inspection cost (rcu), InspC				20	20
probability of FS failure, $a_{i,m}$		0.1	0.15		
probability of FS failure, $\alpha_{i,m}$				0.1	0.15

Also, a two-channel alarm is preferred if a relatively large budget is allowed (see run 3−1 to run 3−6). Note that the purchased PSL 03 sensors are in general fewer than the PSH 02 sensors since, in the former case, the unit cost is higher. As budget decreases, the pressure sensors in PSH 02 channel are removed gradually. Since a PSH 02 sensor is less reliable, this practice is obviously adopted for the dual purposes of cutting purchase cost while minimizing the increased expected loss. As the initial budget drops below 1900 rcu (see run 3−7 to run 3−10), the two-channel alarm configuration is transformed into a single-channel one.

With a large budget, the optimal shutdown subsystem employs five switches and four dampers (see run 3−1). If the budget is reduced to 3000 rcu, additional switches must be introduced to compensate for the cutback made in the alarm subsystem (run 3−2). This practice is driven by its relatively low cost (see Table 7), and the same strategy is also adopted when the alarm subsystem is reconfigured (run 3−7). The switches and dampers are in general removed alternately to meet the requirement of decreasing budget, while the number of dampers never exceeds the number of switches. It can also be observed that the inspection frequency depends primarily on the total number of installed shutdown units. As the unit number decreases, the inspections must be performed more often to preserve the system availability.

10. CONCLUSIONS

In this study, a generic MINLP model has been developed to synthesize the optimal design configurations and the corresponding maintenance strategies for multilayer multichannel interlocks with time-variant failure rates. Specifically, the failure rates of critical components in the interlocks are characterized according to those adopted in Weibull distributions. By minimizing the total expected life-cycle expenditure, one can identify the channel types and the corresponding alarm-generating logic in the alarm subsystem, the number of spare sensors stored offline, the number of redundant sensors installed online, and the corresponding voting-gate structure in every channel, the total number of redundant units in the shutdown subsystem, and the inspection schedule of each and every unit.

Based on the results obtained in case studies, a few additional conclusions can also be drawn:

(1) The optimal design configurations and maintenance strategies are clearly sensitive to the model parameters, including the purchase, inspection, repair and replacement costs, the failure, repair and replacement rates, and the financial losses due to failures, etc.
(2) The system design cannot always be improved by adding hardware items. In other words, the total expected life-cycle expenditure reaches a minimum even without budget constraint.
(3) If the expected loss due to FD failures is relatively large and budget is sufficient, the multichannel and multilayer configurations are preferable.
(4) The number of inspections done to each shutdown unit is inversely proportional to the total number of installed units.

dx.doi.org/10.1021/ie402902q | Ind. Eng. Chem. Res. 2014, 53, 4398−4412

Table 8. Budget Constrained Optimal Interlock Structures and Their Maintenance Programs for a Fan—One Protection Layer, Two Alarms, and Two Shutdown Channels

run		3−1	3−2	3−3	3−4	3−5	3−6	3−7	3−8	3−9	3−10
initial budget (rcu)			3000	2800	2500	2200	1900	1500	1200	1000	800
objective (rcu)		9993.6	10143	10186	10492	11527	13798	15953	17924	21194	71112
total PC (rcu)		3150	3000	2750	2500	2200	1850	1400	1150	1000	750
total Rc (rcu)		3245.8	3033.6	3203.9	3712.8	4685.0	6166.1	4837.2	6062.7	7242.1	3981.8
total loss (rcu)		3597.8	4109.5	4232.2	4278.8	4641.9	5782.3	9715.2	10711	12952	66381
voting gate	PSL 03	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1				
	PSH 02	2oo2	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1	1oo1
spares	PSL 03	1	1	1	1	1	1				
	PSH 02	5	3	2	2	2	1	1	1	1	1
alarm logic		1oo2	1oo2	1oo2	1oo2	1oo2	1oo2	1oo1	1oo1	1oo1	1oo1
no. shutdown unit	switch	5	6	5	5	3	3	3	3	2	2
	damper	4	4	4	3	3	2	3	2	2	1
first inspection, τ_1 (month)	switch	8.74	10.85	8.74	8.74	4.54	4.48	4.48	4.48	2.77	4.48
	damper	7.93	7.61	7.93	5.16	5.41	2.65	5.16	2.70	2.65	2.25
no. inspections	switch	17	12	17	17	47	48	48	48	100	48
	damper	16	17	16	30	28	79	30	76	78	98

