Probabilistic Common Cause Failure Modeling after the Introduction of Defense Mechanisms

Xiaoyu Zheng, Akira Yamaguchi, Takashi Takata
Osaka University
2-1 Yamada-oka, Suita, Osaka, 5650871, Japan
zheng_x@qe.see.eng.osaka-u.ac.jp, yamaguchi@see.eng.osaka-u.ac.jp,
takata_t@see.eng.osaka-u.ac.jp

ABSTRACT

Causal inference is able to assess common cause failure (CCF) events from the viewpoint of causes' risk significances. α-decomposition method is a methodology for probabilistic CCF analysis in which classical α-factor model and causal inference are integrated to conduct a numerical estimation of all causes' risk significances. In this paper, authors focus on the predictive distributions of parameters for the modified nuclear safety system after that a defense mechanism is introduced. Firstly, authors review α-decomposition method, in which a Hybrid Bayesian Network is applied to reveal the relationship between all potential causes and possible failure, besides that, the procedure of Bayesian computation is illustrated which can combine together both prior distributions and the available database. Secondly, when a defense mechanism is developed using protection against a potential common cause, the failure types and failure probability distributions of components will be changed. Usually, there is no exact matching database for newly modified system which means that freqentist probability is far too inaccurate. To avoid considering such question, past work has assumed that all components in system are identical. Based on α-decomposition method, authors propose a procedure to solve the probabilistic modeling of such heterogeneous systems as well as various causes. An example with new defense mechanisms and one hypothetical database are demonstrated, and then posterior predictive distributions of parameters are calculated according to Bayesian inference by Markov Chain Monte Carlo algorithm. This research has proved that α-decomposition method has the potential to do the numerical causality analysis for CCF events and especially for the modified system with introduced defense mechanisms.

KEYWORDS

Common cause failure, α-decomposition method, Bayesian theory, Defense mechanism, Probabilistic safety assessment

1. INTRODUCTION

In the probabilistic safety assessment (PSA) performed by nuclear safety analysts, the identification and quantification of common cause failure (CCF) are essential parts in analyzing the probability distributions of system failures. In order to model systems more logically and reducing uncertainties in the integrated distribution, it is necessary to combine the cause-level (or subcomponent-level) with system fault tree analysis, which is almost implicit in the quantitative basic parameter models (BPM) [1,2] and is located below the component-level. Obviously, the root cause is the basic reason why CCFs occur in system, and the introduction of defense mechanisms against root causes or coupling factors can prevent the recurrence [3]. The defense mechanisms for the CCF system are operational,

maintenance, and design measures taken to defend CCF root causes or coupling factors and then to reduce CCF events. The condition or mechanism through which failures of multiple components are coupled is termed as coupling factors. The widely used BPM has simplified target systems as identical components and treat CCF probability as one constant fraction of global failure probability. However, a CCF event is actually a plant-specific topic, as a result of that the detailed design of systems vary from one plant to another plant, as well as coupling factors and defense mechanisms. Thus, the applying of plant-generic data will inevitably result in the introduction of uncertainties. Lack of CCF data is a permanently unsolved problem which means there is limited pant-specific data available, though a great progress has been made with the publication of CCF databases and tools developed by United States Nuclear Regulatory Commission (U.S. NRC) and the Idaho National Laboratory (INL) [4]. Therefore, it must be discussed the following topics to obtain more explicit analysis: (1) how to combine information from cause-level with system fault tree analysis, (2) how to reasonably utilize plant-specific data and plant-generic data when heterogeneous systems are modified for the introduction of new defense mechanisms.

α-factor model is one of most widely used BPM for CCF, and the value of α_k factor is the fraction of the total probability of failure events which means the occurrence of involving the failure of k components in a system of m components due to a common cause. Based on event insights of CCF [5], global α-factors are affected by all potential causes and coupling factors. Potential causes have different abilities to trigger failures, which might be independent failures, partial failures or global failures. Therefore, the global α-factors are lumped parameters which can be decomposed according to the different risk significance of different causes. α-decomposition method applies hybrid Bayesian network (HBN) to integrate the analysis of system-level, component-level and cause-level together and then to get more reasonable estimates of CCF parameters. As distinguished from BPM by point estimates, the probabilistic reasoning in α-decomposition method applies Bayesian probability which can use empirical or expert opinions as prior distributions avoiding the problem caused by the shortage of data, and can allow the integration of probabilistic distributions from cause-level to component-level and finally to system-level. Because of the causal inference in α-decomposition method, it is realizable to combine different data sources. Especially, when a system is modified in order to defending CCF event and there is no exact failure data for such a new system, α-decomposition method is useful to obtain parameters' posterior distribution with taking into consideration of updated risk significance of potential causes.

2. α-DECOMPOSITION METHOD WITH HYBRID BAYESIAN NETWORK

2.1. α-factor Model

The movement from single-parameter model to multi-parameter model is actually the decomposition from single lumped parameter to multiple lumped parameters in component-level. α-factor model is an event-based multi-parameter model, and in other words, α-factor model is component failure based and more directly related to the observable number of events. Due to the lack of space in this paper, the simplest α-factor model is briefly reviewed and more specific introduction can be obtained in NUREG/CR-4780 [1] and NUREG/CR-5458 [2]. Let us consider a system of three components A, B, and C, with a two-out-of-three success logic, so the common-cause component group (CCCG) is A, B, and C. There, a group of components identified in the process of CCF analysis is called as common cause component group. The failure probability of component A is decomposed as:

$$P(A_t) = P(A_I) + P(C_{AB}) + P(C_{AC}) + P(C_{ABC}) \quad (1)$$

Here, A_t: all failures of component; A_I: failures of component A from independent causes; C_{AB}: failures of components A and B from common causes; C_{AC}: failures of components A and C from common causes; C_{ABC}: failures of components A, B and C from common causes; $P(X)$: probability of event X. And assume that:

$$\begin{gathered} P(A_I) = P(B_I) = P(C_I) = Q_1 \\ P(C_{AB}) = P(C_{AC}) = P(C_{BC}) = Q_2 \\ P(C_{ABC}) = Q_3 \end{gathered} \quad (2)$$

