Reliability Engineering and System Safety 199 (2020) 106915

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

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

Optimal designs of multi-event interlocks

Sing-Zhi Chan, Chuei-Tin Chang*

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

ARTICLE INFO

Keywords:
Interlock
Multi-event
Reliability
Expected loss

ABSTRACT

In order to mitigate the detrimental outcomes of process anomalies, modern chemical plants are generally equipped with various safety interlocks. However, almost every conventional design was created by conjecturing the proper protective mechanism against a single abnormal event. In reality, multiple independent abnormal events may take place in many processes. Thus, there is a definite need to develop a systematic approach for designing the multi-event interlocks. In this paper, a realistic system (the sump of a distillation column and the corresponding fired reboiler) is adopted as an illustrative example to show three possible multi-event scenarios. The ultimate objective of this study is to construct a superstructure-based mixed integer non-linear programming (MINLP) model to generate the optimal design of any given process by minimizing the total expected lifecycle cost. Extensive case studies are also presented to demonstrate the feasibility and effectiveness of the proposed design strategy. The resulting optimum specifications include: (1) the number of online sensors in each measurement channel and the corresponding voting gate, (2) the alarm logic, and (3) the number of actuators for each shutdown operation. Finally, from the optimization results, one can clearly see that the proposed multi-event interlock is always superior to a traditional one.

1. Introduction

In order to mitigate the detrimental outcomes of process anomalies, it is a common practice to install safety interlocks on the processes operated under hazardous conditions. Traditionally, the related design and maintenance issues were addressed with an ad hoc approach according to prior experiences. Since this approach tends to be tedious and error prone, there is a need to carried out the above tasks via the use of mathematical programming model.

There have been a wide variety of effective methods for risk assessment of a given system, e.g., fault tree analysis (FTA), event tree analysis (ETA) and hazard and operability study (HAZOP), etc. With these assessment methods, the potential hazardous events in a given system can be effectively identified and the safety interlocks may be installed accordingly to ameliorate their harmful effects. Generally speaking, every safety interlock consists of two parts, i.e., the alarm subsystem and the shutdown subsystem. The former is equipped with sensors to measure the process states and decide whether an alarm should be set off, while the latter is usually facilitated with one or more shutdown actuator (such as the solenoid valves) to execute the predetermined protective action. However, every hardware item in the safety interlock may fail either safely (FS) or dangerously (FD). Therefore, the design principle of hardware redundancy is often be introduced at the component level to improve system availability [1]. More specifically, multiple sensors and the corresponding voting gate logic [2] may be installed in the alarm subsystem to monitor the same process variables and to determine whether an unsafe condition is reached. On the other hand, multiple shutdown actuators may also be installed in the shutdown subsystem with appropriate logic to execute the proper protective actions. Following is a brief literature review on the conventional interlock design:

Lambert et al. [3] presented a computation method to determine the optimum redundant configuration in multistage systems for achieving a target availability at the minimum cost. Sasaki et al. [4] proposed an efficient algorithm to optimize a repairable system with spare units. Tsai and Chang [5] have developed a statistic-based alarm strategy using the reconciled online process data to reduce the chance of misjudgment in setting off alarms. Lai and Chang [6] introduced a spare-supported corrective maintenance policy into the design of alarm subsystem. Andrews and Bartlett [7] used a branching search algorithm to produce the optimum designs of protective systems. Liang and Chang [8] have developed the mathematical programming model of multilayer protective system and solve the optimization problem with General Algebraic Modelling Systems (GAMS). Liao and Chang [9] then improved the aforementioned corrective maintenance policy by introducing multi-channel alarm subsystem to further increase the

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

https://doi.org/10.1016/j.ress.2020.106915
Received 30 April 2019; Received in revised form 16 December 2019; Accepted 11 March 2020
Available online 14 March 2020
0951-8320/

availability of safety interlock. Since the FD failures of shutdown elements are not detectable during normal operations, the preventive maintenance policy was implemented for the shutdown subsystem. Vaurio [10] suggested that the inspection lengths of shutdown elements could be determined to minimize the cost rate or accident rate of a system. Under this policy, every component is replaced after a fixed number of inspections and/or repairs, even it is still functional.

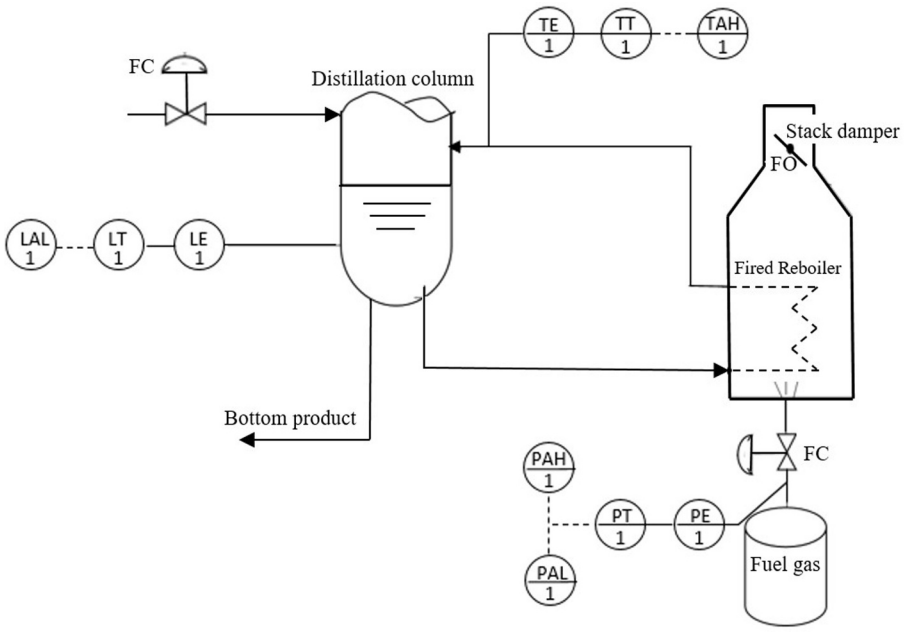
It should be noted that the aforementioned conventional methods to design a safety interlock were usually aimed for prevention of the undesired outcome(s) caused by a single abnormal event. However, any realistic process may be affected by several interrelated undesired events and these events may cause multiple detrimental consequences. For example, Miskin [11] fully investigated the control performance for the high pressure leaching process by process simulation, and multiple dedicated interlocks were considered installed in the model for different independent fault scenarios. The Wendelstein 7-X stellarator incorporates dedicated interlocks for two independent abnormal events, i.e. overheating of the beam dump and stray radiation of electron cyclotron resonance heating [12]. Guo et al. [13] designed the multi-event interlock for the low-energy accelerator facility, by using two sets of protection logic. Obviously, the prevention of undesired outcomes caused by multiple abnormal events is a critical issue in practical applications. However, note that the optimal multi-event interlocks in [11,12] and [13] have not been developed at all. Thus, there is a need to improve the conventional approaches by constructing a mathematical programming model to generate the optimal interlock designs for the more practical multi-input multi-output systems. In the paper, a new mathematical model of the multi-event interlock has been proposed. Specifically, a comprehensive mixed-integer nonlinear program has been built for minimizing the total expected lifecycle cost of any multi-event interlock and for determining the corresponding design specifications, i.e., (1) the number of online sensors in each measurement channel and the corresponding voting-gate configuration, (2) the alarm logic, and (3) the number of actuators for each shutdown operation.

