1979

Optimum trip level of M-out-of-N reactor temperature trip-amplifier systems

J. M. Kontoleon

University of Wollongong

Abstract
This paper determines the optimum high-trip- level setting of m-out-of-n:G temperature- trip-amplifier systems,used for the protection of nuclear reactors against excess temperatures, which results in the maximum reliability. The bivariate normal distribution is used to simulate the fluctuation of the thermocouple signals and the uncertainties of the trip settings. The thermocouples and the trip amplifiers can fail in two modes of failure: fail-safe and fail-danger. It is shown that by properly selecting the trip levels of the amplifier units the reliability of the protection system is maximized. The optimum trip-level is calculated for various commonly used configurations using a computer algorithm.

IEEE Transactions on Nuclear Science, Vol. NS-26, No. 4, August 1979

OPTIMUM TRIP LEVEL OF M-OUT-OF-N REACTOR TEMPERATURE TRIP-AMPLIFIER SYSTEMS

J.M. Kontoleon
Department of Electrical Engineering
University of Wollongong, N.S.W 2500
Australia

ABSTRACT

This paper determines the optimum high-trip-level setting of m-out-of-n:G temperature-trip-amplifier systems, used for the protection of nuclear reactors against excess temperatures, which results in the maximum reliability. The bivariate normal distribution is used to simulate the fluctuation of the thermocouple signals and the uncertainties of the trip settings. The thermocouples and the trip amplifiers can fail in two modes of failure: fail-safe and fail-danger. It is shown that by properly selecting the trip levels of the amplifier units the reliability of the protection system is maximized. The optimum trip-level is calculated for various commonly used configurations using a computer algorithm.

INTRODUCTION

In nuclear power station design every effort is being made to increase the efficiency of the plant, by keeping temperatures as high as possible consistent with an acceptable fuel element failure rate. The fine limits between the normal (full power) reactor temperature and the maximum allowable fuel-clading temperature, demand a detail consideration of the measured variables and equipment used to safeguard the reactor against excessive temperatures. Measured variables are subject to fluctuations[1] because of either the statistical nature of the transducers or the phenomenon under measurement itself. On the other hand, equipment used for assessing the levels of the measured variables are also subject to variations due to the regular (periodic) imperfect checking of their functions; i.e., there is always a spread in the settings of the various levels around the desired mean. Under certain conditions, such fluctuations may cause fail-safe and fail-danger conditions in excess of those which are encountered under conditions of amplifier-unit and thermocouple failures[2,3].

This paper presents an overall reliability assessment of an m-out-of-n temperature trip amplifier system and shows that the overall reliability depends, among other factors, on the trip-level setting. The optimum level of trip-setting is determined using a computer algorithm.

Manuscript received on January 10, 1979.

TEMPERATURE TRIP-AMPLIFIER

The temperature-trip-amplifier (TTA) receives a signal from a thermocouple located in the reactor core. The allowable reactor temperature limit depends on the type of reactor and a number of other design characteristics. The TTA has an adjustable trip-level (usually called high-trip-level) to cover a wide range of reactor types. Usually, the temperature range is covered by a voltage variation at the input of about 50 mV.

The operational ability of TTA units is verified by testing periodically their functions. The aim is to ensure that each unit is free of failures (partial or catastrophic) and that it gives a trip condition as soon as the level of the monitored variable exceeds the TTA preset trip-level. Many designs of TTA units involve redundancies at the component or subsystem level and employ principles which reduce the fail-danger probability, often at the expence of reliability. However, apart from the fail-safe and fail-danger probabilities of a unit (which are due to some combinations of component failures) there exists another pair of similar probabilities which is due to fluctuations of the measured variables and variations of the trip-level settings at the various periodic tests. This additional pair of probabilities also contributes to the TTA fail-safe and fail-danger probabilities. For instance, a conservative setting of the trip-level combined with fluctuations of the monitored variable will increase the frequency of spurious reactor trips; also, a nonconservative trip-level setting will give rise to a higher probability of an unprotected accident.

As it is very important to reduce every contribution to the overall system fail-safe and fail-danger probabilities, m-out-of-n redundant configurations are commonly used. Thus, a coincidence of at least m unit trips (due to failures or parameter fluctuations) must occur in order to cause a reactor shutdown. It must be pointed out that, in contrast to the case of spurious reactor trips, the fluctuations of the monitored variable and trip-level settings, will have an effect (as the other types of failures) only if there exists a concurrent accident involving the monitored variable. In overall, the effect of parameter fluctuations and catastrophic type failures can be minimized by the use of redundancy and by selecting the optimum setting for the TTA trip-level.

In the following, the optimum setting of

0018-9499/79/0800-4645$00.75

trip-level for a given m-out-of-n redundant configuration is obtained; the analysis makes use of fail-safe and fail-danger probabilities for the thermocouple and TTA units and develops expressions for the overall system fail-safe and fail-danger probabilities. Given the system repair rates (for the various fault conditions) these probabilities can be used for determining system downtime or frequency of reactor trips.

