THE SELECTION OF TRIP SYSTEM CONFIGURATION

A.G. Rushton
Department of Chemical Engineering, Loughborough University.

A new methodical approach to the selection of trip system configuration (*m* out of *n* systems) is described.
In principle a rational selection can be made by balancing the losses associated with realisation of the hazard, spurious trips and installation of the system, and by appropriate choice of other design variables (e.g. proof test regime). In practice the rigorous application of this approach may be impractical because insufficient or inadequate data is available. In such cases the method can be used to find the range of values to which any particular configuration is applicable. If these implied values are reasonable, then the selection of that particular configuration is supported.

INTRODUCTION

Trip systems are used as protective measures to reduce the frequency or probability of an anticipated undesirable event. A trip system is essentially a two state control loop. A detected excursion from the acceptable range of a process variable (e.g. temperature, concentration, etc.) results in a discrete response (e.g. valve closure, electrical isolation, etc.). The excursion is thus arrested and the potential event (e.g. loss of containment) is prevented.

In general the event to be avoided will have consequences involving loss of capital equipment, production or product, injury to or loss of life, and/or environmental damage. It is protection against these potential consequences which is sought. The trip system is arranged to intervene automatically so that plant personnel are able to concentrate on maintaining production.

Alarms are often an adequate and cost-effective alternative to trip systems. In the following discussion it is assumed that the alarm option has been ruled out, perhaps because of the required speed of response or because the plant is not constantly staffed.

The selection and specification of an appropriate configuration for a trip system is a skilled task. Examples are described by Lawley and Kletz (1). When selecting from among the more elaborate configurations a compromise is made between protection against the identified potential consequences (the hazard) and avoidance of unnecessary (spurious) trips. The installation of an inappropriate configuration (or none) can occur either because the need to consult an expert is not appreciated or because the approach taken by an expert is based on an incorrect judgement or because poor data or faulty logic has been used. The consequence of such an installation will be either unnecessary risk of consequences from the hazard or increased nuisance (and loss) from spurious trips or excessive cost of the protective system.

Current industrial practice involves considerable use of engineering judgement. Firstly the potential for a hazardous event or incident to occur must be identified. This may be self evident to the design team or may be found by the use of hazard identification techniques. The installation of a trip system to mitigate a serious hazard is normally considered only when the alternatives of inherently safer design or passive protective measures (e.g. pressure relief valves) have been exhausted.

The decision to specify a trip will normally be taken on the basis that the combination of expected incident frequency and magnitude is unacceptable. If minor consequences are anticipated then a single channel trip will be decided upon. If significant consequences are anticipated then more sophisticated configurations might be considered in order to achieve a satisfactorily small fractional dead time (FDT), that is the average fraction of time in which the system will not respond to an excursion. Such systems have a number of channels (n) configured so that the system will operate if some of these channels (m) are activated. The use of more than three channels is not normally considered, but diversity (in which, for example, the sensed variable or method of sensing is not the same for each channel) as well as simple redundancy (in which each channel is a replica of the others) is considered in many cases in order to reduce the susceptibility of the system to common cause failures.

Trip System Reliability Analysis

A trip system has elements which are analogous to those of a control system, i.e. sensors, control devices and actuators. The difference is that the response is usually two-state rather than continuous. A trip loop is thus normally dormant whereas a control loop is continuously active. The state of the plant, as presented by the signals from the sensors, is interpreted by the control device as either acceptable, in which case no action is taken, or unacceptable, in which case the actuator is caused to operate. The control device is usually latched so that once an unacceptable state is sensed the trip cannot be halted, and requires operator action to restore normal operation. The change in state of the plant with the potential for causing a hazardous event (usually the crossing of some threshold value) is described as a demand and the operation of the trip system actuators is described as a trip.

The behaviour of a particular trip system configuration can be analysed in terms of operational and functional failures. Operational failures are those which cause the system to *operate* (or a channel to be activated) needlessly. Operational failure of the system is known as a spurious or nuisance trip. Functional failures are those which cause the system (or channel) to enter a state in which it will not *function* should the need arise. Each type of failure of the system as a whole is described in relation to the corresponding operational and functional failure rates of individual channels of the system, γ_1 and λ_1 respectively.

Spurious trips will involve significant losses in many modern plant designs: integration of several processes and material and heat recycles can mean that the action of one trip will have repercussions causing other protective and trip systems to be initiated. Apart from the economic losses associated with an unnecessary shut-down and the following down-time and start-up, the actions of shutting down and starting up are generally more hazardous than steady state operation and so spurious trips will often have safety implications. Prevention of spurious trips must be balanced against protection from the hazard, as described by van Eijk (2) and Cobb and Monier-Williams (3).