And the component A failure probability is

$$Q_t = Q_1 + 2Q_2 + Q_3 \quad (3)$$

In this paper, the system is assumed as staggered testing scheme. The definition of α-factors (staggered testing scheme):

$$\alpha_1 = \frac{Q_1}{Q_t};\ \alpha_2 = \frac{2Q_2}{Q_t};\ \alpha_3 = \frac{Q_3}{Q_t} \quad (4)$$

2.2. α-decomposition Method for CCF Analysis

CCF events are actually sum contributions from specific root causes and coupling factors. α-factor model provides an approach to consider CCF effect among components and then to calculate the system failure probability. Qualitative analysis of CCF identifies the CCF occurring mechanism and root causes explicitly, therefore how to numerically utilize such information with probabilistic safety analysis is an important topic. Every root cause has particular ability to trigger independent failures or dependent failures, so it provides a hint to numerically model the ability with a single parameter. In this paper, the α-factors in components' level are named as global α-factors, and after decomposition, α-factors in causes' level are named as decomposed α-factors [6], which represent the CCF triggering ability of causes.

Definition 1 (α-decomposition):
Decompose or factorize the global α-factor from standard CCF analysis model (α-factor model) according to different CCF triggering significance of every cause, by applying the Bayesian network to represent the relationship of global α-factors and decomposed α-factors.

For instance, as one of examples depicted in NUREG/CR-6819 [5], 36% of all CCFs are caused by design, etc., and 7.3% by external environment. At the same time, the same kind of causes with different levels of magnitude will have different abilities to cause a CCF. According to the research of seismic probabilistic safety assessment (SPSA), in the low peak ground acceleration (PGA) range, the β-factor is quite small, but in the high PGA range the β-factor is quite large [7]. In other words, the reasons of more CCFs being caused by design are design error frequently happen or design error is good at CCF triggering. Obviously, when two kinds of seismic happen, the higher PGA tends to generate CCF much easier than the lower PGA. One another important failure-triggering characteristic of a cause is that when a cause happens, it might generate a CCF of multiple components or it might generate only an independent failure. In α-factor model the independent part is expressed as α_1 and multiple

failures are expressed as $\alpha_2, \alpha_3, \ldots, \alpha_n$. For example, in the analysis of SPSA, even the common cause seismic event sometimes causes only independent failure, so the β is always less than 1, and also in the analysis of design error, it is obvious that also not all of design error will result in CCF. Thus, we could judge that there are two possible characteristics of causes that lead to different fraction of CCF occurring. One is the CCF-triggering ability of a kind of causes, and the other is the occurring frequency of each cause. Therefore, it is reasonable to decompose the α-factor and find the most hazardous causes which happen frequently with great CCF triggering ability.

The global α-factor could be treated as a joint distribution. Traditionally, it is represented by a joint density function, a curve or even by a summary of distribution (percentiles, mean, and median, etc.). When the joint distribution is represented by a set of random variables $\mathcal{X} = \{X_1, \cdots, X_n\}$, the representation becomes very unmanageable. Bayesian network is a declarative representation that could provide the duality of independencies and factorization as a directed graph. Bayesian network has many advantages. Firstly, the tractable form of this framework allows analysts to understand and evaluate objects' relationships easily, and then provide an accurate reflection of the joint distribution. Secondly, with consideration of logic structure, this network also allows the distribution to be used effectively for inference. Thirdly, the network can learn from new data and provide a good approximation based on prior distribution and new evidence. These three characteristics are named as Representation, Inference, and Learning, which could conduct an intelligent analysis of CCF. In this paper, we apply hybrid Bayesian network (HBN) to express logical relationships between component failures, global α-factors and decomposed α-factors. A hybrid network means to use a combination of two or more topologies, and here the HBN is a combination of Bayesian network and Fault Tree (FT). Let's consider a system of three components A, B, and C. In standard α-factor model, all components of a system are assumed identically, but for α-decomposition method, it is also available for components that are partially identical. For the simplest consideration, we assume three originally identical components, A, B, and C and three potential causes, C_1, C_2, and C_3 that will possibly lead to the component failures (as shown in Fig.1).

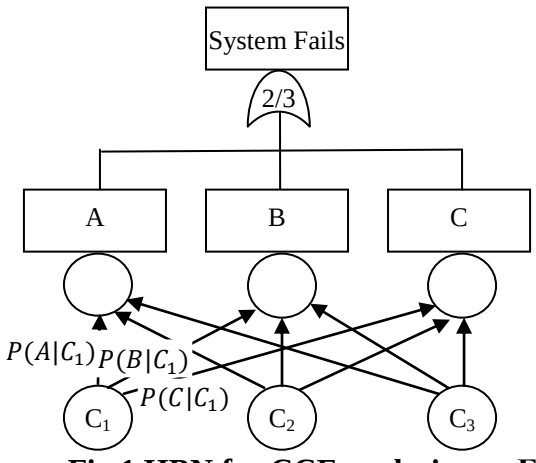

Fig.1 HBN for CCF analysis

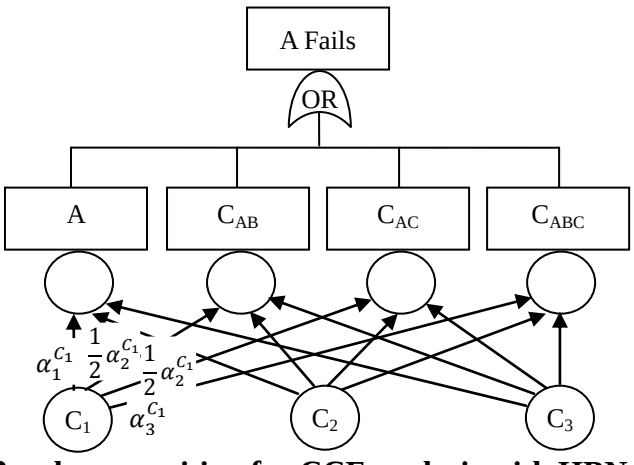

Fig.2 α-decomposition for CCF analysis with HBN

The conditional probabilities of component failure and system failure are expressed in Fig.1. Take component A as an example:

