Common Cause Failure Analysis of Fault Tolerance Systems with Diversity Defense Mechanism

Kai Wang[1], Aidong, Xu[1], Hong Wang[1], Yan Song[1,2],and Zhanyuan, Bai[1]
[1]Key Laboratory of Industrial Informatics, Shenyang Institute of Automation, Chinese Academy of Sciences, China
[2]The Graduate School of the Chinese Academy of Sciences, China
wangkai@sia.cn, xad@sia.cn, wang@sia.cn, songyan@sia.cn, breezyon@sia.cn

***Abstract*-Common cause failures (CCF) are a serious threat to redundant system reliability. It is therefore important to quantify and model CCF in reliability assessments. Design diversity has long been used to protect redundant systems against CCF. However, it is difficult to quantify the effects of diversity on system reliability. Therefore, a novel method based on Root Cause (RC) and Coupling Factor (CF) is proposed to assess diverse redundancy system reliability in this paper. The key idea of the novel method is to classify the RCs into (sub-)categories and then assess the corresponding CFs between redundant components respectively based characteristics of diversity. A novel CCF model is proposed to describe the relationship between CCF probability and diversity. Finally, aiming at the CCF induced by external environment stress an example is given to illustrate the usage of the novel method.**

I INTRODUCTION

In a safety-critical system, the role of a fault-tolerant control system is extremely important. One of its functions is to steer the process to a safe state whenever undesirable events (known as faults) occur. To fulfill this role reliably, the availability of the fault-tolerant control system has to be high [1]. Thus, to achieve a high degree of availability against random failures, redundancy is commonly applied in the fault tolerant systems. If all system failures are statistically independent events, reliability can be significantly improved through the use of redundancy in the design. However, multiple dependent failures of redundant components are not rare. For example, estimates in the nuclear power industry indicate that 1-20% of all hardware failures are of the common-cause variety [2]. Common cause failures (CCF) are a subset of dependent failures. IEC 61511 (2003) [3] defines a CCF as a failure which is the result of one or more events, causing failures of two or more separate channels in a multiple channel system, leading to a system failure. A natural component of the study of CCF is the study of diversity. As early as 1970, diversity was identified as an effective antidote for CCF [4]. While there is clear evidence that diversity can bring benefits in a redundant system, these benefits are extremely difficult to assess. The conventional notion of diversity relies on "independent" generation of "different" implementations. This concept is qualitative and does not provide a basis for comparing the reliabilities of two diverse systems. In [5], the validation of diversity to enhance system reliability has been verified based on a stress-strength failure model and Monte Carlo simulations. However, how to quantify the effects of diversity on system reliability was not proposed. A metric to quantify diversity among several designs is proposed in [6]. However, the prerequisite to applying the metric to calculate diversity is that the distribution of fault pairs of redundant components has to be known in advance. Therefore, the metric proposed is difficult to be applied in the practical design process. In [7], a diversity index was proposed to quantify diversity. The diversity index is mainly determined by the number of different technologies used per subsystems. Although the diversity index is simple enough to be applied in the practical design process, the actual coupling extent between redundant components can't be quantified accurately. Therefore, this diversity index can't describe diversity precisely.

Many authors find it useful to split CCF causes into root causes and coupling factors. A root cause (RC) is the basic reason why components fail (e.g., a harsh environment), while a coupling factor (CF) is a characteristic of a group of components or piece-parts that identifies them as susceptible to the same causal mechanisms of failure (e.g., similarity in design, location, environment, mission, operation, maintenance, and test procedures). Many work [8] [9] [12] has been done involving the RC classification and related data collection recently. As CCF event data collected increased, research of CCF based on RC and CF has prospective advantages. Therefore, CCF analysis is performed from RC and CF point of view in this paper. Cause-Effect Logic Diagram (CELD) based on RC and CF is utilized to illustrate the nature of the design diversity to enhance system reliability and then a novel method is proposed to assess diverse redundancy system reliability. The key idea of the novel method is to classify the root causes into (sub-)categories and then assess the corresponding CFs between redundant components respectively based characteristics of diversity. Further, a novel CCF model is proposed to describe the relationship between CCF Probability and diversity. Finally, aiming at the CCF induced by external environment stress an example is given to illustrate the usage of the novel method.

This paper is structured as follows. In section II, a brief introduction to the concept and models of CCF is given. In section III, the nature analysis of design diversity to enhance system reliability is given and then a novel method to assess diverse redundant system reliability is proposed. In section IV, aiming at the CCF induced by external environment stress an example is given to illustrate the usage of the novel method. Finally, section V concludes the paper.