The system can be in one of four states as shown in Table 1. The normal state is *no demand, no trip* so transitions from this state are considered. The three remaining states each involve losses.

TABLE 1 - System States.

	No Trip	Trip
No Demand	Normal Operation	Spurious Trip
Demand	Hazard	Genuine Trip

In the first (*demand, no trip*) there is a failure of the system to trip on demand. The consequence will be the realisation of the hazard against which the system was intended to offer protection. This will arise if a demand occurs while the system is in a state of functional failure (neglecting the possibility that the system has been disarmed). The frequency with which this state is entered is thus dependent on both the demand rate and on the FDT of the system. The hazard rate, η, of the protected system is then

$$\eta = \delta\phi \qquad (1)$$

where δ is the demand rate
and φ is the fractional dead time.

In the second (*no demand, trip*) there is a trip without a demand. The consequence will commonly be a shut-down of the protected plant. Alternatively the trip may start up mitigation equipment such as an absorber or fire-water system. This consequence would have been avoided if no trip system had been fitted and so is a penalty incurred by the decision to install the system. In principle, the frequency of this state arising is dependent on the operational failure rate of the system, γ. In practice spurious trips can also result from operator and maintenance errors.

In the third (*demand, trip*) the system operates on demand and the hazard is avoided. The loss is reduced to that of a trip. The trip rate β, is given by

$$\beta = \delta(1-\phi) \qquad (2)$$

In simple treatment of trip systems it is normally assumed that operational failures are immediately revealed to the operating personnel (by their action in $1/n$ systems and by alarms in other systems), whereas functional failures remain unrevealed until either a proof test is carried out or a demand occurs. The FDT and operational failure rates are then given in Table 2. These expressions are based on the assumption that all failures are independent, that is there are no common cause failures.

The expressions quoted are for (practically) simultaneous proof testing of all installed channels. Some improvement can be gained by having a staggered testing regime, the benefits are discussed by Green and Bourne (4).

TABLE 2 Trip System Failure.

Configuration *m/n*	Functional Failure Fractional Dead Time φ	Operational Failure Rate γ
1/1	$\frac{\lambda_1\tau_p}{2}$	γ_1
1/2	$\frac{(\lambda_1\tau_p)^2}{3}$	$2\gamma_1$
2/2	$\lambda_1\tau_p$	$2\gamma_1^2\tau_r$
1/3	$\frac{(\lambda_1\tau_p)^3}{4}$	$3\gamma_1$
2/3	$(\lambda_1\tau_p)^2$	$6\gamma_1^2\tau_r$
3/3	$\frac{3\lambda_1\tau_p}{2}$	$3\gamma_1^3\tau_r^2$
m/n	$\binom{n}{r}\frac{(\lambda_1\tau_p)^r}{r+1}$	$n\gamma_1\binom{n-1}{m-1}(\gamma_1\tau_r)^{m-1}$

$$r = n - m + 1$$

$$\binom{n}{r} = \frac{n!}{(n-r)!\,r!}$$

$$\eta = \delta\phi$$

The expressions derived for hazard rate (the product of demand rate and FDT from Table 2) are approximations, valid if

$$\lambda_1\tau_p \ll 1 \quad ; \quad \delta\tau_p \ll 1 \quad ; \quad \eta\tau_p \ll 1 \qquad (3)$$

These inequalities are most often satisfied. The expressions not limited to these cases are discussed by Lees (5). FDT's are considered in detail by Wheatley and Hunns (6).

Current Practice

Where the prospective consequence is minor economic loss or a small hazard the decisions on whether to install a trip system and what configuration to specify will often be taken by a process engineer in the design team. Where the loss is very significant or the need for a complex system is recognised then a reliability specialist will be involved. This involvement of a specialist may be at the request of the design team or may be the result of an action from a hazard review meeting (for example a hazard and operability study meeting).

The path followed by the design engineer will typically be:-

i) Recognise hazard or loss is minor (else consult expert)
ii) Consider use of alarms (rule out if response time inadequate)
iii) Estimate the losses that will be incurred with no trip
iv) Set this against the approximate cost of installing a trip (~ the same as a control loop)
v) Select single channel (1/1) or no trip accordingly.

If a single channel system is selected then, even if the estimates made were good, an error in trip system selection can occur because the spurious trip element of the equation has been neglected. If this element is significant then either a configuration with a lower spurious trip rate would be better or, if the extra expense on channels cannot be justified, then no trip system could be preferable.

