CHEMICAL ENGINEERING TRANSACTIONS Volume 24, 2011
Editor Sauro Pierucci
 ISBN 978-88-95608-15-0 ISSN 1974-9791
DOI: 10.3303/CET1124044

A Mathematical Programming Approach to Generate Optimal System Configurations and Maintenance Policies for Multichannel Multilayer Protective Systems

Chuei-Tin Chang, Yue-Cheng Liao, Kuo-Hwa Liang, Edwin Wibisono

Department of Chemical Engineering, National Cheng Kung University
Tainan, Taiwan 70101, ROC, ctchang@mail.ncku.edu.tw

In order to mitigate the undesirable effects caused by accidents in chemical plants, it is a common practice to install protective systems on processing units operated under hazardous conditions. The aim of this study is to improve and generalize the current practice for determining the design specifications and maintenance policies of multichannel and/or multilayer protective schemes. A spare-supported corrective maintenance policy is devised in this study to enhance the sensor availability, while a preventive strategy is adopted to check/replace every shutdown unit. By solving an integer program, the optimal configurations of sensors and shutdown units, the best corrective and preventive maintenance policies and alarm/shutdown logics can all be identified automatically.

1. Introduction

Generally speaking, a protective system is used to perform two basic functions, namely alarm and shutdown. The former is facilitated by independent sensors. Based on online measurements, a predetermined logic can be applied to make alarm decision. The latter function is usually performed with actuators, e.g., solenoid valves. Since sensor and valve failures are basically random events, the availability of a protective system is highly dependent upon its configuration and the corresponding maintenance policies.

Any hardware item can fail either safely (FS) or dangerously (FD). The FS malfunctions are recoverable because they are mostly caused by noisy signals, whereas the FD failures often require repair or replacement. To achieve a desired availability level, a common practice in the process industries is to introduce hardware redundancy in design. Specifically, each critical process condition may be monitored with more than one independent sensor, and the measurements signals are sent to a voting gate to generate alarm decision. These sensors are assumed to be maintained with spare-supported maintenance program in this study. On the other hand, it should be noted that the FD failure of a shutdown unit cannot usually be detected online. A preventive strategy must be applied to enhance its availability, that is, every unit is required to be inspected regularly at constant time intervals. The broken equipment must be replaced or repaired when detected, whereas the normal ones are kept online until the next inspection. Therefore, the length of the inspection interval should be considered as a design variable

Please cite this article as: Chang C.T., Liao Y.C., Liang K.H. and Wibisono E., 2011, A mathematical programming approach to generate optimal system configurations and maintenance policies of multichannel multilayer protective systems, Chemical Engineering Transactions, 24, 259-264
DOI: 10.3303/CET1124044

There have been a few attempts in the past to generate the optimal configurations and/or the corresponding maintenance policies with a mathematical programming model, e.g., Andrews and Bartlett (2005), Liang and Chang (2008), and Liao and Chang (2010). The objective of the present study is to develop a generalized mathematical programming model to produce the optimal design specifications and maintenance policies of a comprehensive multichannel multilayered protective system for any application.

2. Multichannel System Designs

2.1 General system structure

The general structure of a single-layer protective system is described below in Figure 1:

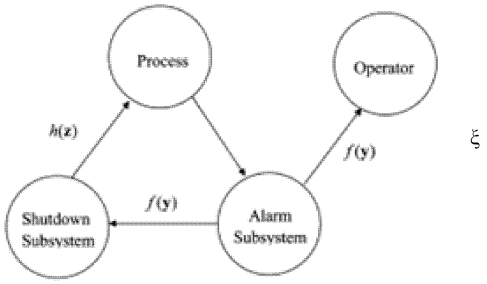

Figure 1: General structure of single-layer protective system.

A binary variable is used to represents the process state, i.e.

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

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

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

Every process variable may be measured with one or more online sensor of identical specifications in an *alarm channel*. The channel outputs also form a binary vector $\mathbf{y} = [y_1, y_2, \cdots, y_M]$. A logic operation can then be applied to these binary values to determine whether an alarm should be set off. This logic can be expressed with an alarm function:

$$f(\mathbf{y}) = \begin{cases} 1 & \text{if the alarm subsystem issues an alarm} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

To facilitate the model formulation, a third binary vector $\mathbf{z} = [z_1, z_2, \cdots, z_N]$ is used to denote whether the designated emergency-response operations are executed by

different shutdown units. More specifically

$$h(\mathbf{z}) = \begin{cases} 1 & \text{if the shutdown subsystem performs the operation successfully} \\ 0 & \text{otherwise} \end{cases} \tag{4}$$