II CCF MODELS AND ANALYSIS

CCF has been defined as "dependent failures that defeat the redundancy or diversity employed to improve the reliability of systems"[10] and it is a serious threat to redundant systems reliability and may lead to simultaneous failures of redundant components and safety barriers. It is therefore important to quantify and model CCF in reliability and risk assessments. Many models have been proposed for the evaluation of CCF. The commonly used CCF models can be classified as shock vs. non-shock. The Binomial Failure Rate (BFR) model [13] which assumes that the system is subject to a common cause "shock" at a certain rate is a classical shock model. While, the most general of the commonly used non-shock CCF model is the Basic Parameter Model. All the other non-shock models, such as the Beta-Factor, the Multiple Greek Letter (MGL) model [14], and the Alpha Factor model [15], can be characterized as reparameterizations of the Basic Parameter model. CCF can appear due to external (such as EMI, power-supply disturbances, and radiation) or internal causes. Design mistakes also constitute an important source of CCF.

Design diversity has long been used to protect redundant systems against CCF. The basic idea is that, with different implementations, CCF will probably cause different error effects. For example, chances of identical design errors may be minimized if two different groups of designers are asked to independently design a hardware block or a software module. A power supply dip may have different effects on two different hardware implementations of the same logic function.

However, all CCF models mentioned above can't be used to assess the diverse redundant systems. As far as non-shock CCF models are concerned, they are built based on the symmetry assumption which said that "the probability of failure of any given basic event within a common cause component group depends only on the number and not on the specific components in that basic event." The symmetry assumption neglects the factor of diversity in the system. While the shock model also assume that all the components in the system are identical. Therefore, it is also not appropriate to assess diverse redundant system.

III A NOVEL METHOD FOR RELIABILITY ASSESSMENT OF DIVERSE REDUNDANCY SYSTEM

A. The nature analysis of design diversity to enhance system reliability

According to [11], a common cause event can be thought of as a combination of three key elements:

- Root Cause (RC): An event or mechanism to which the change in the state of a component can be attributed. The root cause is the basic reason why components fail.
- Coupling Factor (CF): A mechanism or factor that create the condition for multiple components to be affected by the same root cause.
- Component State: Component state defines the component status in regard to the function it is intended to provide. States of interest in common cause analysis are failed, degraded or incipient.

The design diversity is intended to decrease the coupling factor between redundant components and thus decrease the system CCF probability. Cause-Effect Logic Diagram (CELD) is utilized in this paper to illustrate the nature of the design diversity to enhance system reliability. As shown in Fig. 1, when the system is composed of two identical components, a RC is shared between the two redundant components via a CF and thus both of components failed due to CCF. In this case the coupling between the two components is strong. When the design diversity is applied in the system, namely, a different component is imported, the expected effect is shown in Fig. 2: The CCF causes different error effects on the two different components and the coupling between the two components becomes weak. The ideality effect of the design diversity is shown in Fig. 3, where the two components are affected by a RC independently and the coupling between the two components is decreased to zero.

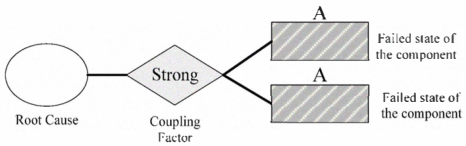

Fig. 1. Both identical redundant components failed due to CCF.

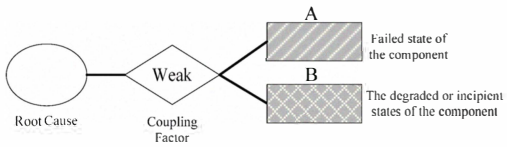

Fig. 2. CCF causes different error effects on the different implementations.

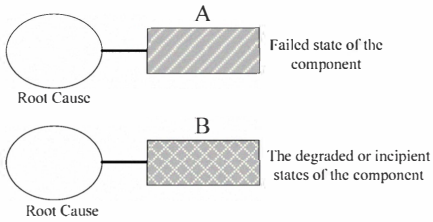

Fig. 3. Two different components are affected by a RC independently.

B. Why the diverse redundancy system is difficult to assess?

While there is clear evidence that diversity can bring benefits in a redundant systems, the benefits are extremely difficult to quantify in the practical system design process. The reasons can be illustrated from the RC and CF point of view.

In practice, CCFs usually result from more than one RC. As shown in Fig. 4, RCs are grouped into 3 classical categories, which are then subdivided to provide a means of recording more detailed information when available. The explanations of each category are as follows.