2. An illustrative example

An illustrative example is presented here to facilitate clear understanding of the research issues at hand. Fig. 1 shows a fired reboiler and sump of a distillation column. Distillation column is an essential equipment in chemical plants for separating mixture into its components based on difference in volatilities. To provide the necessary energy for the distillation process, fuel gas is burnt in the fired reboiler to heat and vaporize the tower bottoms as this liquid circulates through the heater tubes. The vaporized product is then returned to sump of distillation column and contact with the downflowing liquid for mass and heat transfers between the two phases. Note that the fired reboiler is also equipped with a stack damper to regulate the pressure in combustion chamber. Since several abnormal events may take place during the operation horizon, safety interlock is needed to suppress the dangerous outcomes. Different online sensors are available in this system to monitor the liquid level in sump (LE), the feed pressure of fuel gas (PE) and the vaporized product temperature after returning from reboiler (TE). On the other hand, the feed valve, fuel gas feed valve and stack damper are the actuators to protect against the consequences of abnormal events.

Potential upsets of the above system may be identified by applying a standard hazard assessment method, e.g., FTA and HAZOP. For illustration purpose, let us consider the following three possible multi-event scenarios.

- **Case 0:** Let us assume that two independent abnormal events can be identified, i.e., (1) fuel gas shortage, and (2) low flowrate of the column feed. The former is expected to be revealed in the fuel pressure measurement, i.e., PAL-1, while the latter in temperature and level measurements, i.e., TAH-1 and LAL-1. Let us further assume that the column feed can be terminated to protect against the abnormal event (1), while fuel gas feed be terminated to protect against the adverse effect of abnormal event (2).
- **Case 1:** The identified events and the corresponding symptoms detected by the online sensors are assumed to be the same as those considered in Case 0. However, both event (1) and event (2) call for stoppage of column feed flow in the present case, while event (2) alone also requires an extra operation to stop the fuel gas supply.
- **Case 2**: Let us assume that the findings of hazard analysis are slightly different than those listed above. The two abnormal events in this case are found to be (1) high fuel gas pressure and (2) low column feed rate. The online symptoms of event (1) are reflected in sensor signals PAH-1, TAH-1 and LAL-1, while those of event (2) in



Instrument ID

LAL	Level Alarm Low
LE	Level Element
LT	Level Transmitter
PAH	Pressure Alarm High
PAL	Pressure Alarm Low
PE	Pressure Element
PT	Pressure Transmitter
TAH	Temperature Alarm High
TE	Temperature Element
TT	Temperature Transmitter

Fig. 1. Fired reboiler and sump of a distillation column [14].

TAH-1 and LAL-1. Three protective actions are assumed to be effective, i.e., (a) stoppage of column feed flow, (b) termination of fuel gas supply and (c) maximization of stack flow by adjusting the damper position. All three actions should be executed to negate the hazardous impacts of event (1), but only the first two are required to counteract event (2).

From the above discussions, it is clear that the two abnormal events in Case 0 share neither the same observable online symptoms nor common protective actions. Thus, the traditional design practice, i.e., a dedicated interlock is configured independently for each abnormal event, is applicable in this scenario. On the other hand, it is also clear that Case 1 and Case 2 should be treated differently. Notice first that the harmful effects of both events in Case 1 have to be ameliorated with a common protective action, i.e., stoppage of column feed flow. Notice also that two identical corrective measures, i.e., stoppage of column feed flow and termination of fuel gas supply, are needed in Case 2 to eliminate the hazardous effects caused by the two events under consideration. On the other hand, one should note that two out of three online measurements, i.e. temperature and level measurement, deviate from their normal levels toward the same directions in the detecting the independent events of Case 2. In Case 1, the detection of each independent event depends on its unique measurement(s), i.e. pressure measurement for event (1) and temperature and level measurements for event (2). In other words, the online symptoms of both events are partially indistinguishable in Case 2 while those in Case 1 are differentiable.

The generalized system structure, i.e., the superstructure, of the interlocks in latter two cases is detailed in the following section to facilitate formulation of a mathematical programming model for generation of the optimal multi-event interlock designs.

3. . Superstructure

To facilitate unambiguous illustration of the system structure for any multi-event interlock, let us consider the sketch in Fig. 2.

In this structure, ξ_p ($p = 1, 2, \cdots, P$) is a binary variable which denotes whether or not the pth abnormal event is present, i.e.

$$\xi_p = \begin{cases} 1, & \textit{the } p\text{th } \textit{abnormal event is present} \\ 0, & \textit{otherwise} \end{cases} \tag{1}$$

For the sake of formulation conciseness, let us introduce a binary row vector to include all such variables, i.e. $\boldsymbol{\xi} = \langle \xi_1, \xi_2, ..., \xi_P \rangle$.

Another binary variable u_i ($i = 1, 2, \cdots, I$) is adopted here to denote whether or not the ith process variable violates the corresponding safety limit, i.e.

$$u_i = \begin{cases} 1, & \textit{the } i\text{th } \textit{process variable exceeds its safety limit} \\ 0, & \textit{otherwise} \end{cases} \tag{2}$$

A binary vector is also introduced for brevity, i.e., $\boldsymbol{u} = \langle u_1, u_2, ..., u_I \rangle$. Note that, for any given system, there always exists an inherent multi-input multi-output (MIMO) mapping from $\boldsymbol{\xi}$ to $\boldsymbol{u}$. In other words, the functions $u_i(\boldsymbol{\xi})$s ($i = 1, 2, \cdots I$) are given a priori.

It is also assumed that all process variables in the superstructure are monitored with online sensors and, since measurement errors are unavoidable, hardware redundancy is introduced to enhance reliability. A sketch of the corresponding measurement channel is shown in Fig. 3. Specifically, a total of N_i identical sensors may be installed in this channel to measure the i^{th} variable, and each sensor measurement can be characterized with a binary variable v_{i,m_i}.