If an expert is consulted then a more detailed assessment of the case can be made. The expert may consider operational factors and check the appropriateness of simplifying assumptions to the case in hand. An assessment of the maximum permissible FDT can be made. An initial selection of a trip system configuration, based on the target FDT, may later be revised if the operational failures are considered unacceptable (or for other reasons).

For typical cases the ranking of *m/n* configurations with respect to functional failure (as reflected by FDT) and with respect to operational failure rate will be invariant and these are shown in Table 3. 1/2, 2/3 and 1/1 systems are commonly selected, depending on the desired balance between operational and functional behaviour. A 1/3 system is rarely justified for hazards with only financial implications as the increase in reliability is only marginal, because of dependent failures, and the operational failure rate is also relatively high. The consequences of spurious trips are rarely so onerous as to warrant 2/2 or 3/3 configurations.

For serious hazards a fault tree will normally be constructed. The effect of various trip systems can then be seen by including the protective system in the logic of the tree, an example is given by Stewart (7). In these cases, the required reliability may be determined by the need to achieve a specified trip system reliability for effective control of the hazard. There may however also be financial considerations as described in this paper, which could be taken into account by the methods described here in choosing a system which meets the reliability needs most cost-effectively.

Operational factors may colour the final decision. For example

i) In a marginal case a 2/3 system may be favoured because

TABLE 3 - Configuration Failure Ranking.

φ or γ	Functional	Operational
Low	1/3	3/3
	1/2	2/2
	2/3	2/3
	1/1	1/1
	2/2	1/2
High	3/3	1/3

a) It can be tested without being disarmed. The risk of the system being left in a disarmed condition is thus reduced.

b) During testing there is an improvement in functional reliability if the tested channel is put into an activated state (2/3 becomes 1/2).

ii) In a marginal case a proliferation of 1/1 systems may be deprecated because the frequent spurious trips may frustrate the operators and lead to a culture in which trips are regarded as a nuisance.

Limitations to Current Practice

There are two principal objections to current practice. Firstly, where a trip is decided upon, there is no published formal method for checking that the selected configuration is optimal. Secondly, the consequences of operational trip system failure (spurious trips) are often neglected.

PROPOSED METHOD FOR SELECTION OF OPTIMAL TRIP CONFIGURATION

The method of trip selection proposed here is based on the contention that the optimal configuration will be the one for which the sum of the cost of the trip system, the cost of failures on demand, the cost of spurious trips and the cost of genuine trips is minimal. Each term in the sum can be expressed as an annual cost, for convenience.

Denoting C as the annual cost of a trip system channel, and H, S and G as the costs assigned to the consequences of a hazard, a spurious trip and a genuine trip respectively, it follows that for a particular configuration a measure of the anticipated expense, V, is

$$V = nC + \eta H + \gamma S + \beta G \tag{4}$$

Substitution from Equations (1) and (2) gives,

$$V = nC + \delta\phi H + \gamma S + \delta(1-\phi)G \tag{5}$$

The system configuration giving minimum V should be optimal.

[Note that a simple model is used for the trip system installed cost. Experience of maintenance costs (dependent on proof test interval and plant life) and non-proportionality (e.g. two channels cost less than twice one channel) could be easily incorporated.]

For a genuine trip there is an element of loss related to the process failure which caused the demand. This cannot be avoided by any configuration. Neglecting this element, the cost of a genuine trip is approximately the same as that of a spurious one so Equation (5) becomes

$$V = nC + \delta\phi H + [\gamma + \delta(1-\phi)]S \tag{6}$$

Thus, in principle, for a given application (defining δ, H, S) the optimal configuration of trips (described by n, φ, γ, C) can be selected.

In practice the engineer exercises some control over the specification of the system variables, in particular by selecting the proof test interval, but also, for example, by the quality of components in the system.

The question of selecting a proof testing interval is a thorny one. Many companies have standard intervals for such checks (8). The simple expressions for FDT neglect the fact that too frequent testing may adversely affect the reliability. These adverse effects arise from, for example, opportunities for error (in particular failure to isolate before testing, leading to spurious trip, and failure to re-arm after testing), and perhaps reduced redundancy during testing, depending on the configuration. These problems are discussed by Enzinna (9). In addition, less frequent testing represents an economic saving in its own right. These refinements are not addressed here.