- Design/Construction/Manufacture Inadequacy. Encompasses actions and decisions taken during

design, manufacture, or installation of components both before and after the plant is operational.

- External Environment. Represents causes related to a harsh external environment that is not within component design specifications. Specific mechanisms include electromagnetic interference, fire/ smoke, impact loads, moisture (sprays, floods, etc.), radiation, abnormally high or low temperature, and acts of nature.
- Operations/Human Error (Plant Staff Error).Represents causes related to errors of omission and commission on the part of plant staff.

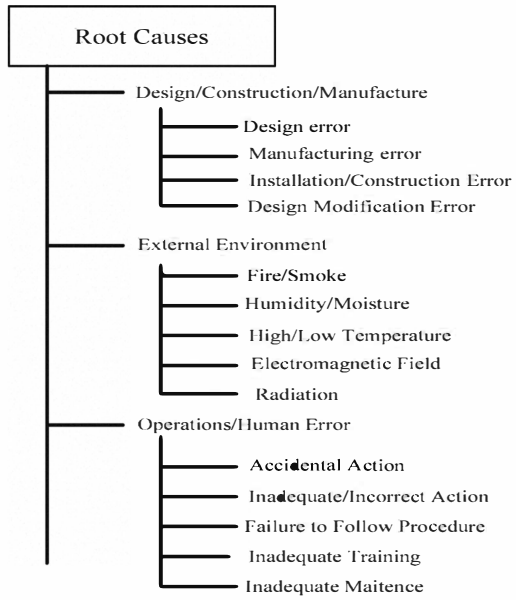

Fig. 4. Categories for Root Causes.

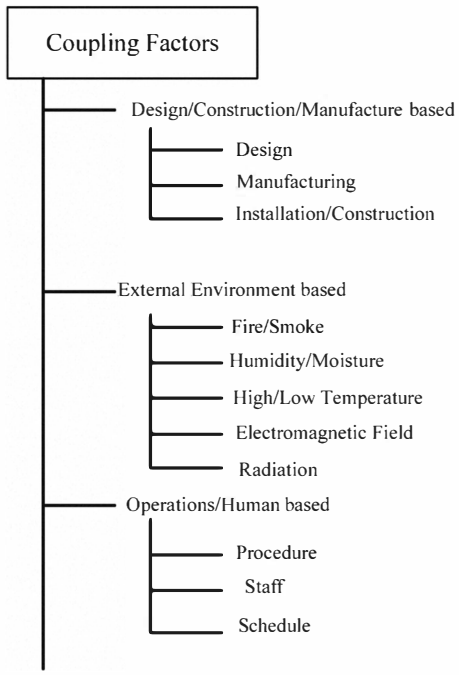

Fig. 5. Categories for Coupling Factors.

Accordingly, each RC category corresponds to a specific CF category. Thus categories for CFs can be built as shown in Fig. 5. The explanations of each category are as follows.

- Design/Construction/Manufacture based. Refers to the same design staff, manufacturing staff, quality control procedure, manufacturing method, construction/installation staff, and construction/installation procedure.
- External Environment based. Refers to all redundant systems/components exposed to the same external environmental stresses.
- Operations/Human based. Refers to the cases when operation of all (functionally or physically) identical components is governed by the same operating procedures.

When design diversity is applied in redundant systems, more than one CFs change simultaneously. For example, chances of identical design errors may be minimized if two different groups of designers are asked to independently design a hardware block or a software module. At the same time, the different implementations will have different environmental strength, such as temperature strength, humid strength, and so on. Therefore, the CFs of the two categories, namely Design/Construction/Manufacture based and External Environment based, change simultaneously. It is the reason why diverse redundancy system is difficult to assess.

C. A novel method to assess diverse redundancy system

Since diversity affects more than one CFs simultaneously, it is advisable to classify the RCs into (sub-)categories and then assess the corresponding CFs between redundant components respectively based characteristics of diversity. In practice, RCs can be classified into categories, each of which can be further divided into sub categories, as long as failure reports can provide enough information. The relationship between CCF Probability and diversity can be researched through the related CFs. Consequently, a novel CCF model is proposed as follows.

$$prob.of\ CCF = \sum_{i=1}^{n} (prob.\ of\ RC_i) \times CF_i \qquad (3.1)$$

Where,

n is the number of root cause (sub-)categories which are considered in CCF analysis.