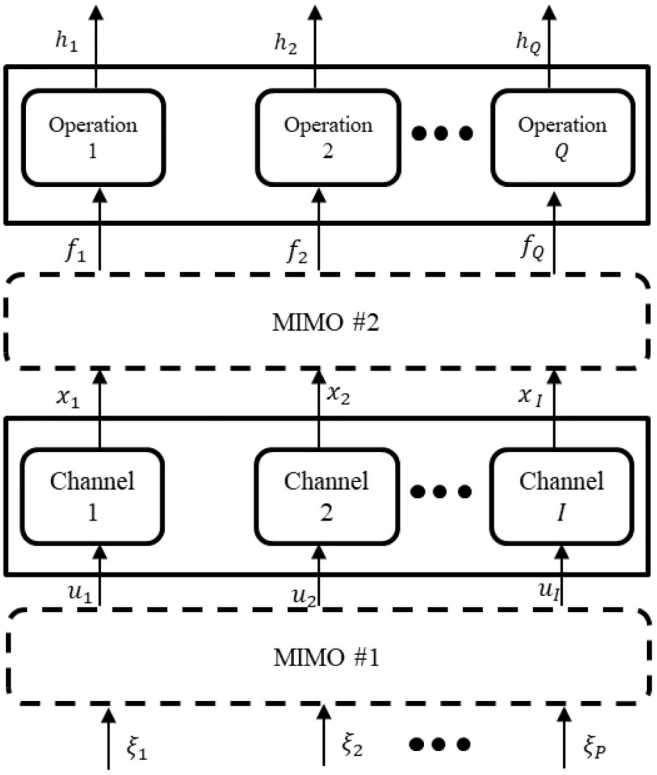


Fig. 2. Superstructure of proposed multi-event interlock.

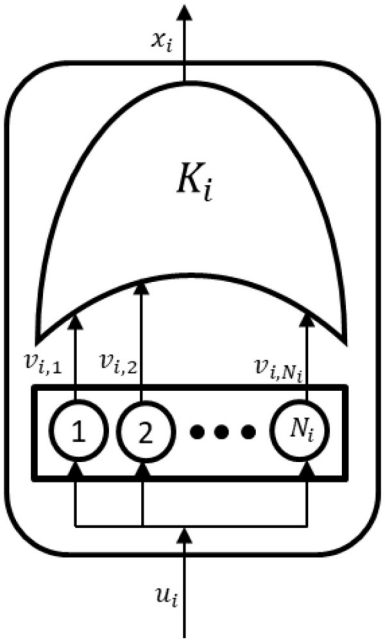


Fig. 3. Superstructure of a measurement channel.

$$v_{i,m_i} = \begin{cases} 1, & \textit{measurement of the } m_i^{th} \textit{ sensor for variable i violates safety limit} \\ 0, & \textit{otherwise} \end{cases} \tag{3}$$

where, $m_i = 1, 2, ..., N_i$. Notice also that each channel is assumed to be equipped with a designer-specified K_i-*out-of-*N_i voting gate to verify whether or not the corresponding process variable exceeds the safety limit. A binary vector $\boldsymbol{x} = \langle x_1, x_2, ..., x_I \rangle$ is used in this study to

represent all channel outputs, i.e.

$$x_i = \begin{cases} 1, & \textit{the } i\text{th } \textit{channel indicates an unsafe state} \\ 0, & \textit{otherwise} \end{cases} \tag{4}$$

where $i = 1, 2, \cdots, I$. In addition, let us introduce additional two integer vectors to store the numbers of identical sensors and the corresponding voting-gate logics, i.e. $\boldsymbol{N} = \langle N_1, N_2, ..., N_I \rangle$, $\boldsymbol{K} = \langle K_1, K_2, ..., K_I \rangle$ and $\boldsymbol{N} \geq \boldsymbol{K}$.

The above channel outputs (x_i) are then fed into a second MIMO function in superstructure to determine the proper protective actions. In the present study, this MIMO function is referred to as the *alarm logic* and its outputs can be regarded as the decisions to activate certain predetermined protective actions.

Let us introduce the binary variable f_q to decide if implementation of the qth shutdown operation is needed.

$$f_q = \begin{cases} 1, & \textit{confirmation of the decision to implement } q\text{th } \textit{shutdown operation} \\ 0, & \textit{otherwise} \end{cases} \tag{5}$$

where, $q = 1, 2, \cdots, Q$. Let us next define a column vector $\boldsymbol{F}_q$ with 2^I elements and each element is the value of f_q that corresponds to a unique combination of the binary variables in $\boldsymbol{x}$. Furthermore, let us define a 2^I-by-Q binary matrix to include all such values, i.e. $\mathbb{F} = [\boldsymbol{F}_1, \boldsymbol{F}_2, ..., \boldsymbol{F}_Q]$.

The design principle of hardware redundancy is again introduced into superstructure for enhancing reliability of the shutdown operation. To be specific, a sketch of the corresponding shutdown configuration is shown in Fig. 4, in which a total of S_q identical elements are incorporated for implementing the q^{th} shutdown operation. Let us use the binary variable z_{q,j_q} to express whether or not the desired shutdown operation is executed by the j_q^{th} element, i.e.

$$z_{q,j_q} = \begin{cases} 1, & \textit{the } q\text{th } \textit{shutdown operation is executed by the } j_q^{th} \textit{ element} \\ 0, & \textit{otherwise} \end{cases} \tag{6}$$

where $j_q = 1, 2, ..., S_q$. Another integer vector is also utilized in this paper to store the numbers of shutdown elements for all operations, i.e., $\boldsymbol{S} = \langle S_1, S_2, ..., S_Q \rangle$. Every output of superstructure is denoted by the binary variable h_q, which is adopted to represent whether the qth shutdown operation is successfully carried out, i.e.

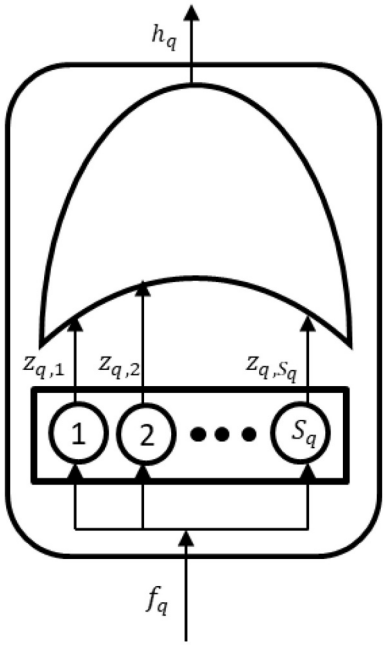


Fig. 4. Superstructure of a shutdown operation.

$$h_q = \begin{cases} 1, & \textit{the } q\text{th } \textit{shutdown operation is completed successfully} \\ 0, & \textit{otherwise} \end{cases} \tag{7}$$

A binary vector $\boldsymbol{h} = \langle h_1, h_2, ..., h_Q \rangle$ is adopted to represent all outputs of shutdown operations. To simplify model formulation, it is assumed in this work that the "OR" logic is utilized to connect h_q and z_{q,j_q} ($j_q = 1, 2, ..., S_q$), i.e.

$$h_q = 1 - \prod_{j_q=1}^{S_q} \left(1 - z_{q,j_q}\right) \tag{8}$$

It should be noted that Fig. 2 can also be used for characterizing the traditional design approach by repeatedly setting $P = 1$ for every abnormal event. This is because of the fact that a dedicated interlock is supposed to be configured independently for each event.

