INTERACTIVE SYSTEM DESIGN USING THE COMPLEMENTARITY OF AXIOMATIC DESIGN AND FAULT TREE ANALYSIS

GYUNYOUNG HEO*, TAESIK LEE and SUNG-HEE DO[1]
Massachusetts Institute of Technology Department of Mechanical Engineering
77 Massachusetts Avenue, Cambridge, MA 02139, USA
[1]Axiomatic Design Solutions Inc.221 North Beacon Street, Brighton, MA 02135, USA
*Corresponding author. E-mail : gheo@mit.edu

Received April 10, 2006
Accepted for Publication September 18, 2006

To efficiently design safety-critical systems such as nuclear power plants, with the requirement of high reliability, methodologies allowing for rigorous interactions between the synthesis and analysis processes have been proposed. This paper attempts to develop a reliability-centered design framework through an interactive process between Axiomatic Design (AD) and Fault Tree Analysis (FTA). Integrating AD and FTA into a single framework appears to be a viable solution, as they compliment each other with their unique advantages. AD provides a systematic synthesis tool while FTA is commonly used as a safety analysis tool. These methodologies build a design process that is less subjective, and they enable designers to develop insights that lead to solutions with improved reliability. Due to the nature of the two methodologies, the information involved in each process is complementary: a success tree versus a fault tree. Thus, at each step a system using AD is synthesized, and its reliability is then quantified using the FT derived from the AD synthesis process. The converted FT provides an opportunity to examine the completeness of the outcome from the synthesis process. This study presents an example of the design of a Containment Heat Removal System (CHRS). A case study illustrates the process of designing the CHRS with an interactive design framework focusing on the conversion of the AD process to FTA.

KEYWORDS : Axiomatic Design, Fault Tree Analysis, System Reliability, Functional Requirement, Design Parameter, Failure Mode

1. INTRODUCTION

Design is divided primarily into two processes: 'synthesis' and 'analysis'. For the purposes of this paper, synthesis is regarded as the process of decision-making regarding parameters, and analysis as the process of optimizing those parameters. It is known from experience that the mistakes made during the synthesis process are never completely corrected in the analysis process. For example, in the design of a safety-critical system where a critical concern is its reliability, if the upstream synthesis process results in an unreliable system, the system is rarely transformed into a highly reliable system. The downstream detailed analysis process only slightly improves its reliability. It is commonly known that it is possible to achieve higher reliability with less cost if reliability is built into the system from the early design phase. Many approaches have been proposed in order to integrate synthesis and analysis into a single framework that minimizes the overall design efforts toward maximizing the reliability. This paper shares that goal with those proposals. The claim here is that as the synthesis and analysis processes more closely interact, a high level of system reliability becomes more achievable. Because uncertainty and subjectivity are inherent to the synthesis process while the analysis process cannot tolerate uncertainty and subjectivity, their consummated integration poses significant challenges. If synthesis and analysis methodologies can be found with the following properties, their integration should be more promising:

- It should be applicable to all of the design phases, from the early design phase to a detailed design phase.
- It should provide a means to quantitatively as well as qualitatively evaluate design decisions. Qualitative decision-making is usually dominant in the early design phase, while quantitative evaluation is necessary in the detailed design phase.
- It should share a fundamental framework in performing the synthesis and analysis processes to reduce the effort and resources required for the integration. An integrated framework is valuable only if the effort to carry out it

is less than the sum of the effort required to complete each step separately.