RC_i represents a specific (sub-)category of RC, such as Design/Construction/Manufacture, Humidity/Moisture, High/Low Temperature, and so on.

CF_i represents the corresponding CF of the RC_i.

IV AN EXAMPLE: CCF ANALYSIS USING THE NOVEL METHOD PROPOSED

A. Assumptions

Firstly, assume that the system to be analyzed is composed of two redundant components. The fail mode is defined as follows: the system failed only when both of the redundant components failed.

CCF analysis is performed respectively in the following two situations:

- S1: System composed of two identical redundant components (as shown in Fig. 6).
- S2: System composed of two diverse redundant components (as shown in Fig. 7).

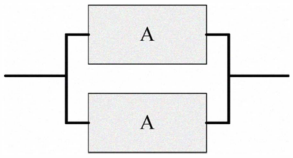

Fig. 6. System composed of two identical redundancy components.

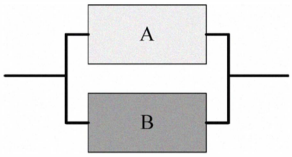

Fig. 7. System composed of two diverse redundancy components.

As far as RC categories are concerned, only External Environment category is considered here. In detail, two specific sub-categories, namely Humidity/Moisture (HUM) and High/Low Temperature (TEM), are taken into account. Therefore, the equation (3.1) becomes,

$$prob.\,of\,CCF = (prob.\,of\,RC_1)\times CF_1 + (prob.of\,RC_2)\times CF_2 \quad (4.1)$$

Where,

RC_1 and CF_1 correspond to the HUM sub category,
RC_2 and CF_2 correspond to the TEM sub category.

TABLE I
DESCRIPTION OF NAMES OF STOCHASTIC VARIABLES

stochastic variable name	Description
X	Environmental HUM stress
Y	Environmental TEM Stress
X_A	Component A HUM Strength
X_B	Component B HUM Strength
Y_A	Component A TEM Strength
Y_B	Component B TEM Strength

TABLE II
MEANS AND VARIANCES OF STOCHASTIC VARIABLES.

	(μ,σ) of X_A	(μ,σ) of X_B	(μ,σ) of Y_A	(μ,σ) of Y_B	(μ,σ) of X	(μ,σ) of Y
Case (1)	+2.3, 2	+3↑, 1.8	+3.5, 2	4.1↑, 1.7	0,1	+1, 2
Case (2)		+3↑, 1.8		2.6↓, 3		
Case (3)		+1.2↓, 4		2.6↓, 3		

Probability values are determined based on the stress-strength failure model in the example. Assume that all the stochastic variables representing the Environmental HUM stress, the Environmental TEM stress, Component HUM strength and Component TEM strength conform to Normal distribution. Obviously, not all stochastic variables of stress and strength will exhibit such statistical characteristics, but it is likely that many types of variables of stress and strength will. Further, note that the method proposed in this paper does not depend on variables of stress and strength being Normal distribution. Descriptions of names of stochastic variables are listed in Table I and their Mean and Variance parameters are shown in Table II.

Since all kinds of performance parameters of component B may be different from those of component A, to research the effects of diversity in a more common manner, three classical cases are discussed in S2. As shown in Table II:

- Case (1): both of the means of B HUM Strength and B TEM Strength are greater than those of A.
- Case (2): mean of B HUM Strength is greater than that of A while mean of B TEM Strength is less than that of A.
- Case (3): both of means of B HUM Strength and B TEM Strength are less than those of A.

B. Calculation of RC Probability

Firstly, specify the Harsh Environment HUM critical point: Xha = 0.53. When the Environmental HUM Stress value exceeds Xha, consider that harsh HUM environment happens. Consequently, Probability of RC_1 is defined as follows.

$$prob.\,of\,RC_1 = P(X > Xha) \quad (4.2)$$

Similarly, specify the Harsh Environment TEM critical point: Yha = 1.6. Consequently,

$$prob.\,of\,RC_2 = P(Y > Yha) \quad (4.3)$$

Since the two redundant components are exposed to the same environment, it is reasonable to assume that Probability of RC_1 and RC_2 are constant in S1 and S2.

C. Calculation of CF

According to the stress-strength failure model, failures occur when environmental stress is greater than component strength. Further, a CCF occurs in redundant systems when the environmental stress is greater than the strength of two or more components. Therefore, define CF_i corresponding to RC_i as follows.

$$CF_i = \prod_{j=1}^{n} P(CS_j < CP_i) \quad (4.4)$$

Where,

CS_j refers to the jth Component strength,

CP_i refers to the critical point of harsh environment which corresponds to RC_i .

n refers to the number of the redundant components in the system.