4. Mathematical programming model

The illustrative example in Section 2 is adopted here to illustrate the construction procedure of mathematical programming model for a safety interlock system triggered by two or more independent events. For the sake of simplicity, only the mathematical programming model constructed according to the superstructures in Figs. 2–4 is shown below. Let us first assume that each event takes place independently at a constant probability, i.e.

$$PrE_p = Pr\{\xi_p = 1\} \tag{9}$$

where, PrE_p denotes the average occurrence probability of the pth event during a definite period of time (say 1 year) and $p = 1, 2, \cdots, P$. On the other hand, the first MIMO mapping in Case 0 and Case 1 should both be expressed as: $u_1 = \xi_1$, $u_2 = \xi_2$ and $u_3 = \xi_2$, and MIMO #1 in Case 2 can be stipulated according to Table 1.

The conditional probabilities of FS and FD failures of the ith measurement channel in Fig. 2 (denoted respectively by $A_{AL,i}$ and $B_{AL,i}$) can be expressed as follows:

$$A_{AL,i} = Pr\{x_i = 1 | u_i = 0\} \tag{10}$$

$$B_{AL,i} = Pr\{x_i = 0 | u_i = 1\} \tag{11}$$

If K_i-*out-of*-N_i voting gate (see Fig. 3) is used to trigger the ith channel, $A_{AL,i}$ and $B_{AL,i}$ can be further expressed as functions of the FS and FD probabilities of a single sensor in the ith alarm channel respectively.

$$A_{AL,i}(N_i, K_i) = \sum_{j=K_i}^{N_i} \frac{N_i!}{j!(N_i - j)!} \times (a_i)^j \times (1 - a_i)^{N_i - j} \tag{12}$$

$$B_{AL,i}(N_i, K_i) = 1 - \sum_{j=K_i}^{N_i} \frac{N_i!}{j!(N_i - j)!} \times b_i^{N_i - j} \times (1 - b_i)^j \tag{13}$$

where, a_i and b_i denotes the aforementioned single-sensor FS and FD probabilities for channel i and they are regarded as constant parameters extracted from maintenance data. For model simplicity, it is assumed that the FS error of each sensor is temporary (i.e., it is due to spurious measurement signals only and the subsequent repair is unnecessary) while the FD error of each sensor is permanent.

As mentioned before, the second MIMO function (MIMO #2) in

Table 1
The MIMO #1 mapping from $\boldsymbol{\xi}$ to $\boldsymbol{u}$ in Case 2.

$\boldsymbol{\xi}$	u_1	u_2	u_3
<1,1>	1	1	1
<1,0>	1	1	1
<0,1>	0	1	1
<0,0>	0	0	0

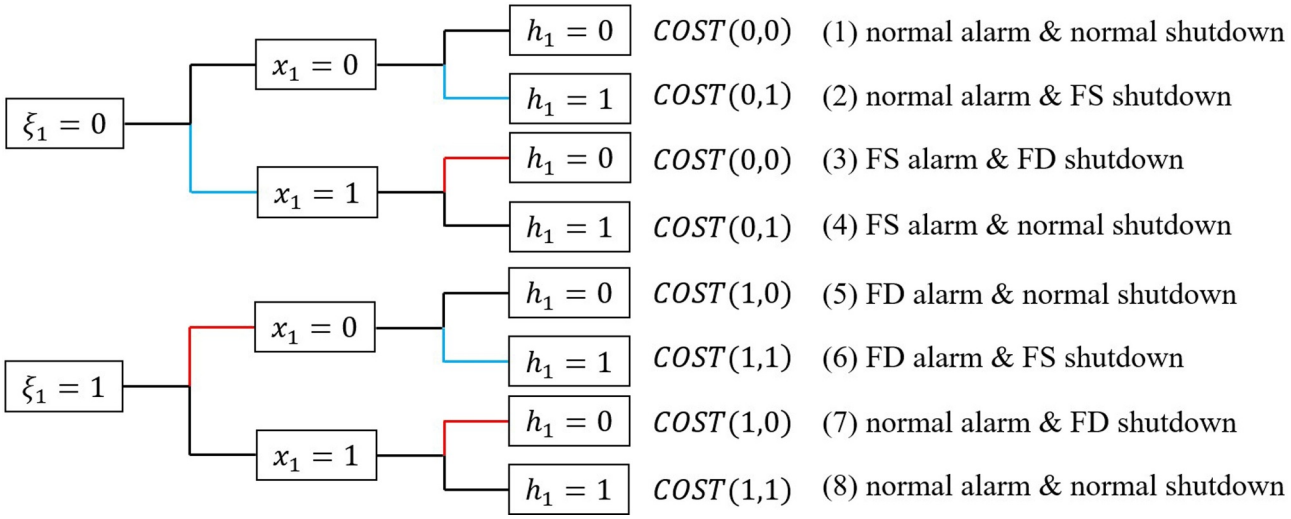


Fig. 5. All possible scenarios of protective system.

superstructure (Fig. 2) are usually referred to as the *alarm logic*, which is essentially the mapping from channel outputs to the signals that trigger the shutdown actions. However, this MIMO mapping cannot be obtained a priori and the corresponding alarm logic must be selected so as to minimize the total expected lifecycle cost.

In the shutdown subsystem, the conditional probabilities of FS and FD failures of the qth shutdown operation (denoted respectively by $A_{SD,\,q}$ and $B_{SD,\,q}$) can be expressed as follows:

$$A_{SD,q} = Pr\{h_q = 1 | f_q = 0\} \tag{14}$$

$$B_{SD,\,q} = Pr\{h_q = 0 | f_q = 1\} \tag{15}$$

Let us assume that the qth shutdown operation is facilitated with S_q identical actuators and this operation is successful when one or more actuator behaves normally. In other words,

$$A_{SD,\,q}(S_q) = 1 - (1 - \alpha_q)^{S_q} \tag{16}$$

$$B_{SD,\,q}(S_q) = (\beta_q)^{S_q} \tag{17}$$

where α_q and β_q represent the FS and FD probability of a single actuator for the qth shutdown operation, respectively, and they are also regarded as given parameters.