$$P(A) = P(A|C_1)P(C_1) + P(A|C_2)P(C_2) + P(A|C_3)P(C_3) \quad (5)$$

The process of α-decomposition method is illustrated in Fig.2, and the mechanism of Cause i is operated by generating independent A failure; A and B failures; A and C failures; A, B and C failures:

$$P(A|C_i) = P(A_I|C_i) + P(AB|C_i) + P(AC|C_i) + P(ABC|C_i) \quad (6)$$

Both sides of equation are divided by $P(A|C_i)$:

$$1 = \alpha_1^{C_i} + \alpha_2^{C_i} + \alpha_3^{C_i} \quad (7)$$

Here, $\alpha_1^{C_i} = \frac{P(A_I|C_i)}{P(A|C_i)}$; $\alpha_2^{C_i} = \frac{P(AB|C_i)}{P(A|C_i)} + \frac{P(AC|C_i)}{P(A|C_i)}$; $\alpha_3^{C_i} = \frac{P(ABC|C_i)}{P(A|C_i)}$. On the purpose of distinguishing the difference between two kinds of α-factors, in this paper, we named the $\alpha_j\ (j = 1,2,3)$ as global α-factors, and named the $\alpha_j^{C_i}\ (i,j = 1,2,3)$ as causes' α-factors. The independent failure of component is affected by Cause 1, Cause 2 and Cause 3, and according to Fig.2, the relationship is expressed as:

$$P(A_I) = P(A_I|C_1)P(C_1) + P(A_I|C_2)P(C_2) + P(A_I|C_3)P(C_3) \quad (8)$$

Replace the independent part of probability with $\alpha_1^{C_i}$ elements as follows,

$$P(A_I) = \alpha_1^{C_1}P(A|C_1)P(C_1) + \alpha_1^{C_2}P(A|C_2)P(C_2) + \alpha_1^{C_3}P(A|C_3)P(C_3) \quad (9)$$

Both sides of equation are divided by $P(A)$ and because $\frac{P(A_I)}{P(A)} = \alpha_1$, so we get as follows,

$$\alpha_1 = \alpha_1^{C_1}\frac{P(A|C_1)P(C_1)}{P(A)} + \alpha_1^{C_2}\frac{P(A|C_2)P(C_2)}{P(A)} + \alpha_1^{C_3}\frac{P(A|C_3)P(C_3)}{P(A)} \quad (10)$$

Extrapolate the α_1 to any α_j, and we get very simple form of α_j-decomposition; and deduced from Fig.1, it is known that failure of A is generated by three parts, and we notate these three parts as fractions or rates;

$$\alpha_j = \alpha_j^{C_1}r_1 + \alpha_j^{C_2}r_2 + \alpha_j^{C_3}r_3;\ (j = 1,2,3) \quad (11)$$

$$r_i = \frac{P(A|C_i)P(C_i)}{P(A)} = P(C_i|A);\ (i = 1,2,3.\ and\ \sum_{i=1}^{3} r_i = 1.) \quad (12)$$

Here, $\alpha_j\ (j = 1,2,3)$: global α-factors for j components failure; $\alpha_j^{C_i}\ (i,j = 1,2,3)$: decomposed α-factors for j components faiure as a result of Cause i; $r_i\ (i = 1,2,3)$: the occurrence fraction for Cause i. Here, the $\alpha_j^{C_i}, r_i (i,j = 1,2,3)$ have practical engineering meanings: The $\alpha_j^{C_i}$means the ability of Cause i to lead to the j components failure; the r_i means that among all failures, totally there are $r_i \times 100\%$ failures generated by Cause i. In other words, r_i is the occurrence fraction over the occurrence of all effective causes. (Effective cause means the cause really triggers a failure whether independent or dependent and oppositely, if a cause happens but no failure is generated, it is not an effective cause.) For example, if Cause 1 happens much more frequently than other causes, the global α_j will tend

to be $\alpha_j^{C_1}$; on the other side, if Cause 2 happens rarely with low $\alpha_j^{C_2}$, it means that risk-significance of Cause 2 is negligible.

3. SYSTEM ANALYSIS AFTER INTRODUCTION OF DEFENSE MECHANISMS

3.1. System Modeling Involving Defense Mechanisms

According to α-decomposition method, it is realizable to analyze asymmetric systems, as a result of that the decomposed α-factors mean the risk significance of a certain cause to a single component. A coupling factor is a way to explain how a root cause propagates to involve equipment items, which is defined as the condition or mechanism through which failures of multiple components are coupled, e.g. quality-based couplings, design-based couplings and environment-based couplings, etc.. It is an environment-based coupling that redundant equipments located in identical external environment are more probable of higher chance of simultaneous failures, and for example, a water injection system leak on an inlet pipe caused the AFW pump motors in the same location to be sprayed with the water. Traditionally, there are two strategies to defend against a CCF events: one is to defend against the failure root cause; and the other is to defend against the CCF coupling factor. Because the defense against a root cause contains too many subjects of knowledge, here we only discuss about the defense strategy using protection against a coupling factor. When a defense strategy is developed using protection against a coupling factor, the number of failures may not be decreased, but the severity of CCF would be reduced, such as global CCF events would become partial CCF events and partial CCF events would become independent failures. In three-cause-three-component system, one defense mechanism against Cause 1's coupling factor is assumed as shown in Fig.3, which protects component from root Cause 1 but introduces one more independent root cause (Cause 1'). It has practical engineering meanings, and let us take the environment-based coupling factor as an example: the physical separation of Component C from Component A & B is a defense strategy to reduce the chance of simultaneous failure of equipments due to some environmental effects. The Cause 1 is assumed as one cause which happens in the location of Component A & B, and after the introduction of physical separation of Component C, which is not affected by Cause 1 any longer. On the other side, Component C might be affected by one new root cause (C_1') which exists in the new location originally. All the logical CCF modeling of system failure is shown in Fig.3 with hybrid Bayesian network (HBN), and symbols in red color are the modified parts in the system after the introduction of defense mechanisms.