2.2 Total expected loss

The following formula is used in this work to compute the total expected loss for operating a single-layer multichannel system during the *k*th year of its entire life:

$$L1_{PT,k}^{LC} = (1-P_{FS}^{SD})C_{b,k}p - P_{FD}^{SD}C_{a,k}(1-p) - (1-P_{FS}^{SD}-P_{FD}^{SD})\sum_{y} f(\mathbf{y})g(\mathbf{y}) \tag{5}$$

where, $p = \Pr\{\xi = 1\}$ denotes the average existence probability of unsafe state, and $C_{a,k}$ and $C_{b,k}$ respectively represent the financial losses incurred from FS and FD failures of the protective system in the *k*th year. Notice that the function $g(\mathbf{y})$ is defined as

$$g(\mathbf{y}) = C_{b,k}\, p \Pr\{\mathbf{y} \mid \xi = 1\} - C_{a,k}(1-p) \Pr\{\mathbf{y} \mid \xi = 0\} \tag{6}$$

If the outputs of alarm channels are statistically independent, the conditional probabilities in this function can be written as

$$\begin{aligned} P\{\mathbf{y} \mid \xi = 0\} &= \prod_{i=1}^{M} \Pr\{y_i \mid \xi = 0\} = \prod_{i=1}^{M} [A_i^{y_i}(1-A_i)^{1-y_i}] \\ P\{\mathbf{y} \mid \xi = 1\} &= \prod_{i=1}^{M} \Pr\{y_i \mid \xi = 1\} = \prod_{i=1}^{M} [B_i^{1-y_i}(1-B_i)^{y_i}] \end{aligned} \tag{7}$$

By assuming that a *k*-out-of-*n* voting gate is adopted to trigger the alarm channel, the conditional probabilities of the FS and FD failures of alarm channel i (denoted as A_i and B_i respectively) can be expressed as

$$\begin{aligned} A_i &= 1 - (1 - a_i^{\,k})^{n!/k!} \\ B_i &= 1 - \overline{Av}_i^{Corr} \end{aligned} \tag{8}$$

where a_i is the FS probability of a single sensor in i^{th} channel and $\overline{Av}_i^{Corr}$ is the average availability of the *i*th alarm channel. The conditional probabilities of FS and FD faiures of shutdown subsystem can be expressed as

$$\begin{aligned} P_{FS}^{SD} &= \Pr\{h(\mathbf{z}) = 1 \mid f(\mathbf{y}) = 0\} = 1 - \prod_{j=1}^{N}(1-\alpha_j) \\ P_{FD}^{SD} &= \Pr\{h(\mathbf{z}) = 0 \mid f(\mathbf{y}) = 1\} = \prod_{j=1}^{N}\beta_j \end{aligned} \tag{9}$$

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

$$\beta_j = 1 - \overline{Av}_j^{\Pr ev} \tag{10}$$

where $\overline{Av}_j^{\Pr ev}$ is the average availability of the *j*th shutdown unit.

2.3 Life cycle costs

Because the corrective maintenance policy is employed to improve the availability of every alarm channel, the corresponding expenditures should include (a) the purchase cost, (b) the expected repair cost, and (c) the expected replacement cost. The total life cycle cost of alarm subsystem can thus be determined by summing these costs over the entire operation life of the protective system. On the other hand, since the preventive strategy is used to maintain the shutdown subsystem, its life cycle cost must include (a) the purchase cost, (b) the inspection cost, and (c) the expected repair/replacement cost.

3. Multilayer System Designs

For illustration convenience, let us consider a fictitious CSTR reaction system as an example. It is assumed that two kinds of sensors are installed in the first layer to monitor the feed flow rate and reactor temperature respectively. The outputs of corresponding alarm channels are subject to a logic operation so as to determine if the feed flow should be stopped. If this layer fails to function properly, the exceedingly high flow rate and/or temperature will result in high pressure in reactor. To mitigate the potentially dangerous consequences, the reactor vessel is equipped with a pressure relief valve for use as the second layer of protection.

All possible failure-induced scenarios in this multilayer protection system can be enumerated on the basis of an *event tree analysis*. Let FS^{TF} and FS^{P} represent the fail-safe scenarios of the high temperature/flow interlock and pressure relief system respectively, while FD^{TF} and FD^{P} denote the corresponding fail-dangerous scenarios. It should also be noted that the total expected loss of this protective system should not include the cost of normal shutdowns. The total expected loss of operating the 2-layer protective system in the *k*th year can be expressed in a general form as

$$\begin{aligned} L2_{PT,k}^{LC} = {} & C_{a,k}^{TF}\left(1-p^{TF}\right)\Pr\left\{FS^{TF}\right\} + C_{a,k}^{P}\left(1-p^{TF}\right)\left(1-\Pr\left\{FS^{TF}\right\}\right)\Pr\left\{FS^{P}\right\} \\ & + C_{b,k}^{TF}p^{TF}\Pr\left\{FD^{TF}\right\}\left(1-\Pr\left\{FD^{P}\right\}\right) + C_{b,k}^{TFP}p^{TF}\Pr\left\{FD^{TF}\right\}\Pr\left\{FD^{P}\right\} \end{aligned} \tag{11}$$