To evaluate the expected loss of a multi-event interlock, it is also necessary to identify the financial loss caused by every possible scenario and this loss is denoted as $COST(\boldsymbol{\xi}, \boldsymbol{h})$ in the present study. In this study, $COST(\boldsymbol{\xi}, \boldsymbol{h})$ is assumed to be constant throughout the entire operation horizon. To be specific, let us consider these losses in Case 1 and Case 2 as examples and these examples are detailed in Appendix. For every given combination of voting gates ($\boldsymbol{N}$, $\boldsymbol{K}$), alarm logic ($\mathbb{F}$) and shutdown configuration ($\boldsymbol{S}$), the yearly expected loss of the safety interlock can be expressed as

$$ExpLoss(\boldsymbol{N}, \boldsymbol{K}, \mathbb{F}, \boldsymbol{S}) = \sum_{\boldsymbol{\xi},\boldsymbol{x},\boldsymbol{h}} \left[COST(\boldsymbol{\xi}, \boldsymbol{h}) \prod_{p=1}^{P} PrEvent_p \prod_{i=1}^{I} PrAl_i \prod_{q=1}^{Q} PrSd_q \right] \tag{18}$$

where

$$PrEvent_p = PrE_p^{\xi_p}(1 - PrE_p)^{\left(1-\xi_p\right)} \tag{19}$$

$$PrAl_i = A_{AL,i}^{(x_i)(1-u_i(\xi))}(1 - A_{AL,\,i})^{(1-x_i)(1-u_i(\xi))} B_{AL,\,i}^{(1-x_i)(u_i(\xi))}(1 - B_{AL,\,i})^{(x_i)(u_i(\xi))} \tag{20}$$

$$PrSd_q = A_{SD,\,q}^{\left(1-f_q(\boldsymbol{x})\right)(h_q)}(1 - A_{SD,\,q})^{\left(1-f_q(\boldsymbol{x})\right)(1-h_q)} B_{SD,\,q}^{\left(f_q(\boldsymbol{x})\right)(1-h_q)} (1 - B_{SD,\,q})^{\left(f_q(\boldsymbol{x})\right)(h_q)} \tag{21}$$

Notice that $A_{AL,\,i}$, $B_{AL,\,i}$, $A_{SD,\,q}$ and $B_{SD,\,q}$ can be determined according to Eqs. (12), (13), (16) and (17) respectively. A simple example (1 abnormal event, 1 measurement channel, 1 shutdown operation) is provided here to further illustrate Eq. (18).

Example:

Suppose we want to install the safety interlock for single abnormal event, and there is only 1 measurement channel and 1 shutdown operation. MIMO #1 can be expressed as $u_1 = \xi_1$, while MIMO #2 is assumed to be $f_1(x_1 = 0) = 0$ and $f_1(x_1 = 1) = 1$. The yearly expected loss of the safety interlock can be expressed as follow by using Eq. (18):

$$\begin{aligned}
&ExpLoss(N_1, K_1, \langle 1, 0\rangle^T, S_1) \\
&= \sum_{\xi,x,h} [COST(\xi, h) \prod_{p=1}^{1} PrEvent_p \prod_{i=1}^{1} PrAl_i \prod_{q=1}^{1} PrSd_q] \\
&= (1 - PrE_1)(1 - A_{AL,1})(1 - A_{SD,1})\ COST(0, 0) \\
&+ (1 - PrE_1)(1 - A_{AL,1})(A_{SD,1})\ COST(0, 1) \\
&+ (1 - PrE_1)(A_{AL,1})(B_{SD,1})\ COST(0, 0) \\
&+ (1 - PrE_1)(A_{AL,1})(1 - B_{SD,1})\ COST(0, 1) \\
&+ (PrE_1)(B_{AL,1})(1 - A_{SD,1})\ COST(1, 0) \\
&+ (PrE_1)(B_{AL,1})(A_{SD,1})\ COST(1, 1) \\
&+ (PrE_1)(1 - B_{AL,1})(B_{SD,1})\ COST(1, 0) \\
&+ (PrE_1)(1 - B_{AL,1})(1 - B_{SD,1})\ COST(1, 1)
\end{aligned}$$

Note that the aforementioned calculation of expected loss can be illustrated with Fig. 5, in which all possible scenarios are enumerated. Clearly Eq. (18) is also applicable to complicated systems with more abnormal events, alarm channels and shutdown operations.

Therefore, the objective function of the optimization problem at hand can be regarded as the total expected lifecycle cost, i.e., the sum of the total expected lifecycle loss and the total purchase cost. Specifically,

$$obj(\boldsymbol{N}, \boldsymbol{K}, \mathbb{F}, \boldsymbol{S}) = ExpLoss(\boldsymbol{N}, \boldsymbol{K}, \mathbb{F}, \boldsymbol{S}) \times \gamma + CostAL(\boldsymbol{N}) + CostSD(\boldsymbol{S}) \tag{22}$$

where, $CostAL(\boldsymbol{N})$ and $CostSD(\boldsymbol{S})$ denote the total purchase costs of the alarm and shutdown subsystems, respectively. In particular, they can be estimated as follows

$$CostAL(\boldsymbol{N}) = \sum_{i=1}^{I} PCSensor_i \times N_i \tag{23}$$

$$CostSD(\boldsymbol{S}) = \sum_{q=1}^{Q} PCSdElement_q \times S_q \tag{24}$$

where, $PCSensor_i$ is the purchase cost of a sensor in the ith alarm channel, $PCSdElement_q$ is the purchase cost of a shutdown actuator in the qth shutdown operation. On the other hand, γ is a multiplier converting the expected loss during each year over the horizon of lifecycle to their present values, i.e.

$$\gamma = \sum_{k=1}^{H} \frac{1}{(1+r)^{k-1}} \tag{25}$$

where, r is the interest rate and H is the horizon of lifecycle in years.

Finally, if we need to consider budget, the following inequality can be incorporated into the mathematical program as an additional constraint,

$$CostAL(\boldsymbol{N}) + CostSD(\boldsymbol{S}) \le PC_{IB} \tag{26}$$

where PC_{IB} is the maximum allowable purchase cost for all elements in the safety interlock.

5. Case studies

The feasibility and effectiveness of the proposed design strategy are demonstrated with the case studies described in this section. The purchase costs of different types of sensors and their conditional FS and FD probabilities are shown in Table 2, while those of the shutdown actuators are shown in Table 3. Notice that the conditional probabilities of FS and FD failures of damper are assumed to be negligible when compared with other shutdown elements. Notice also that, for calculation simplicity, it is assumed in the following case studies that $H = 1$.