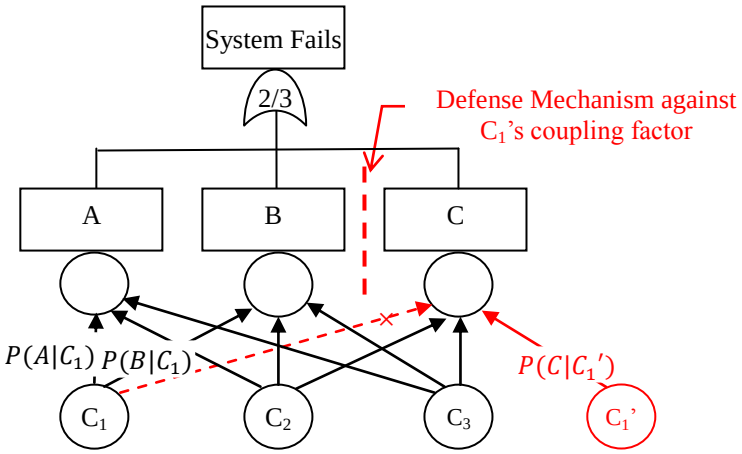

Fig.3 CCF system's modeling involving a defense mechanism against one coupling factor

3.2. α-decomposition Modeling Involving Defense Mechanisms

The introduction of defense mechanisms generates the asymmetry in the system, and as shown in Fig.3, the failure probability of Component A or B varies from Component C. It is because the Cause 1 does not affect Component C any longer, but maintain the affection on Component A & B. Thus, it is necessary to analyze CCF probability distributions of Component A (or Component B) and Component C to numerically evaluate the defense mechanism. In the following part, the analysis of Component A and C will be conducted respectively.

3.2.1. Degradation of CCF involving Component A

The defense strategy using protection system against Cause 1's coupling factor results in some of CCF events unable to happen, and specifically the CCF of Component A and C produced by Cause 1 and the global CCF of Component A, B, and C produced by Cause 1 are impossible to happen. Fig.4 shows the causal inference for Component A's failure, and the red dashed arrows are causal relationships interrupted by the defense strategy, which in fact means that the basic events C_{AC} and C_{ABC} will no longer occur. Let us consider the transformation of CCF events qualitatively and take the environmental coupling factor and physical separation strategy as an example once again. Because Cause 1 is a local cause only which occurs only in the location of Component A and B, when the physical separation strategy has been applied, the local Cause 1 only generate the failure events of Component A and B. The assumed C_{AC} and C_{ABC} (generated by Cause 1) will be transformed to independent failure A_I and C_{AB} (generated by Cause 1) in the new system with the introduced defense mechanism. Therefore, such a defense mechanism is effective to degrade the CCF level, which means to reduce the number of components affected so as to reduce the severity of CCF events. Based on conditional probability, this degradation could be expressed as

$$P(C_{AC}|C_1) \rightarrow P(A_I{}^*|C_1);\ P(C_{ABC}|C_1) \rightarrow P(C_{AB}{}^*|C_1) \tag{13}$$

There, in order to distinguish with the original failure types, the new incoming independent failure and CCF for Component A and B are noted as $A_I{}^*$ and $C_{AB}{}^*$, respectively. Therefore, deducing from equation (6) and (13), the cutset for A failure due to Cause 1 is

$$P(A|C_1) = P(A_I|C_1) + P(C_{AB}|C_1) + P(A_I{}^*|C_1) + P(C_{AB}{}^*|C_1) \tag{14}$$

According to the definition of decomposed α-factors, the new parameters are expressed as

$$\begin{aligned} updated\ \alpha_1^{C_1} &= \alpha_1^{C_1} + \alpha_1^{C_1{}^*} = \alpha_1^{C_1} + \frac{1}{2}\alpha_2^{C_1} \\ updated\ \alpha_2^{C_1} &= \alpha_2^{C_1} + \alpha_2^{C_1{}^*} - \alpha_1^{C_1{}^*} = \frac{1}{2}\alpha_2^{C_1} + \alpha_3^{C_1} \\ updated\ \alpha_3^{C_1} &= \alpha_3^{C_1} - \alpha_2^{C_1{}^*} = 0 \end{aligned} \tag{15}$$

It can be observed from equations (15) that the global CCF events produced by Cause 1 has been reduced to 0, and the independent failures has been increased. The variation of partial CCF events depends on which parameter is larger $\alpha_2^{C_1{}^*}$ or $\alpha_1^{C_1{}^*}$.

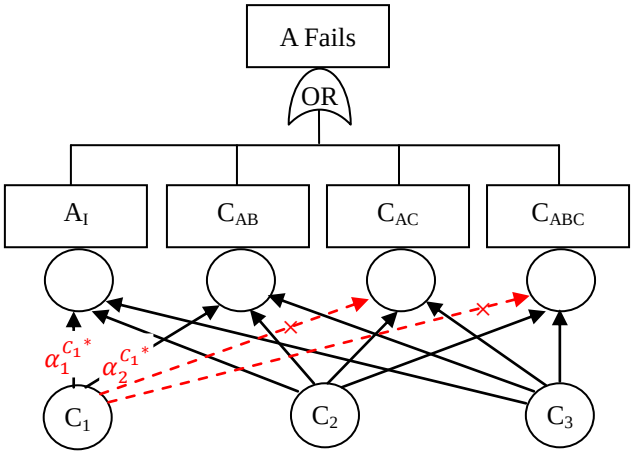

Fig.4 Causal inference for Component A after the introduction of defense mechanisms

3.2.2. Degradation of CCF involving Component C

Similar to the discussion of Component A, let us discuss about the degradation of CCF severity involving Component C. Fig.5 depicts the causal relationships after the introduction of defense mechanisms, where red dashed arrows are causal relationships interpreted and the red lined arrow is the new causal relationship introduced by the new location of Component C. Therefore, all the CCF events produced by Cause 1 involving Component C are transformed to independent failure A_I or B_I, and CCF events C_{AB}, besides one new kind of independent failure events will be generated by the upcoming cause C_1'. Based on conditional probability, the degradation could be expressed as

$$P(C_I|C_1) \to 0$$
$$P(C_{CA}|C_1) \to P(A_I|C_1);\ P(C_{CB}|C_1) \to P(B_I|C_1);\ P(C_{CAB}|C_1) \to P(C_{AB}|C_1) \quad (16)$$