D. Calculation of CCF probability and analysis.

According to the Standard Normal Distribution Function Table and Probability Theory, the Probability of RC_1 and RC_2, CF_1, CF_2 and the system CCF Probability can be achieved in S1 and S2 based on equation (4.1-4.4). The final results of system CCF Probability in S1 and S2 are shown in Table III.

TABLE III
CCF PROBABILITY

	CCF Prob. (S1)	CCF Prob. (S2)
Case (1)	0.02189	0.0094↓
Case (2)		0.029↑
Case (3)		0.0486↑

As shown in Table III, the CCF probability may increase or decrease when design diversity is applied. For example, in Case (2) of S2, although the HUM performance of B is better than A, while the TEM performance is poorer than A. Due to the TEM factor is the dominated one compared to the HUM factor ($RC_2 > RC_1$), this leads to CCF probability increases in the end. Therefore, the CCF probability is determined by more than one factor when design diversity is applied. The important thing is to determine which factor is the dominated one in the practical conditions.

V CONCLUSIONS

Recently, RC and CF classification and related data collection have been performing in related domains, such as nuclear energy, spacecraft, and so on. Therefore, the method proposed has good applying prospective in the future. As more CCF event information is collected, it is possible to quantify the effects of diversity based on the method proposed.

ACKNOWLEDGMENT

This work is supported by the Natural Science Foundation of China under contract 61004068.

REFERENCES

[1] Jin Jiang, "Why does one need fault-tolerant control systems anyway?", 2010 Conference on Control and Fault Tolerant Systems, Nice, France, October 6-8, 2010

[2] Peter J. Rutledge, Ali Mosleh, " Dependent-failures in Spacecraft: Root Causes, Coupling Factors, Defenses, and Design Implications", 1995 PROCEEDINGS Annual RELIABILITY and MAINTAINABILITY Symposium.

[3] International Electrotechnical Commission, IEC 61511: Functional safety—safety instrumented systems for the process industry. Part 1: Framework, definitions, system, hardware and software requirements, 2003.

[4] I. M. Jacobs, "The common mode failure study discipline," IEEE Trans. Nucl. Sci., vol. 17, no. 1, pp. 594–598, Feb. 1970.

[5] J. V. Bukowski and W. M. Goble, "Verifying common-cause reduction rules for fault tolerant systems via simulation using a stress-strength failure model," ISA Transactions, 183-190, 2001.

[6] S. Mitra, N.R. Saxena, and E.J. McCluskey, "A Design Diversity Metric and Analysis of Redundant Systems," IEEE Transactions on Computers, vol. 51, no. 5, pp. 498-510, May 2002.

[7] A.C.Torres-Echeverria, S.Martorell, H.A.Thompson, "Design optimization of a safety-instrumented system based on RAMS+C addressing IEC61508 requirements and diverse redundancy," Reliability Engineering and System Safety, pp. 162–179, 2009.

[8] Peter J.Rutledge and Ali Mosleh, "Dependent-Failure in Spacecraft: Root Causes, Coupling Factors,Defenses, and Design Implication", 1995 Proceedings Annual Reliability and Maintainability Symposium.

[9] Idaho National Laboratory, "Common-Cause Failure Database and Analysis System: Event Data Collection, Classification, and Coding", NUREG/CR-6268, Rev.1.

[10] A.Mosleh,Guest Editorial, In:Reliability Engineering and System Safety-Special Issue on Dependent Failure Analysis,Vol.34,Elsevier Science Publishers,Ltd.,Essex,UK,1991.

[11] A. Mosleh, "Interaction Between Model and Data in Common Cause Failure Analysis", http://www.iasmirt.org/iasmirt-3/SMiRT10/DC_250567, August 1989.

[12] NEA (2004). International common-cause failure data exchange. ICDE general coding guideline – technical note. Number NEA/CSNI/R(2004)4. Nuclear Energy Agency.

[13] Corwin L.Atwood, Dana L.Kelly, "The binomial failure rate common-cause model with WinBUGS," Reliability Engineering and System Safety, pp. 990–999, 2009.

[14] A. Mosleh, "Common cause failures: An analysis methodology and examples,"Reliability Engineering and System Safety, vol. 34, no. 3, pp.249–292, 1991.

[15] Jussi K. Vaurio, "Consistent mapping of common cause failure rates and alpha factors," Reliability Engineering and System Safety, pp. 628–645, 2007.