- Case 0: It is not necessary to consider this case here because both the traditional and the proposed approaches end up with the same design.
- Case 1: Let's assume that the process under consideration is scheduled to go through a thorough maintenance program every year and the average probabilities of abnormal events per year can be regarded as constants, i.e., $P_1 = 0.05$ (fuel gas shortage) and $P_2 = 0.10$ (low flowrate of the column feed). The maximum number of sensors allowed in each channel is set to be 3, while the maximum number of solenoid valves allowed for each shutdown operation is also 3. In this study, the financial losses due to various accidents are assumed to be constants over the entire operation horizon. In particular, these losses in four different scenarios, i.e., C_1, C_2, C_3 and C_4 defined in Appendix, are chosen to be 100,000, 50,000, 30,000 and 5000 USD respectively. All optimization runs were carried out with the SBB solver in the GAMS environment on an Intel Core i7 3.60 GHz PC. The optimum interlock configurations of proposed strategy are shown in Table 4. Note that the abbreviation "koon" is adopted to denote $k-$out $-$ of$-n$ voting gate, while the special case "0oo0" represents the corresponding channel does not exist. For the sake of illustration brevity, only the optimum alarm logic in the interlock design without budget limit is presented in Table 5. For comparison purpose, the traditional design approach, i.e., a dedicated interlock is configured individually for each abnormal event, has also been applied in the present case study. As mentioned before, the superstructure in Fig. 2 can be used to build the corresponding mathematical programming model by setting $P = 1$ for every abnormal event. The resulting optimum interlock configurations are shown in Table 6, while the alarm logic in the interlock design without budget limit is given in Table 7. Note that in the latter table a superscript is added to the q^{th} alarm function, i.e. f_q^p, to denote the corresponding event p.
- Case 2: Again the average probabilities of abnormal events per year are assumed to be constants, i.e., $P_1 = 0.03$ (high fuel gas pressure) and $P_2 = 0.10$ (low flowrate of the column feed). The maximum number of sensors allowed in each channel is set to be 2, while the maximum number of solenoid valves allowed for each shutdown

Table 2
Specifications of sensors.

Sensor Type	$PCSensor_i$ (USD)	a_i	b_i
Pressure ($i = 1$)	250	0.10	0.02
Temperature ($i = 2$)	100	0.15	0.05
Liquid Level ($i = 3$)	200	0.10	0.03

Table 3
Specifications of shutdown actuators.

Actuator Type	$PCSdElement_q$ (USD)	α_q	β_q
Solenoid Valve ($q = 1, 2$)	150	0.005	0.003
Damper ($q = 3$)	260	0	0

Table 4
Optimum interlock configurations obtained with the proposed strategy (Case 1).

Run #		1-A1	1-A2	1-A3	1-A4
Initial budget (USD)		None	1250.0	1000.0	750.0
Voting gate logic	Pressure	2oo2	2oo2	1oo1	1oo1
	Temperature	2oo3	2oo3	2oo3	0oo0
	Level	0oo0	0oo0	0oo0	1oo1
Number of actuators	Feed	1	1	1	1
	Fuel gas	1	1	1	1
Total expected lifecycle loss (USD)		962.4	962.4	1275.2	1513.3
Purchase cost (USD)		1100.0	1100.0	850.0	750.0
Objective value (USD)		2062.4	2062.4	2125.2	2263.3
Execution time (min)		1316	1300	773	237

Table 5
Optimum alarm logic obtained with the proposed strategy in run 1-A1.

$\boldsymbol{x} = \langle x_1, x_2, x_3 \rangle$	$f_1(\boldsymbol{x})$	$f_2(\boldsymbol{x})$
<1, 1, 1>	1	1
<1, 1, 0>	1	1
<1, 0, 1>	1	1
<1, 0, 0>	1	1
<0, 1, 1>	1	1
<0, 1, 0>	1	1
<0, 0, 1>	0	0
<0, 0, 0>	0	0

Table 6
Conventional optimum configurations (Case 1).

Run #		1-B1	1-B2	1-B3	1-B4
Initial budget (USD)		None	1250.0	1000.0	750.0
Voting gate logic	Pressure	2oo2	2oo2	1oo1	Infeasible
	Temperature	2oo3	2oo3	2oo3	(minimum
	Level	0oo0	0oo0	0oo0	requirement of
Number of actuators	Feed (event 1)	1	1	1	purchase cost is
	Feed (event 2)	1	1	1	800.0 USD)
	Fuel gas (event 2)	1	1	1	
Total expected lifecycle loss (USD)		2112.5	2112.5	2524.8	
Purchase cost (USD)		1250.0	1250.0	1000.0	
Objective value (USD)		3362.5	3362.5	3524.8	
Execution time (min)		597	589	234	3

Table 7
Conventional optimum alarm logic obtained in run 1-B1.

(a)	Optimum alarm logic of event 1.
$< x_1 >$	$f_1^1(x_1)$
1	1
0	0

(b)	Optimum alarm logic of event 2.	
$<x_2,\ x_3>$	$f_1^2(x_2,\ x_3)$	$f_2^2(x_2,\ x_3)$
<1, 1>	1	1
<1, 0>	1	1
<0, 1>	0	0
<0, 0>	0	0

Table 8
Optimum interlock configurations obtained with the proposed strategy (Case 2).

Run #		2-A1	2-A2	2-A3	2-A4
Initial budget (USD)		None	1500.0	1250.0	1000.0
Voting gate logic	Pressure	2oo2	2oo2	1oo1	1oo1
	Temperature	1oo2	1oo2	1oo2	1oo1
	Level	1oo1	1oo1	1oo1	0oo0
Number of actuators	Feed	1	1	1	1
	Fuel gas	1	1	1	1
	Damper	1	1	1	1
Total expected lifecycle loss (USD)		985.7	985.7	1250.5	1910.8
Purchase cost (USD)		1460.0	1460.0	1210.0	910.0
Objective value (USD)		2445.7	2445.7	2460.5	2820.8
Execution time (min)		147	114	109	15

Table 9
Optimum alarm logic obtained with the proposed strategy in run 2-A1.

$\boldsymbol{x} = \langle x_1, x_2, x_3 \rangle$	$f_1(\boldsymbol{x})$	$f_2(\boldsymbol{x})$	$f_3(\boldsymbol{x})$
<1, 1, 1>	1	1	1
<1, 1, 0>	1	1	1
<1, 0, 1>	1	1	1
<1, 0, 0>	0	0	1
<0, 1, 1>	1	1	0
<0, 1, 0>	0	0	0
<0, 0, 1>	0	0	0
<0, 0, 0>	0	0	0

operation is also 2. However, there is only 1 damper in the fired reboiler. Similarly, the financial losses due to various accidents are assumed to be constants over the entire operation horizon. In particular, these losses in six different scenarios, i.e., C_1, C_2, C_3, C_4, C_5 and C_6 defined in Appendix, are chosen to be 100,000, 50,000, 30,000, 5000, 40,000 and 3000 USD respectively. All optimization runs were also carried out with the SBB solver in GAMS environment on an Intel Core i7 3.60 GHz PC. The optimum interlock configurations obtained by the proposed strategy are shown in Table 8, while only the alarm logic in the interlock design without budget limit is presented in Table 9 for the sake of brevity. For comparison purpose, the traditional design approach has also been applied in the present case study. The resulting optimum interlock configurations are shown in Table 10, while the alarm logic in the interlock design without budget limit is given in Table 11.

Table 11
Conventional optimum alarm logic obtained in run 2-B1.