Therefore the new probability of C failures due to Cause C_1 is 0 and that due to Cause C_1' is

$$P(C|C_1') = P(C_I|C_1') \quad (17)$$

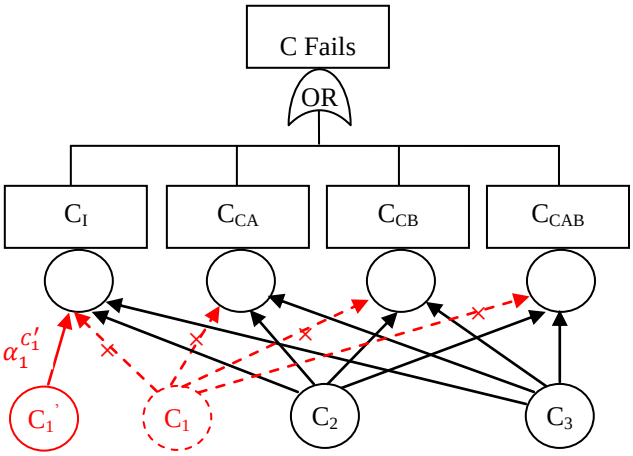

Fig.5 Causal inference for Component C after the introduction of a defense mechanism

According to the definition of decomposed α-factors, the new parameters are expressed as

$$updated\ \alpha_1^{C_1} = updated\ \alpha_2^{C_1} = updated\ \alpha_3^{C_1} = 0$$
$$updated\ \alpha_1^{C_1'} = 1;\ updated\ \alpha_2^{C_1'} = updated\ \alpha_3^{C_1'} = 0 \quad (18)$$

4. BAYESIAN INFERENCE FOR MODIFIED SYSTEM ANALYSIS

4.1. Stochastic Modeling and Bayesian Theorem

CCF events are actually plant-specific or even system-specific, so the shortage of enough data would be a major problem to conduct an explicit quantitative PSA analysis. Especially for some new system or modified system according to the improvement design, there is always no enough operational data, so it is inevitable to predict by combining different data source reasonably. As introduced in last section, the prediction for Component A requires the re-evaluation of system model; and the prediction for Component C requires the combination of other database to consider the affection of Cause C_1'. The development and implementation of Markov Chain Monte Carlo (MCMC) methods make the Bayesian statistics practically available to solve such complicated re-modeling problem and to predict data-missing problem. Based on the analysis of α-decomposition method, the relationship between global α-factors and decomposed α-factors is

$$\alpha_j = \alpha_j^{C_1} r_1 + \alpha_j^{C_2} r_2 + \alpha_j^{C_3} r_3, (j = 1,2,3) \quad (19)$$

This stochastic process consists of one response variable $\alpha_j (j = 1,2,3)$, three explanatory variables $r_i (i = 1,2,3)$ and three parameters $\alpha_j^{C_i} (i,j = 1,2,3)$. These three parameters are actually a linking mechanism between the response variable and explanatory variables. The interest lies on evaluating three parameters that represent risk significances of all causes.

$$\alpha_j | r_1, r_2, r_3 \sim \mathcal{D}(\theta) \quad (20)$$

Here, $\mathcal{D}(\theta)$ is a distribution with parameter vector θ, and the signal "~" means the stochastic form of global α-factor $\alpha_j (j = 1,2,3)$ given explanatory variables $r_i (i = 1,2,3)$. Bayesian theorem provides an expression for the conditional probability of decomposed α-factors given global α-factors and the rates of causes' occurrence, which is shown as

$$P\left(\alpha_j^{C_i} \middle| \boldsymbol{\alpha_j}, \boldsymbol{r}\right) = \frac{P\left(\boldsymbol{\alpha_j}, \boldsymbol{r} \middle| \alpha_j^{C_j}\right) P\left(\alpha_j^{C_j}\right)}{P(\boldsymbol{\alpha_j}, \boldsymbol{r})} \quad (21)$$

In equation (21), $P\left(\alpha_j^{C_i}\right)$ could be defined as the prior distribution of decomposed α-factors, and $P\left(\boldsymbol{\alpha_j}, \boldsymbol{r} \middle| \alpha_j^{C_i}\right)$ could be defined as the likelihood of parameters. Therefore, the posterior distribution could be written as

$$f\left(\alpha_j^{C_i} \middle| \boldsymbol{\alpha_j}, \boldsymbol{r}\right) = \frac{f\left(\boldsymbol{\alpha_j}, \boldsymbol{r} \middle| \alpha_j^{C_j}\right) f\left(\alpha_j^{C_j}\right)}{f(\boldsymbol{\alpha_j}, \boldsymbol{r})} \propto f\left(\boldsymbol{\alpha_j}, \boldsymbol{r} \middle| \alpha_j^{C_j}\right) f\left(\alpha_j^{C_j}\right) \quad (22)$$

Here, $\alpha_j^{C_i}$ is the decomposed α-factor due to Cause i involving j components; $\boldsymbol{\alpha_j}$ is the set

global α-factors for j components' CCF; $\boldsymbol{r}$ is the set of explanatory variables representing each cause's occurrence rate.

4.2. An Example for Modified System Analysis

The following example is proposed to explain how to do numerical estimation about the introduction of defense mechanisms with Bayesian inference with α-decomposition method. We would like to caution that all the CCF data used in this paper is for illustration only and not from real database, and the calculation of Bayesian inference is conducted by WinBUGS version 1.4.3 and R version 2.13.1. The hypothetical database is assumed in Table 1 with the occurrence rates of root causes for Component A and C after the introduction of defense mechanisms, as well as the recording global α-factors which are used to calculate the posterior distributions of decomposed α-factors.