■ ASSOCIATED CONTENT

Supporting Information

Average unavailabilities of flow channel used in case 1. This material is available free of charge via the Internet at http://pubs.acs.org.

■ AUTHOR INFORMATION

Corresponding Author

*E-mail: ctchang@mail.ncku.edu.tw.

Notes

The authors declare no competing financial interest.

■ NOMENCLATURE

A_i = conditional probabilities of FS failure on i^{th} alarm channel
$\overline{Av}^{Corr}$ = average availability of an alarm channel
$\underline{Av}^{Prev}$ = availability of a shutdown unit
$\overline{Av}^{Prev}$ = average availability of a shutdown unit
B_i = conditional probabilities of FD failure on i^{th} alarm channel
C_a = financial losses incurred from FS failures
C_b = financial losses incurred from FD failures
C_{budget} = maximum allowable budget for purchasing protective units
C_{AL}^{LC} = life cycle cost for an alarm system
C_{SD}^{LC} = life cycle cost for a shutdown system
C_{AL}^{PC} = total purchased cost of an alarm system
C_{SD}^{PC} = total purchased cost of a shutdown system
ENRpr = expected number of repairs
ENRpl = expected number of replacements
$F(t)$ = failure probability (unavailability)
$f(\boldsymbol{y})$ = binary variable indicating whether alarm system issues an alarm
H = system lifetime
$h(\boldsymbol{z})$ = binary variable indicating whether the shutdown system carries the shutdown operation successfully
$InspC_j$ = inspection cost for j^{th} shutdown unit
k = number of online sensors detecting an unsafe state
L_{AL} = total expected loss of an standalone alarm system
LCC_i^{AL} = life cycle cost for i^{th} alarm channel
LCC_j^{SD} = life cycle cost for j^{th} shutdown unit
L_{PT}^{LC} = total expected loss by applying protective system
m = total purchased sensor units
n = total online sensor units
p = probability of an unsafe state
P_k = probability of event at node k in Markov diagram
PCS_i = purchase cost for one sensor in i^{th} alarm channel
PCS_j = purchase cost for one j^{th} shutdown unit
P_{FS}^{AL} = conditional probabilities of FS failure on alarm system
P_{FD}^{AL} = conditional probabilities of FD failure on alarm system
P_{FS}^{SD} = conditional probabilities of FS failure on shutdown system
P_{FD}^{SD} = conditional probabilities of FD failure on shutdown system
$R(t)$ = reliability (availability)
$\underline{RprC}_i$ = repair cost for j^{th} shutdown unit
$\overline{RprsC}_i$ = average repair cost for i^{th} alarm channel
$\overline{RplsC}_i$ = average replacement cost for i^{th} alarm channel
s_j = binary variable indicating whether j^{th} shutdown unit is selected for implementation
$w_{i,m,n,k}$ = binary variable indicating whether i^{th} alarm channel with m purchased sensors, n online sensors, and a k-out-of-n voting gate is selected for implementation
x_s = binary variable representing the condition of the s^{th} process variable
y_i = binary variable indicating whether i^{th} sensor detect an unsafe state
$z(t)$ = failure rate
z_j = binary variable indicating whether j^{th} shutdown unit takes a shutdown action
α = Weibull shape parameter
α_j = conditional probabilities of FS failure of j^{th} shutdown unit
β_j = conditional probabilities of FD failure of j^{th} shutdown unit
λ = Weibull scale parameter
Ω_i = maximum allowable purchased sensors for i^{th} channel
τ_p = time at where p^{th} inspection is conducted
ξ = binary variable representing the condition of the manufacturing process