Equation 6 can be rewritten, by division through by C, in terms of the ratios of hazard cost to channel cost, and spurious trip cost to channel cost.

$$\frac{V}{C} = n + \delta\phi\left(\frac{H}{C}\right) + [\gamma + \delta(1-\phi)]\left(\frac{S}{C}\right) \tag{7}$$

For any particular application (characterised by the demand rate, δ), if a proof test interval is chosen and if repair time, single channel annual cost and single channel failure rates (λ_1, γ_1) are specified, then a plot or 'map' showing the optimum configuration for any combination of these two ratios, H/C and S/C, can be drawn up (with the aid of a computer). The effect of changes in demand rate, proof test interval, repair time or single channel failure specification can be quickly evaluated by regenerating this map. The region in which any particular configuration is indicated will be bounded by points where two or more configurations give identical values for V/C.

EXAMPLE CONFIGURATION MAP

An example of a map showing system configuration for minimum V is given as Figure 1. The data from which the map was generated is given in Table 4. The map was produced by simple computer implementation of Equation (7). If values of H/C and S/C are (approximately) known then the location on the map will show the optimal configuration and how clearly this configuration is distinguished from the alternatives.

TABLE 4 - Example Values.

λ_1	0.2 yr^{-1}
γ_1	0.5 yr^{-1}
τ_p	1/12 yr
τ_r	1/52 yr
δ	0.01 yr^{-1}
t	10 yr

Here, for example, the location X has 2/3 as its optimal configuration but is close to a region where 1/2 would be indicated. In a more sophisticated implementation the user could obtain a ranking of the various configurations for a given location or view a 'section' through the map for a given value of H/C or S/C showing how (V/C) varies for each configuration.

Where the ratios H/C and S/C are unknown then the map can provide ranges of values of these ratios which are compatible with a proposed selection.

The second map given in Figure 2 shows the effect of a higher demand rate. Sensitivity to other variables, such as proof test interval, can similarly be explored. Often the selection of proof test interval will be to suit other operations, so fine variation of proof test interval in the model will not be realistic because such variation would incur hidden costs. Some variables are interdependent and must be varied together, for example a higher specification of single channel operational failure rate may be made, but with an increased cost associated with each channel installed.

It is envisaged that a default set of values $(\tau_p, \tau_r, C, \lambda_1, \gamma_1)$ would be made available to process design engineers, whilst a reliability engineer would use a database, providing for greater flexibility.

A preference for, say, 2/3 systems could be incorporated by, for example, discounting a proportion of V for this configuration, enlarging the region in which this configuration would be indicated.

BENEFITS

The main benefits of the proposed method are:-

i) Because rapid evaluation is possible the cost of exploring alternative configurations is reduced.
ii) The possibility of non-optimal selection is reduced. In particular where the loss is not sufficiently high to warrant expert consideration under current practice and 1/1 is worse than no trip or 1/1 is worse than a more elaborate configuration.
iii) Where there is insufficient data to pursue the method, then the decision arrived at by current practice can be validated by finding the range of values for which the configuration is optimal. The reasonableness of these ranges (in the sense that they probably include the unknown values) will support (or not) the proposed selection.
iv) The sensitivity of the selection to design variables can be investigated.
v) The systems installed in existing plant can be audited. This may be to confirm the initial selection or to make use of data gleaned from operating experience.

CONCLUSIONS

If sufficient data is available, different trip system configurations can be compared in respect of their suitability for a given duty by summing the costs of installation, spurious trips, genuine trips and hazard realisations for each candidate configuration. In principle the lowest sum indicates the optimum selection.

A particular configuration will be favoured over a range (or envelope) of conditions. The three key variables (channel cost, spurious trip cost and hazard cost) can be reduced to two by taking the ratios of any two to the third. The optimal configurations can then be presented as regions on a map of the two chosen ratios.

Where insufficient data is available to establish the position of interest on the map, then the map can be used to support, audit or challenge any selection made by other means, or a selection can be made by judging the probable position.

The strength of this approach does not lie in its rigorous application but in its usefulness for cases where there is sparse information.

Use by expert :-

i) Affirmation of a decision arrived at by other means,
ii) Review of existing installations,
iii) Assessment of sensitivity to proof test interval, component failure rates etc.

Use by process engineer :-

i) Decision aid for simple low priority trips (e.g. protection of heating element),
ii) Decision aid for choosing to consult with expert.

FUTURE WORK

Data from industrial selection cases is being obtained in order to test and refine the model. An implementation of the model on a PC will then be made available to an industrial collaborator for evaluation.