Table 1. Hypothetical database for modified system analysis

System	Root causes' occurrence rate (A)			Root causes' occurrence rate (C)			Global α-factors (data before modification)		
	r_1	r_2	r_3	r_1'	r_2'	r_3'	α_1	α_2	α_3
1	16.00%	73.60%	10.40%	8.72%	80.00%	11.28%	9.21E-01	6.97E-02	8.90E-03
2	20.70%	21.80%	57.50%	11.54%	24.36%	64.10%	8.46E-01	9.94E-02	5.50E-02
3	43.90%	9.10%	47.00%	28.16%	11.65%	60.19%	8.00E-01	8.18E-02	1.18E-01
4	20.00%	33.33%	46.67%	11.11%	37.04%	51.85%	8.63E-01	9.17E-02	4.58E-02
5	14.00%	66.00%	20.00%	7.53%	70.97%	21.51%	9.16E-01	7.76E-02	6.75E-03
6	35.30%	44.10%	20.60%	21.43%	53.57%	25.00%	9.29E-01	7.05E-02	0.00E+00
7	6.50%	71.00%	22.50%	3.33%	73.33%	23.33%	9.16E-01	8.11E-02	2.70E-03
8	25.20%	22.00%	52.80%	14.41%	25.23%	60.36%	8.86E-01	9.42E-02	1.97E-02
9	31.80%	18.20%	50.00%	18.92%	21.62%	59.46%	8.97E-01	8.86E-02	1.40E-02
10	36.60%	22.00%	41.40%	22.39%	26.87%	50.75%	7.89E-01	8.24E-02	1.29E-01
11	47.60%	38.10%	14.30%	31.25%	50.00%	18.75%	9.31E-01	5.28E-02	1.65E-02
12	15.80%	31.60%	52.60%	8.57%	34.29%	57.14%	8.30E-01	9.84E-02	7.16E-02
13	43.80%	18.80%	37.40%	28.00%	24.00%	48.00%	8.74E-01	7.11E-02	5.53E-02
14	33.30%	20.00%	46.70%	20.00%	24.00%	56.00%	7.86E-01	8.55E-02	1.28E-01
15	36.40%	45.50%	18.10%	22.22%	55.56%	22.22%	8.81E-01	6.47E-02	5.39E-02
16	11.10%	66.70%	22.20%	5.88%	70.59%	23.53%	8.57E-01	7.93E-02	6.34E-02

Based on hypothetical database, α-decomposition method and Bayesian inference, we are able to evaluate the posterior distributions of decomposed α-factors after the introduction of defense mechanisms. Because there is a Sum-to-One constraint for every set of α-factors, the $\alpha_1^{C_i}$ can be estimated based on the result of $\alpha_2^{C_i}$ and $\alpha_3^{C_i}$ and because $\alpha_1^{C_i}$ represents the ability to trigger independent failure, the discussion of $\alpha_1^{C_i}$ is omitted in current paper.

$$\alpha_1^{C_i} = 1 - \alpha_2^{C_i} - \alpha_2^{C_i}, (i = 1,2,3) \tag{23}$$

For the simplest consideration, here the distribution of the response variables (α_2, α_3) are assumed as a truncated normal distribution $(0 \le \alpha_j \le 1, j = 2,3)$ and the response can be written as a truncated normal regression model with mean (μ_j) and variance(σ_j^2):

$$\alpha_j \sim Normal(\mu_j, \sigma_j^2), (j = 2,3) \quad (24)$$

$$\mu_j(\alpha_j^{C_1}, \alpha_j^{C_2}, \alpha_j^{C_3}, r_1, r_2, r_3) = \sum_{i=1}^{3} \alpha_j^{C_i} r_i \quad (25)$$

The mathematical models of updated decomposed α-factors have been defined in Section 3, as shown in equations (15) and (18). Prior distributions of decomposed α-factors are assumed as lognormal distribution and the prior distributions of global α-factors' variance are assumed as gamma distribution, and then based on prior distributions as well as likelihood, posterior distributions could be calculated.

$$Prior\ \alpha_j^{C_i} \sim Lognormal(0.01,0.1), (i = 1,2,3; j = 2,3) \quad (26)$$

$$Prior \sigma_j^2 \sim Gamma(0.01,0.01), (j = 2,3) \quad (27)$$

$$Posterior\ \alpha_j^{C_i} \sim Prior \alpha_j^{C_i} \times Likelihood\left(r, \alpha_j \middle| \alpha_2^{C_i}\right), (i = 1,2,3; j = 2,3) \quad (28)$$

Calculating with tools (R & WinBUGS) based on the theory of Bayesian inference with MCMC Gibbs Sampling, we could get the posterior distributions for all α-factors after the introduction of defense mechanisms. The summary of posterior probability density functions (PDF) is shown in Table 2 and the detailed PDF of all analyzed α-factors are shown in Fig.6~Fig.9.

Table 2. Summary of posterior distributions after Bayesian inference

		Node	Mean	SD	MC Error	2.5%	Median	97.5%
Previous	**A & C**	$\alpha_2^{C_1}$	4.45E-02	4.40E-02	1.42E-03	5.31E-04	3.08E-02	1.57E-01
		$\alpha_3^{C_1}$	6.61E-02	5.66E-02	1.58E-03	7.97E-04	5.26E-02	1.95E-01
		Typical α_2	7.86E-02	1.06E-02	1.15E-04	5.76E-02	7.87E-02	9.98E-02
		Typical α_3	5.00E-02	1.40E-02	1.86E-04	2.09E-02	5.01E-02	7.77E-02
Updated	**A**	$\alpha_2^{C_1}$	8.83E-02	6.12E-02	1.73E-03	6.14E-03	7.61E-02	2.28E-01
		$\alpha_3^{C_1}$	0.00E+00	0.00E+00	-	0.00E+00	0.00E+00	0.00E+00
		Typical α_2	9.06E-02	1.95E-02	4.92E-04	5.58E-02	8.86E-02	1.32E-01
		Typical α_3	3.19E-02	1.74E-02	4.74E-04	2.94E-03	3.15E-02	6.58E-02
	C	$\alpha_2^{C_1'}$	0.00E+00	0.00E+00	-	0.00E+00	0.00E+00	0.00E+00
		$\alpha_3^{C_1'}$	0.00E+00	0.00E+00	-	0.00E+00	0.00E+00	0.00E+00
		Typical α_2	7.68E-02	1.77E-02	4.97E-04	3.71E-02	7.90E-02	1.06E-01
		Typical α_3	3.70E-02	2.02E-02	5.51E-04	3.39E-03	3.66E-02	7.62E-02