In order to make the two processes more interactive, this paper endeavors to develop a design framework based on the complementarity of Axiomatic Design (AD) and Fault Tree Analysis (FTA). AD provides a framework that allows designers to synthesize systems systematically [1]. Many systems have been designed on the basis of heuristics or empirical experience rather than within a formal theoretical framework. The validation or testing process of these systems is generally expensive and unpredictable due to the uncertainties associated with experience-based design. The two axioms of AD guide designers so that such a validation can be minimized. In contrast, FTA has been widely used to quantify the reliability of safety-critical systems. FTA was developed by Watson in 1961 and its use has become widespread since the early 1970s when computer-based analysis techniques were developed. FTA is a logical tool for understanding the reliability of a system both qualitatively and quantitatively. A reactor safety study by the US Nuclear Regulator Commission (NRC) [2] and a space shuttle study performed by the National Aeronautics and Space Administration (NASA) [3] are well-known examples of FTA. The AD and FTA methodologies are acknowledged as novel tools for synthesis and analysis, respectively. The strategy in this study is to pull the characteristics of FTA into AD. The proposed framework enables us to develop insights into reliability-informed synthesis by bringing reliability analysis into the synthesis process. It is believed that AD and FTA have fully shown the first and second properties mentioned above through industrial, as well as academic studies [1,4,5]. This study focuses on the third property, and argues that complementarity between AD and FTA offers a basis for a common framework. It is observed that the hierarchical tree and Design Matrix (DM) of AD have close relationship with FT. The complementary characteristics of the functional hierarchical trees of AD and FT enable the development of an interactive design framework. In the next sections, the theoretical background of the complimentarity is described along with the relevant guidelines to construct the interactive design framework. We also present an example of a design of safety features in nuclear power plants, which serves to illustrate the proposed framework.

2. THEORETICAL BACKGROUND

In this chapter, AD and FTA in addition to their complementarity are briefly introduced. Following this, an interactive design framework is proposed.

2.1 Introduction to Axiomatic Design

Axiomatic Design (AD) originated in the field of design. Its purpose is to provide guidelines for a systematic design process during a synthesis process. AD defines four design domains. These four domains consist of the Customer Attribute (CA) domain, the Functional Requirement (FR) domain, the Design Parameter (DP) domain, and the Process Variable (PV) domain [1]. From the CA domain, the FRs of "what we want to achieve" are resolved. A FR domain is the technical representation of customers' needs, as defined in a CA domain. It shapes an ideally desirable functional range, known as a Design Range (DR). In order to implement the DR given by the FR domain, the DPs of "how we achieve it" are decided. They consist of a DP domain. The decision of sub-FRs and corresponding sub-DPs is repeated until an appropriate design level is reached. This process is characterized by 'decomposition' and 'zigzagging', as shown in Fig. 1. To minimize subjectivity during these processes, attempts are made to ensure that a FR domain is mutually exclusive and collectively exhaustive [6] and that it is in neutral environment without any bias for a particular DP to be selected. The operational ranges of the selected DPs form the functional reach of the system. This is known as the System Range (SR), which is the actually achievable functional range.

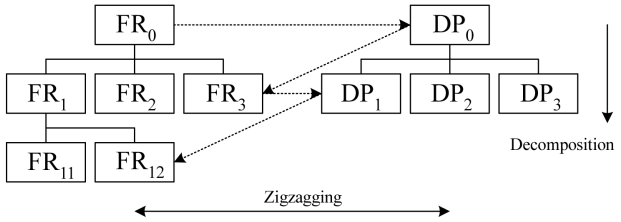


Fig. 1. Decomposition and Zigzagging of a FR-DP Hierarchical Tree

In contrast, AD offers two representation tools to efficiently present design products: a FR-DP hierarchical tree and a Design Matrix (DM). A FR-DP hierarchical tree is a type of Success Tree (ST) depicting all of the sets of FRs and DPs established by the decomposition and zigzagging process. By definition, a ST is a top-down logic model generated in the success domain. Therefore, an upper and a lower level in a FR-DP tree are connected by 'AND' logic gates despite the fact that there is no explicit expression.

A DM whose physical meaning is the ratio of the variation of FRs caused by the variation of DPs, which can be termed sensitivity, is defined by Eq. (1).

$$\{FRs\} = [A]\{DPs\} \tag{1}$$

where [*A*] is a matrix defined as a DM, $A_{ij} = \partial FR_i / \partial DP_j$

$\{FRs\}$ is a vector that constitutes a set of FRs,

{*DPs*} is a vector that constitutes a set of DPs.

According to the configuration of a DM, the design is classified into one of three types. When a DM is diagonal, each of the FRs is satisfied independently by means of a unique corresponding DP. Such a design is termed an uncoupled design. If a DM is triangular, such a design is termed a decoupled design. All other designs are known as coupled designs. In other words, off-diagonal elements that are larger than zero are regarded as functional couplings. Along with the four domains and two visualization tools, AD provides two design axioms to provide the proper direction while seeking a better solution.