(a)	Optimum alarm logic of event 1.		
$<x_1,\ x_2,\ x_3>$	$f_1^1(x_1,\ x_2,\ x_3)$	$f_2^1(x_1,\ x_2,\ x_3)$	$f_3^1(x_1,\ x_2,\ x_3)$
<1, 1, 1>	1	1	1
<1, 1, 0>	1	1	1
<1, 0, 1>	1	1	1
<1, 0, 0>	0	0	1
<0, 1, 1>	1	1	0
<0, 1, 0>	0	0	0
<0, 0, 1>	0	0	0
<0, 0, 0>	0	0	0

(b)	Optimum alarm logic of event 2.	
$<x_2,\ x_3>$	$f_1^2(x_2,\ x_3)$	$f_2^2(x_2,\ x_3)$
<1, 1>	1	1
<1, 0>	0	0
<0, 1>	0	0
<0, 0>	0	0

Several prominent features can be observed from the aforementioned optimization results. Specifically,

i The objective value (i.e., the total expected lifecycle cost) of interlock design can in generally be reduced by relaxing the budget constraint, but this value eventually approaches a constant level after the budget exceeds an upper threshold. This is because, although an increase in total spending to raise hardware redundancy can usually bring down the FD probability, the same practice also tends to push the corresponding FS probability higher simultaneously.
ii The total expected lifecycle cost obtained with the proposed design strategy is always lower than its counterpart with the traditional approach. More specifically:
   (a) The purchase cost required by the proposed strategy is not significantly different from that by traditional design approach in both Case 1 and Case 2 when budget constraints are not imposed. However, if the budget constraint is tightened to a small value (see Run#1-A4 and Run#1-B4 for Case 1, and also see Run#2-A4 and Run#2-B4 for Case 2), only the proposed approach is feasible. This is due to the fact that the minimal

Table 10
Conventional optimum configurations (Case 2).

Run #		2-B1	2-B2	2-B3	2-B4
Initial budget (USD)		None	1500.0	1250.0	1000.0
Voting gate logic	Pressure	1oo1	1oo1	1oo1	Infeasible (minimum requirement of purchase cost is 1210.0 USD)
	Temperature	1oo1	1oo1	1oo1	
	Level	1oo1	1oo1	0oo0	
Number of actuators	Feed shutdown (event 1)	1	1	1	
	Fuel gas shutdown (event 1)	1	1	1	
	Damper shutdown (event 1)	1	1	1	
	Feed shutdown (event 2)	1	1	1	
	Fuel gas shutdown (event 2)	1	1	1	
Total expected lifecycle loss (USD)		1965.5	1965.5	2498.4	
Purchase cost (USD)		1410.0	1410.0	1210.0	
Objective value (USD)		3375.5	3375.5	3708.4	
Execution time (min)		924	743	382	15

Table 12
Comparison of expected lifecycle loss in Case 1 (Run#1-A1 and Run#1-B1).

$<\xi_1, \xi_2>$	Probability of occurrence	Expected loss (USD) Proposed strategy	Traditional strategy
<0, 0>	0.855	835.7	1982.5
<1, 0>	0.045	53.9	53.4
<0, 1>	0.095	70.9	71.6
<1, 1>	0.005	2.0	5.0
Total expected lifecycle loss (USD)		962.4	2112.5

Table 13
Comparison of expected lifecycle loss in Case 2 (Run#2-A1 and Run#2-B1).

$<\xi_1, \xi_2>$	Probability of occurrence	Expected loss of (USD) Proposed strategy	Traditional strategy
<0, 0>	0.873	718.3	1510.0
<1, 0>	0.027	60.3	29.0
<0, 1>	0.097	200.4	423.3
<1, 1>	0.003	6.7	3.2
Total expected lifecycle loss (USD)		985.7	1965.5

hardware requirement of the proposed design is less than that of the traditional one.

(b) It can also be observed that the total expected lifecycle loss of proposed strategy is much lower than that of traditional strategy in both Case 1 and Case 2. The expected losses in all possible scenarios are listed in detail in Tables 12 and 13. The expected FS loss without abnormal events, i.e., $\langle \xi_1, \xi_2 \rangle = \langle 0, 0 \rangle$, is clearly the major contributor of the total expected lifecycle loss. Since the traditional design induces a higher FS probability, the corresponding expected loss becomes greatly larger than its counterpart caused by the proposed approach. Finally, it should be noted that the expected losses in other scenarios are insignificant due to their low occurrence probabilities.

iii From Tables 4 and 8, which present the results obtained with the proposed strategy, it can be observed that all optimum numbers of actuators are at their lower bounds, while there is adequate hardware redundancy in the alarm channel provided that the initial budget is enough. This is due to the fact that both FS and FD probabilities of the actuators are much lower than those of the sensors and, thus, hardware redundancy is preferred to be introduced into the measurement channel rather than shutdown subsystem. From Tables 6 and 10, which present the results obtained with the conventional strategy, the optimum number of actuators corresponding to each event is also at its lower bound. However, more actuators must be used for the same shutdown operation if the conventional strategy is adopted. This is because both events in Case 1 and Case 2 share common protective actions. By using conventional strategy, we may lose the opportunity to install a high-quality measurement channel when there is a limitation in initial budget (for example, please compare Run#2-A3 in Table 8 and Run#2-B3 in Table 10).

6. Conclusions

Multi-event interlocks are essential for mitigating the detrimental consequences of more than one abnormal event in realistic processes. In this research, a MINLP model has been developed to systematically design the corresponding interlocks by minimizing the total expected lifecycle cost. A realistic illustrative example, i.e., the sump of a distillation column and its fired reboiler, is presented to demonstrate the presence of three possible cases in interlock designs. The feasibility and effectiveness of the proposed strategies are demonstrated with case studies. From the optimization results obtained so far, one can conclude that the proposed strategy is superior to the traditional design approach for cases 1 and 2. One can also determine the corresponding design specifications, i.e., (1) the number of online sensors in each measurement channel with its voting-gate logics, (2) the alarm logic, and (3) the number of actuators for each shutdown operation, in the proposed multi-event interlock.

CRediT authorship contribution statement

Sing-Zhi Chan: Software, Validation, Investigation, Writing - original draft, Visualization. **Chuei-Tin Chang:** Conceptualization, Methodology, Validation, Resources, Writing - review & editing, Supervision, Project administration.

Declaration of Competing Interest

None.

Appendix

In this part, we will illustrate the determination of $COST(\boldsymbol{\xi}, \boldsymbol{h})$ in Case 1 and Case 2 to evaluate the financial loss caused by every possible scenario.