The example presented here is based on an assumption of no common cause failures. This is often an unacceptable simplification but is not a restriction of the methodical approach described above. An extension to the computer code is underway, using the *beta* method of handling common cause failures to revise the values of operational and functional failure rate for each configuration. The *beta* method and other methods of handling common cause failure are discussed by Smith (10). A further complication is the probability of common cause between demand and trip system failure, this can be addressed by similar methods.

SYMBOLS USED

m	= number of channels that must survive for trip system to survive.
n	= number of channels in trip system.
r	= number of channels that must fail for trip system to fail.
C	= annual cost (per channel) of trip system (£ year^{-1}).
G	= cost of genuine trip (£).
H	= cost of hazard (£).
S	= cost of spurious trip (£).
V	= annual sum cost of trips and hazards (£ year^{-1}).
β	= genuine trip rate (year^{-1}).
γ	= overall operational failure rate of trip system (year^{-1}).
γ_1	= operational failure rate of single channel (year^{-1}).
δ	= demand rate (year^{-1}).
η	= hazard rate (year^{-1}).
λ	= overall functional failure rate of trip system (year^{-1}).
λ_1	= functional failure rate of single channel (year^{-1}).
τ_p	= proof test interval (year).
τ_r	= repair time (year).
φ	= fractional dead time of trip system.

REFERENCES

1. Lawley, H.G., and Kletz, T.A., 1975, Chem. Engng 82, 81.

2. Van Eijk, F.P., 1975, Chem. Engng Prog. 71, 48

3. Cobb, A.J., and Monier-Williams, S., 1988, Plant Oper. Prog. 7, 243.

4. Green, A.E., and Bourne, A.J., 1972, "Reliability Technology", Wiley, New York, USA.

5. Lees, F.P., 1982, Reliab. Engng 3,N 1.

6. Wheatley, C.J., and Hunns, D.M., 1981, "Third National Reliability Conference - Reliability 81".

7. Stewart, R.M., 1974, Chem. Engnr 290, 622.

8. Lees, F.P. 1980, "Loss Prevention in the Process Industries", Butterworth, Seven Oaks, England.

9. Enzinna, R., 1985, Nuc. Engng Int. 30, 29.

10. Smith, D.J. 1985, "Reliability and Maintainability in Perspective", Macmillan, London, England.

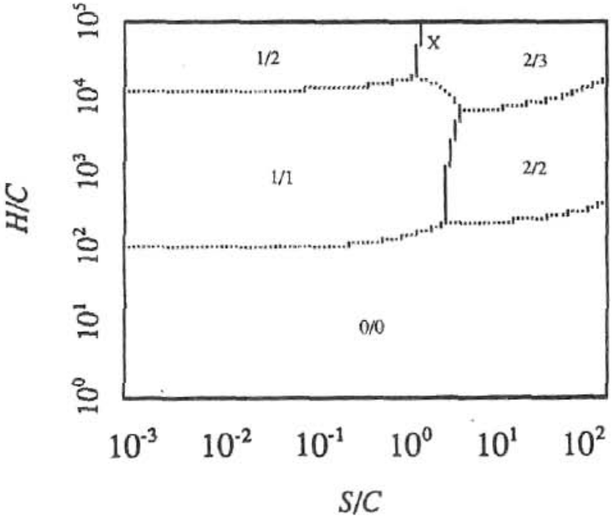

Figure 1 Example map of optimal trip system configuration, data from Table 4 [Note that 1/1 systems are under-rated in this map because common cause failures have been neglected]

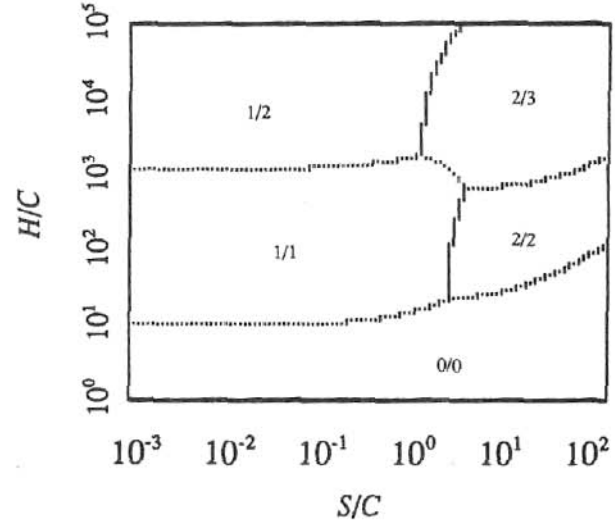

Figure 2 Example map of optimal trip system configuration, data as in Table 4 but with $\delta = 0.1$ [Note that 1/1 systems are under-rated in this map because common cause failures have been neglected]