■ REFERENCES

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

(2) Chang, C. T.; Tsai, C. S.; Chen, K. H. Resilient Alarm Logic Design for Process Networks. *Ind. Eng. Chem. Res.* **2000**, *39*, 4974.
(3) Andrews, J. D.; Bartlett, L. M. A Branching Search Approach to Safety System Design Optimization. *Reliab. Eng. Syst. Saf.* **2005**, *87*, 23.
(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) Okasha, N. M.; Frangopol, D. M. Lifetime-oriented Multi-objective Optimization of Structural Maintenance Considering System Reliability, Redundancy, and Life-cycle Cost Using GA. *Structural Safety* **2009**, *31*, 460.
(11) Wang, Y.; Pham, H. A Multi-objective Optimization of Imperfect Preventive Maintenance Policy for Dependent Competing Risk Systems with Hidden Failure. *IEEE Trans. Reliab.* **2011**, *60*, 770.
(12) Kouedeu, A. F.; Kenne J. P.; Songmene V. Production, Preventive, and Corrective Maintenance Planning in Manufacturing Systems under Imperfect Repairs. In *3rd International Workshop on Dependable Control of Discrete Systems (DCDS)*, 15−17 July, Saarbrucken, DE, 2011; Vol. *59*.
(13) Wang, Y.; Pham, H. Maintenance Modeling and Policies. In *Stochastic Reliability and Maintenance Modeling*; Dohi, T., Nakagawa, T., Eds.; Springer Series in Reliability Engineering: London, 2013; Vol. *9*, pp 141−158.
(14) 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.
(15) Liao, Y. C.; Chang, C. T. Design and Maintenance of Multichannel Protective Systems. *Ind. Eng. Chem. Res.* **2010**, *49*, 11241.
(16) Barlow, R.; Hunter, L. Optimum Preventive Maintenance Policies. *Operations Res.* **1960**, *8*, 90.
(17) Park, K. S. Optimal Number of Minimal Repairs before Replacement. *IEEE Trans. Reliab.* **1979**, *R-28*, 137.
(18) Brown, M.; Proschan, F. Imperfect Repair. *J. Appl. Probab.* **1983**, *20*, 851.
(19) Brown, M., Proschan, F. Imperfect Maintenance. *IMS Lecture Notes—Monograph Series 2: Survival Analysis*; Institute of Mathematical Statistics: Hayward, CA, 1982; pp 179−188.
(20) Aven, T. Optimal Replacement under a Minimal Repair Strategy: A General Failure Model. *Adv. Appl. Probab.* **1983**, *15*, 198.
(21) Aven, T.; Jensen, U. A General Minimal Repair Model. *J. Appl. Probab.* **2000**, *37*, 187.
(22) Li, H.; Shaked, M. Imperfect Repair Models with Preventive Maintenance. *J. Appl. Probab.* **2003**, *40*, 1043.
(23) Doyen, L.; Gaudoin, O. Classes of Imperfect Repair Models Based on Reduction of Failure Intensity or Virtual Age. *Reliab. Eng. Syst. Saf.* **2004**, *84*, 45.
(24) Marlow, N. A., and Tortorella, M. Strong and Weak Minimal Repair, The Revival Process, and Maintained System Reliability Models; Industrial & Systems Engineering Technical Report; Rutgers University: Piscataway, NJ, 2009.
(25) Yevkin, O.; Krivtsov, V. Comparative Analysis of Optimal Maintenance Policies under General Repair with Underlying Weibull Distributions. *IEEE Trans. Reliability* **2013**, *62*, 82−91.
(26) Weibull, W. A Statistical Distribution Function of Wide Applicability. *J. Appl. Mech.-Trans.* **1951**, *18*, 293−297.
(27) Henley, E. J.; Kumamoto, H. *Designing for Reliability and Safety Control*; Prentice-Hall: Englewood Cliffs, NJ, 1985.
(28) Liptak, B. G. *Optimization of Unit Operations*; Chilton Book Co.: New York, *227*, 1987.