For Component A, because Cause 1 only produces the CCF events including Component A and B, the decomposed $\alpha_3^{C_1}$ for Component A become 0, which is also shown in Fig.6 that the posterior PDF of $\alpha_3^{C_1}$ appears as a green horizontal dash (PDF=0); simultaneously, since all the

global CCF events including Component A have turned into partial CCF events, the typical distribution of α_3 moves to the left, which shows in Fig.7. It means that the global CCF events have been degraded successfully. On the other side, all the global CCF risk has been degraded to partial CCF risk and half of the partial CCF risk has been degraded as independent failure risk. It can be judged from Table 2 that in the previous system, $\frac{1}{2}\alpha_2^{C_1} < \alpha_3^{C_1}$, so the updated $\alpha_2^{C_1}$ has increased slightly compared with the previous $\alpha_2^{C_1}$. If analyze other systems with $\frac{1}{2}\alpha_2^{C_1} > \alpha_3^{C_1}$, the partial CCF risk will be reduced numerically. The posterior PDFs of $\alpha_2^{C_1}$ and typical α_2 are shown as red dashed curves in Fig.6 and Fig.7, respectively. As a conclusion, after the introduction of defense strategy again Cause 1's coupling factor, the CCF events including Component A are actually not diminished but degraded to failures of lower severity.

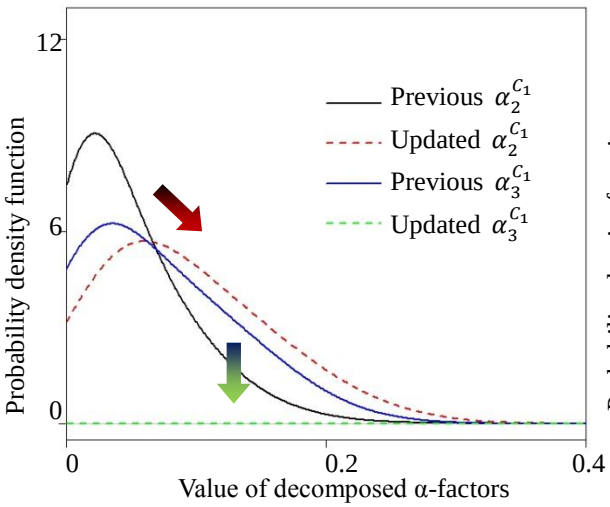

Fig.6 Posterior PDFs for Compt.A

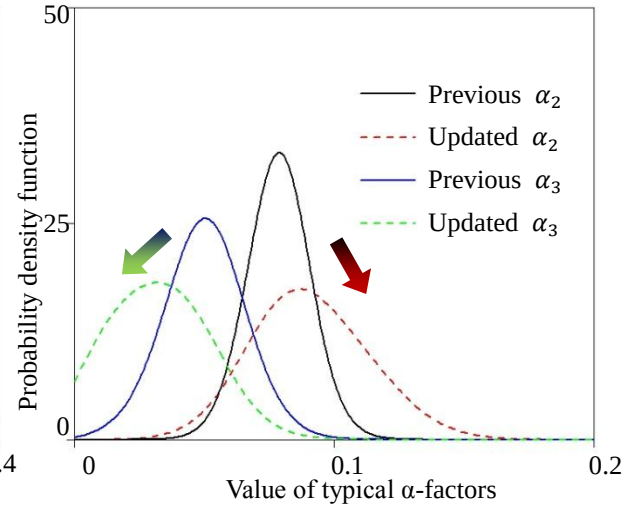

Fig.7 PDFs for typical parameters for Compt.C

For Component C, it should be mentioned that the data of Cause 1' is dug from other data sources as a result of that there is no recording of Cause 1' in the database of previous system. Because Cause 1 does not affect Component C anymore and Cause 1' is an independent cause affecting only Component C, the posterior $\alpha_2^{C_1'}$ and $\alpha_3^{C_1'}$ of Component C are 0, which practically means that the CCF events including Component C is only a sum contribution of Cause 2 and Cause 3. Fig.8 depicts posterior PDFs of $\alpha_2^{C_1'}$ and $\alpha_3^{C_1'}$, which have been updated from back and blue lined curves and turned in to the red horizontal dash. The CCF events including multiple components are reduced since both typical α_2 and α_3 have been reduced by the measure of physical separation, which are described in Fig.9 as red and green dashed curves moves to left slightly. However there are uncertainties in the changing of parameters for Component C. At first, the failures produced by Cause 1 are totally diminished but new potential failure are introduced by the new Cause 1', so there would be a variation in the amount of total failures. Secondly, because the Cause 1' is an independent failure, the parameters representing CCF risk are joint distributions as results of Cause 2 and Cause 3. Therefore, the CCF events including Component C are actually partly diminished, such as C_{CA}, C_{CB}, C_{CAB}, but the change of independent failures depends on the new Cause 1'. After the introduction of defense mechanisms, the judgment of CCF risk including Component C should take into the consideration of absolute failure amounts and α-factors together, as a result of that it might happen that the failure amounts decrease but the global α-factors increase slightly.