- Case 1: As mentioned previously in Section 2, the interlock superstructure should have two binary inputs and two binary outputs in this case. A total of 16 scenarios can be distinguished with these 4 binary digits (i.e., ξ_1, ξ_2, h_1, h_2) and, for the sake of convenience, the scenarios are labelled with the corresponding decimal numbers. On the other hand, only four types of losses are considered in this system, i.e. C_1, C_2,C_3 and C_4. Table A-1 shows the scenarios that result in each type of losses.
  - C_1 and C_2 are the losses due to two different levels of decreases in liquid flow to the bottom of distillation column. For example, the initiating events in scenarios 4 (0100) and 6 (0110) in Table A-1 are the same, i.e., the feed rate to the column decreases ($\xi_2 = 1$) while the pressure of fuel gas is kept at the normal level ($\xi_1 = 0$). As a result, the liquid level in sump should be lowered in both cases. However, since the column feed is cut off ($h_1 = 1$) in scenario 6, the corresponding liquid level in sump may drop even lower to empty. Therefore, it is required to set

Table A1
The financial loss caused by each scenario in Case 1.

$COST(\boldsymbol{\xi}, \boldsymbol{h})$	Scenarios
0	0, 7, 10, 11, 15
C_1	2, 6, 14
C_2	4
C_3	1, 5, 8, 9, 12, 13
C_4	3

Table A2
The financial losses caused by each scenario in Case 2.

COST($\boldsymbol{\xi}$, $\boldsymbol{h}$)	Scenarios
0	0, 14, 23, 31
C_1	4, 5, 12, 13, 20, 21, 28, 29
C_2	8, 9, 16, 17, 24, 25
C_3	2, 3, 10, 11, 18, 19, 26, 27
C_4	6, 7, 15, 22, 30
C_5	16, 18, 20, 22, 24, 26, 28, 30
C_6	1, 3, 5, 7, 9, 11, 13, 15

$C_1 \gg C_2$ to signify that scenario 6 is much more hazardous than scenario 4.

- Let us next consider scenario 1 (0001) as an example. In this scenario, the fuel gas supply is cut off ($h_2 = 1$) when the system in under normal conditions. Consequently, the distillation products may become off spec for a period of time since the reboiler is without heating indefinitely. The corresponding loss is denoted by C_3 and $C_3 < C_2$ because the current scenario is less hazardous than scenario 4.
- C_4 is the loss resulting from complete system shutdown under the normal operating conditions, i.e., scenario 3 (0011). It is assumed that $C_3 \gg C_4$ since the amounts of off-spec products produced in this case are much less than those in scenarios resulted in C_3.
- Finally, if the interlock responds to a given $\boldsymbol{\xi}$ normally according to the original design, the corresponding loss (if exists) should be ignored. These scenarios are listed in the first row.
- Case 2: As described previously in Section 2, the interlock superstructure should have two binary inputs (ξ_1, ξ_2) and three binary outputs (h_1, h_2, h_3) in this case. A total of 32 scenarios can be distinguished with these 5 binary digits and they are also labelled with the corresponding decimal numbers. On the other hand, six types of losses can be identified in this case and Table A-2 shows the corresponding scenarios.
- C_1 to C_4 have already been defined in Table A-1.
- C_5 is the loss of high pressure in furnace, while C_6 is the loss of low pressure in furnace. Because the outcomes of former incident is much more severe than those of the latter, $C_5 \gg C_6$. Because the hazardous level of high pressure in furnace is lower than that of low liquid level at sump, so we have $C_5 < C_2$. Besides, the loss of high pressure in furnace should be higher than the loss of off spec products, so we set $C_5 > C_3$. Furthermore, the production of a chemical plant is too massive that the loss resulting from complete system shutdown under normal operating condition is higher than the loss of low pressure in furnace, so we have $C_4 > C_6$.
- Finally, row 1 shows the scenarios in which interlock behaves normally.

Note that some scenarios in Table A-2 are listed in two rows, e.g., scenarios 26, 28 and 30. This is due to the need to consider the losses associated with both column and furnace. In these cases, the total financial loss should be computed by summing up the corresponding *COST*($\boldsymbol{\xi}$, $\boldsymbol{h}$)s. From the aforementioned discussion of the relative magnitude of these six types of losses, we set that $C_1 > C_2 > C_5 > C_3 \gg C_4 > C_6 > 0$ in our system.

References

[1] Hoyland A, Rausand M. System reliability theory: model and statistical methods. System reliability theory: model and statistical methods. New York, NY: John Wiley & Sons; 1994.

[2] Kuo W, Zuo MJ. Optimal reliability modeling: principles and applications. Optimal reliability modeling: principles and applications. Hoboken, NJ: John Wiley & Sons; 2003.

[3] Lambert BK, Walvekar AG, Hirmas JP. Optimal redundancy and availability allocation in multistage systems. IEEE Trans Reliab 1971;20:182–5. https://doi.org/10.1109/TR.1971.5216123.

[4] Sasaki M, Kaburaki S, Yanagi S. System availability and optimum spare units. IEEE Trans Reliab 1977;26:182–8. https://doi.org/10.1109/TR.1977.5220110.

[5] Tsai CS, Chang CT. A statistics based approach to enhancing safety and reliability of the batch-reactor charging operation. Comput Chem Eng 1996;20:S647–52. https://doi.org/10.1016/0098-1354(96)00117-2.

[6] Lai CA, Chang CT, Ko CL, Chen CL. Optimal sensor placement and maintenance strategies for mass-flow networks. Ind Eng Chem Res 2003;42:4366–75. https://doi.org/10.1021/ie020567j.

[7] Andrews JD, Bartlett LM. A branching search approach to safety system design optimisation. Reliab Eng Syst Saf 2005;87:23–30. https://doi.org/10.1016/j.ress.2004.03.026.

[8] Liang KH, Chang CT. A simultaneous optimization approach to generate design specifications and maintenance policies for the multilayer protective systems in chemical processes. Ind Eng Chem Res 2008;47:5543–55. https://doi.org/10.1021/ie071188z.

[9] Liao YC, Chang CT. Design and maintenance of multichannel protective systems. Ind Eng Chem Res 2010;49:11421–33. https://doi.org/10.1021/ie901818e.

[10] Vaurio JK. Optimization of test and maintenance intervals based on risk and cost. Reliab Eng Syst Saf 1995;49:23–36. https://doi.org/10.1016/0951-8320(95)00035-Z.

[11] Miskin JJ. Control performance assessment for a high pressure leaching process by means of fault database creation and simulation. Control performance assessment for a high pressure leaching process by means of fault database creation and simulation. Stellenbosch University; 2016.

[12] vanEeten P, Kallmeyer JP, McNeely P, Rust N, Hartmann D, Schacht J, et al. W7-X NBI beam dump thermocouple measurements as safety interlock. Fusion Eng Des 2019;146:1329–33. https://doi.org/10.1016/j.fusengdes.2019.02.069.

[13] Guo YH, Cheng Y, Wang BH, Xie N, Zhan TX, Chen ZN, et al. Design of equipment interlocking control system for leaf. Radiat Detect Technol Methods 2019. https://doi.org/10.1007/s41605-019-0144-9.

[14] Liptak B. Optimization of unit operations. Optimization of unit operations. Radnor, PA: Chilton Book Company; 1987.