Assumptions

a) The thermocouples and the TTA units can fail in either the fail-safe or the fail-danger mode of failure.

b) The thermocouple signal levels and the TTA trip-levels are s-independent and normally distributed.

c) The reactor operates close to its temperature limit (maximum efficiency); the process which involves the monitored variable is stationary.

Notation

n	total number of TTA units and thermocouples.
m	minimum number of signal excursions above the trip-level for initiating the protective action.
x	it is one of g, s, d and it is used as subscript; g, s, d denote the good, fail-safe and fail-danger states respectively.
P_{tx}	probability that the thermocouple is in state x.
P_{ax}	probability that the amplifier unit is in state x.
μ_t, σ_t	mean and standard deviation of the thermocouple signal.
μ_a, σ_a	mean and standard deviation of the TTA trip-level.
$Pr\{\cdot\}$	probability of event $\{\cdot\}$
$P_x(m;n)$	probability that the m-out-of-n:G system is in state x.
T_{max}	limit for reactor temperature

1-OUT-OF-1:G SYSTEM ANALYSIS

The general analysis is simplified by considering first the case of 1-out-of-1:G system; for a single thermocouple in series with a trip-amplifier define the following states:

1) GG: The series system is good and the thermocouple signal is above the trip-level and above T_{max}, or the series system is good and the thermocouple signal is below the trip-level and below T_{max}.

2) GS: The series system is good and the thermocouple signal is above the trip-level but lower than T_{max}.

3) GD: The series system is good and the thermocouple signal is below the trip-level but above T_{max}.

4) FS: The series system is in the fail-safe state irrespectively of the levels of the thermocouple signal and the trip-setting.

5) FD: The series system is in the fail-danger state irrespectively of the levels of the thermocouple signal and the trip setting.

The corresponding probabilities are:

$$Pr\{GG\} = P_{tg}P_{ag}\cdot(1 - Pr\{GS\} - Pr\{GD\}) \qquad (1)$$

$$Pr\{GS\} = P_{tg}P_{ag}\int_{-\infty}^{T_{max}}\int_{-\infty}^{x} f(x,y)\,dydx \qquad (2)$$

$$Pr\{GD\} = P_{tg}P_{ag}\int_{T_{max}}^{\infty}\int_{x}^{\infty} f(x,y)\,dydx \qquad (3)$$

$$Pr\{FS\} = P_{ts}P_{ag} + P_{as} \qquad (4)$$

$$Pr\{FD\} = P_{td}P_{ag} + P_{ad} \qquad (5)$$

where

$$f(x,y) = \frac{1}{2\pi\sigma_t\sigma_a}\exp\left(-\frac{(x-\mu_t)^2}{2\sigma_t^2} - \frac{(y-\mu_a)^2}{2\sigma_a^2}\right) \qquad (6)$$

is the bivariate density function.

Since the thermocouple signal and the trip-level setting are s-independent, the bivariate normal density is partitioned into $f_x(x)$ and $f_y(y)$, with

$$f(x,y) = f_x(x)\,f_y(y) \qquad (7)$$

$$f_x(x) = \frac{1}{\sigma_t\sqrt{2\pi}}\exp\left(-\frac{(x-\mu_t)^2}{2\sigma_t^2}\right) \qquad (8)$$

$$f_y(y) = \frac{1}{\sigma_a\sqrt{2\pi}} \exp\left(-\frac{(y-\mu_a)^2}{2\sigma_a^2}\right) \qquad (9)$$

Then eqn. (2) becomes,

$$\Pr\{GS\} = P_{tg}P_{ag} \cdot \int_{-\infty}^{T_{max}} f_x(x)dx \cdot \int_{-\infty}^{x} f_y(y)dy$$

$$= \frac{P_{tg}P_{ag}}{\sqrt{2\pi}} \cdot \int_{-\infty}^{(T_{max}-\mu_t)/\sigma_t} e^{-z^2/2}dz \cdot \int_{-\infty}^{x=z\sigma_t+\mu_t} f_y(y)dy$$

$$= \frac{P_{tg}P_{ag}}{2\pi} \cdot \int_{-\infty}^{A_1} e^{-z^2/2}dz \cdot \int_{-\infty}^{(z\sigma_t+\mu_t-\mu_a)/\sigma_a} e^{-u^2/2}du$$

$$= C \cdot \int_{-\infty}^{A_1} e^{-z^2/2}dz \cdot \int_{-\infty}^{A_2} e^{-u^2/2}du \qquad (10)$$

where

$$C = P_{tg}P_{ag}/2\pi \qquad (11)$$

$$z = (x-\mu_t)/\sigma_t \qquad (12)$$

$$A_1 = (T_{max}-\mu_t)/\sigma_t \qquad (13)$$

$$A_2 = (z\cdot\sigma_t - \mu_t - \mu_a)/\sigma_a \qquad (14)$$

Similarly, eqn. (3) becomes,

$$\Pr\{GD\} = C \cdot \int_{A_1}^{\infty} e^{-z^2/2}dz \left(1 - \int_{-\infty}^{A_2} e^{-u^2/2}du\right) \qquad (15)$$