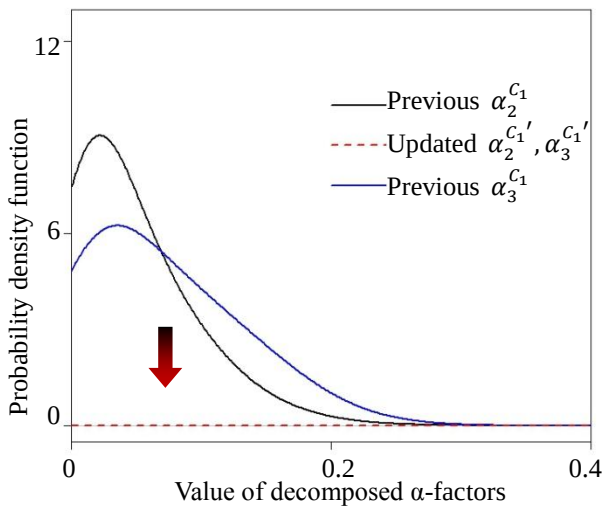

Fig.8 Posterior PDFs for Compt.C

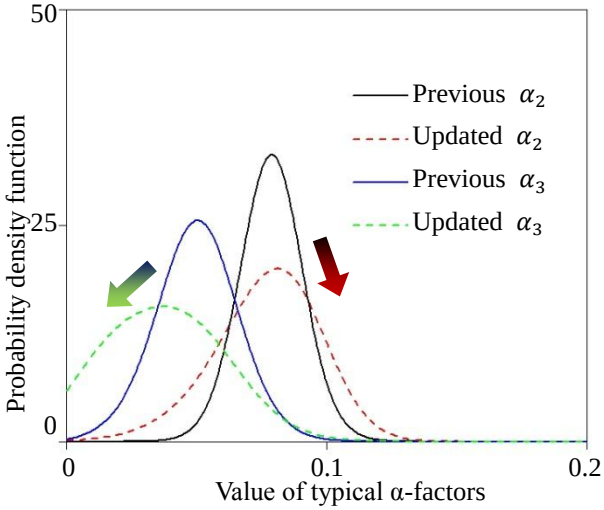

Fig.9 PDFs for typical parameters for Compt.C

It is easy to conclude that all the posterior distributions spread along X-axis more flat than the corresponding prior distributions. The uncertainty in PSA analysis is an important but very complicated topic. In the current example, uncertainties of decomposed α-factors and typical α-factors should be considered separately. (1) In Fig.6 and Fig.8, there is only one PDF ($\alpha_2^{C_1}$) obtained from Bayesian inference with database, and the increase of uncertainty in the posterior PDF of $\alpha_2^{C_1}$ comes from the degradation of global CCF, since the global CCF events caused by Cause 1 have been totally transformed into partial CCF events and the uncertainty of $\alpha_3^{C_1}$ has been turned into part of $\alpha_2^{C_1}$. (2) Generally speaking, the introduction of new information would tend to confirm the posterior distribution more accurately which behaves as a steeper bell curve with smaller variance. However, during the process of decomposition, there is a quite different situation which could be called the loss of information. It means that the integrated distribution has less uncertainty than the decomposed distributions and it is a result of the shortage of available data for specific decomposed parameter. The collected database is the representation of integrated state and if we decompose the integrated database without using enough new specific new information, the uncertainty will inevitably increase. As shown in Fig.7 and Fig.9, all posterior PDFs of typical global α-factors are of more uncertainties than prior PDFs. There are two possible reasons: firstly, for Component A in Fig.7, part of increased uncertainty of posterior typical α_2 is inherited from the degradation of global CCF; secondly, for other posterior typical α-factors, the increase of uncertainty comes from the diminishment of Cause 1 that has been excluded from posterior typical α_3(A), α_2(C) and α_3(C), so it is the source of uncertainty that loss of available information but without inputting other new information about global α-factors in modified system.

5. CONCLUSIONS

Based on α-decomposition method and Bayesian theory, the numerical estimation of CCF modeling involving defense mechanisms has been discussed in this paper. α-decomposition is an approach that has been introduced to analyze in the aspect of causal inference by means of combining information from cause-level, component-level and system-level. It has been mathematically proved that all global α-factors are integrated parameters, whose joint distributions combine all information generated by various causes and characteristics of system. Because α-decomposition treats CCF events by single component and set of causes, it

is useful to analyze asymmetrical system, especially for modified system designed to interrupt coupling factors. When the system has been modified for adopting a defense mechanism, there would be no exact database to evaluate the CCF risk for new system, and α-decomposition method is capable to reasonably utilize different data sources. In this paper, an example with is provided to illustrate, (1) how to numerically analyze the CCF based on the information from cause-level, (2) how to combine different data sources (system-specific data of root causes and global α-factors), and finally more explicit estimates of parameters are calculated.

ACKNOWLEDGMENTS

The authors would like to acknowledge the consistent encouragement and valuable criticism received from past and present members of Yamaguchi Lab at Osaka University.

REFERENCES

1. NUREG/CR-4780, Vol.1 and Vol.2, *Procedures for treating common-cause failure in safety and reliability studies: procedural framework and examples*, U.S. Nuclear Regulatory Commission, Washington, DC (1989).
2. NUREG/CR-5485, *Guidelines on modeling common-cause failures in probabilistic risk assessment*, U.S. Nuclear Regulatory Commission, Washington, DC (1998).
3. NUREG/CR-6268, *Common-cause failure database and analysis system: event data collection, classification, and coding,* U.S. NRC, Washington, DC (2007).
4. *CCF parameter estimations, 2003 - 2009 update.* U.S. NRC, Washington, DC (2011).
5. NUREG/CR-6819, *Vol.1~Vol.4*, *Common-cause failure event insights*, U.S. NRC, Washington, DC (2003).
6. Xiaoyu Zheng et al., "α-Decomposition Method: A New Approach to the Analysis of Common Cause Failure," *In proceedings of PSAM11 & ESREL 2012*, Helsinki, Finland (2012).
7. Akira Yamaguchi et al., "Seismic fragility analysis of the heat transport system of LMFBR considering partial correlation of multiple failure modes," *SMiRT 11 Transaction Vol.M*, Tokyo, Japan (1991).
8. Rasmuson DM and Kelly DL, "Common-cause failure analysis in event assessment," *Journal of Risk and Reliability*, **Vol.222**, pp.521-532 (2008).
9. Kelly DL et al., "Common-cause failure treatment in event assessment: basis for a proposed new model," *In proceedings of probabilistic safety assessment and management (PSAM) 10*, Seattle, USA (2010).
10. Akira Yamaguchi et al., "Epistemic Uncertainty Reduction in the PSA of Nuclear Power Plant using Bayesian Approach and Information Entropy," *In proceedings of probabilistic safety assessment and management (PSAM) 10*, Seattle, USA (2010).
11. Daphne Koller and Nir Friedman, *Probabilistic graphical models*, Cambridge, Massachusetts: The MIT Press (2009).
12. Judea Pearl, *Causality: models, reasoning, and inference, second edition*, Cambridge University Press (2009).
13. Peter Congdon, *Bayesian Statistical modeling*, John Wiley & Sons, Ltd (2006).
14. Dani Gamerman and Hedibert F.Lopes, *Markov Chain Monte Carlo: stochastic simulation for Bayesian inference, second edition*, Chapman & Hall/CRC (2006).
15. Ioannis Ntzoufras, Bayesian modeling using WinBUGS. John Willey & Sons, Inc., 2009.
16. John K. Kruschke, *Doing Bayesian data analysis: a tutorial with R and BUGS*, Elsevier Inc. (2011).