where, $p^{TF} = \Pr\left\{\xi^{TF} = 1\right\}$; ξ^{TF} is a binary variable reflecting the unsafe process state that triggers high temperature/flow interlock; $C_{a,k}^{TF}$ and $C_{b,k}^{TF}$ respectively represent the financial losses incurred from FS and FD failures of the first protection layer in the *k*th year; $C_{a,k}^{P}$ is the corresponding financial loss incurred from FS failure of the second layer; $C_{b,k}^{TFP}$ the corresponding financial loss incurred from FD failures of both layers. Finally, it should be noted the life cycle costs of a multilayer system can be computed with the same approach described previously in section 2.

4. Case Study

The aforementioned CSTR system is considered in the case study reported here. Due to space limitation, let us focus only on the first protection layer, i.e. the high temperature/flow interlock. It is assumed that the operating life of the system (H) is 5 years and the probability of unsafe state (p^{TF}) in every year is 0.2. At an interest rate (r) of 6% per year, the average yearly costs associated with the FS and FD failures are $\overline{C}_a^{TF} = 8.9302\times10^3$ USD and $\overline{C}_b^{TF} = 8.9302\times10^5$ USD, respectively. The maintenance and cost parameters of the flow sensors and temperature sensors are given in Table 1. The specifications of the solenoid valves are provided in Table 2. These data are adopted from Liao and Chang (2010).

Seven optimization runs were carried out with GAMS based on different initial budgets, and the results are presented in Table 3. The abbreviations 3oo3, 2oo2, and 1oo1 in this table are used to specify alarm logics, which denote 3-out-of-3, 2-out-of-2, and 1-out-of-1 respectively. Notice that the objective value, i.e., the sum of total expected loss during the operation life of the protective system and also the life cycle costs of alarm and shutdown subsystems, can generally be reduced if there is sufficient initial budget which can be allocated to purchase the critical components in the protective system (see case 1-1). In this situation, the total number of temperature sensors is larger than that of flow sensors since the former is cheaper. Despite its higher failure rates, the availability of the temperature alarm channel can be enhanced basically with more components. It can be observed that the optimal purchase cost is actually much lower than the initial budget in case 1-1. This finding implies that 1850 USD is the true optimum without setting any maximum allowable cost limit. If the initial budget is reduced to a lower-than-optimum level, a different system structure must be selected to satisfy the more stringent budget constraint. The resulting structural changes can be summarized as follows:

(i) If initial budget is 1800 USD, the number of spares for temperature sensor must be reduced from 2 to 1.

(ii) If initial budget is 1700 USD, the voting gate of channel 2 must be simplified from 3oo3 to 2oo2.

(iii) If initial budget is 1600 USD or lower, the flow alarm channel should be removed. There is only a single temperature alarm channel left in the protective system.

Table 1: Maintenance and cost parameters of sensors in CSTR system

subsystem	flow channel	temperature channel
λ_i (yr^{-1})	0.3	0.5
μ_i (yr^{-1})	6.0	8.0
ε_i (yr^{-1})	365	365
a_i	0.1	0.15
PCS_i (USD)	350	100
$\overline{RprsC}_i$ (USD)	44.7	17.9
$\overline{RplsC}_i$ (USD)	22.3	17.9

Table 2: Maintenance and cost parameters of shutdown units in CSTR system

subsystem	temperature-flow shutdown subsystem
λ_j (yr^{-1})	0.35
a_j	0.1
PCV_j (USD)	400
$\overline{InspC}_j$ (USD)	89.3
$\overline{RplsC}_j$ (USD)	535.8

Table 3: Optimization results: multichannel alarm configuration

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

5. Conclusion

A mathematical programming approach is taken to generate optimal multichannel and multilayer protective systems configurations and the corresponding maintenance policies. The proposed programming models can be extended for any similiar protective system. A case study is presented in this paper to demonstrate the feasibility and effectiveness of this approach. From the results obtained so far, it can be concluded that the use of either multichannel or multilayer significantly enhances the reliability of protective system. It can be also concluded that, given a sufficient budget, the expenditure of the protective system can be lowered to a level that is not achievable with an ordinary single-channel or single-layer system.

References

Andrews J.D. and Bartlett L.M.A., 2005, Branching search approach to safety system design optimization, *Reliab. Eng. Syst. Saf.* **87**, 23.

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

Liao Y.C. and Chang C.T., 2010, Design and maintenance of multi-channel protective systems, *Ind. Eng. Chem. Res.* **49**, 11421.