GENERAL ANALYSIS

The reliability of the m-out-of-n:G system is evaluated after considering the fail-safe and fail-danger probabilities.

a) Fail-safe analysis

At least m subsystems (1-out-of-1) should be in GS or FS (in total) in order to give a fail-safe condition; then,

$$P_s(m;n) = \sum_{k=0}^{n} \sum_{\substack{j=r \\ j>0}}^{n-k} \Phi(k,\ j,\ n-k-j) \qquad (16)$$

where

$$r = m - k \qquad (17)$$

and

$$\Phi(k,\ j,\ n-k-j) = \frac{n!}{k!\,j!\,(n-k-j)!} \cdot (\Pr\{GS\})^k \cdot (\Pr\{FS\})^j \cdot (1-\Pr\{GS\}-\Pr\{FS\})^{n-k-j} \qquad (18)$$

is the multinomial density.

b) Fail-danger analysis

At least n-m+1 subsystems should be in GD or FD (in total); then the l.h.s (16) holds with r=n-m-k+1.

c) Reliability

$$P_g(m;n) = 1 - P_s(m;n) - P_d(m;n) \qquad (19)$$

OPTIMUM TRIP-LEVEL SETTING

In order to investigate the dependence of reliability on the trip-level setting of the TTA units a computer algorithm was developed. The computer program (TRIP) accepts the following:

i) m and n : system configuration
ii) q_{ts}, q_{td} : thermocouple probabilities
iii) q_{as}, q_{ad} : amplifier probabilities
iv) T_{max} : reactor temperature (limit)

v) σ_t/σ_a : ratio of standard deviations

vi) Option parameter for controlling type of analysis. : it is either 1 or 2. Option 1 requests the trip-level setting and provides $P_s(m;n)$, $P_d(m;n)$ and $P_g(m;n)$. Option 2, gives the optimum trip-level setting which results to the maximum $P_g(m;n)$; $P_g(m;n)$ is also printed out.

Option 1 employs Simpson's rule to evaluate the double integrals in (2)-(3) which are used in (13)-(16). Option 2 involves in addition the pattern search technique[4] for obtaining the optimum trip-level setting. Some specific results are given below.

a) Example 1 : Let m=1, n=1, q_{ts}= 0.005, q_{td}= 0.008, q_{as}= 0.001, q_{ad}= 0.015, σ_t/σ_a= 1 T_{max}= μ_t+ $3\sigma_t$; option 1 with μ_a= μ_t+ $3\sigma_t$ gives $P_s(1;1)$ = 0.0309, $P_d(1;1)$= 0.0232 and $P_g(1;1)$= 0.9457; for the same example, if μ_a= μ_t+ $6\sigma_t$, $P_s(1;1)$= 0.0148, $P_d(1;1)$= 0.0240 and $P_g(1;1)$= 0.9610.

b) Example 2 : Consider a 2-out-of-3:G system with thermocouple and amplifier probabilities as in the previous example. Let T_{max}=μ_t+ $3\sigma_t$ and σ_t/σ_a= 1.5. Option 2 gives the optimum trip-level setting equal to μ_t+ $5\sigma_t$; the corresponding reliability is 0.9976 and the fail-safe, fail-danger probabilities are $6.57\text{x}10^{-4}$ and $17.12\text{x}10^{-4}$ respectively. If instead, a 2-out-of-4:G system is used, then Option 2 gives μ_a= μ_t+ $6\sigma_t$ and the maximum reliability equal to 0.9986; the corresponding fail-safe and fail-danger probabilities are $13.01\text{x}10^{-4}$ and $0.5\text{x}10^{-4}$ respectively.

CONCLUSIONS

The analysis reaveals that the reliability of m-out-of-n:G systems can be maximized by selecting appropriately the TTA units trip level. The optimum setting depends on the configuration of the system (m,n), fail-safe and fail-danger probabilities and statistical parameters of the thermocouple signals and TTA trip-levels. By changing from one system configuration to another, as for example when additional redundancy is introduced, a new optimum trip-level usually results.

REFERENCES

1. S.H. Hanauer and C.S. Walker, "Design Principles of Reactor Protection Instrument Systems" ORNL-NSIC-51, UC-80, September 1968.
2. J.M. Kontoleon, "Analysis of a Dynamic Redundant System", IEEE Trans. Reliability, R-27, No. 2, June 1978.
3. J.M. Kontoleon, "Optimal Design of a Quasi-Redundant Protective System for Nuclear Reactors", IEEE Trans. Nuclear Science, NS-25, Dec. 1978.
4. R. Hooke and T.A. Jeeves, "Direct Search Solution of Numerical and Statistical Problems", J. Assoc. Comp. Mach., Vol. 8 (2), April 1961.