- Axiom 1, independent axiom: maintain the independence of FRs
- Axiom 2, information axiom: minimize the information content of a design

The independence axiom indicates that a DM must be either uncoupled or decoupled. The information axiom indicates that the best design will be the one with the lowest level of information content from among the solutions that fulfill the independent axiom. Information content is defined as the log of the probability of satisfying given FR sets [1]. The probability of satisfying given FRs is calculated from the DR, the probabilistic distribution of the SR, and their overlapping area, which is known as the 'common range'. Though the calculation of the information content is theoretically feasible, the enormous variables affecting the information content make this practically impossible in many cases. For this reason, a small number of studies have proposed their own estimator for application in specific situations [7-10].

2.2 Complementarity

FTA is a well-known methodology in reliability engineering. FTA is a deductive procedure for determining various combinations of hardware and software failures, as well as human errors, which can result in a specified undesirable event, referred to as a top event. Its guidelines are well established, and many industrial-scale applications have been executed.

Although AD and FTA were developed as entirely different disciplines, with entirely different purposes, complementarity can be found in their reasoning processes, representation schemes, and in the quantification of success or failure to put them into a single design framework. During decomposition, all of the sub-FRs are chosen such that they are necessary to achieve their parent FR. Therefore, by definition, a FR-DP tree is a success tree, thus it is theoretically convertible into a FT by changing logic gates [11]. This complementarity makes the FR-DP tree and a FT compatible.

It is possible to observe another complementarity in the way that AD and FTA define success and failure, respectively. FTA classifies three failure categories, taking into account the existence of interaction with other failures [11]: a primary, a secondary, and a command failure. Although modern FTA does not strictly follow this classification while performing probabilistic safety assessment, the grouping of failures into the three classes is useful for highlighting the complementarity. A primary failure is defined as a component being in a nonworking state for which the component is held accountable. A primary failure randomly occurs within a design envelope without any interaction with other failures. A secondary failure is identical to a primary failure except that the component is not held accountable for the failure. A command failure is defined as the component being in a nonworking state due to improper control signals or noise. A secondary and a command failure are caused by an abnormal operation or failure of other physical parts. Fig. 2 qualitatively shows the relationship of the functional coupling defined in AD and failure events defined in FTA. In terms of AD, the probability of success is equal to the common range of a DR and a SR. Therefore the area of the SR located outside the DR corresponds to the probability of failure. One of the factors characterizing a SR is functional coupling. In Fig. 2, the SR of an uncoupled design has no failure caused by functional coupling. Thus, the black portion represents the only primary failure defined in FTA. On the other hand, the SR of a (de)coupled design involves all of the types of failures defined in FTA, which matches the meshed portion. Based on the known facts in AD and FTA, it was deduced that the probability of satisfying given FR sets can be characterized by the failure frequency defined in FTA. In other words, the failure frequency can play the role of approximating information content when designing safety-critical systems.

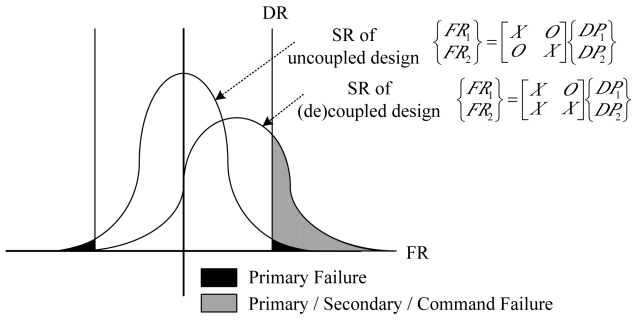


Fig. 2. Comparison of Functional Coupling and Failure Events

While both methodologies have a number of common characteristics, and there are definite differences between them as well. Firstly, AD provides a reasoning process particularly for synthesizing a new design, but FTA is a

tool for assessing an existing design. Secondly, a FR-DP tree is an explicit functional hierarchy, but a FT represents a failure propagation which is not usually equal to a functional hierarchy. This signifies that it is not always possible to convert a FT into a FR-DP tree by merely changing the logic gates. Thirdly, the lowest level of a FR-DP tree is DPs, but that of a FT, known as the basic event, should be a physical part whose failure data is available. A DP can be a physical property, as well as a physical part itself. Even if a DP is a physical part, it is likely that it does not satisfy the requirements that could make it a basic event. Therefore, there is a clear difference between the resolutions of the two methodologies. On account of these differences, a few supplementary rules for converting a FR-DP tree into a FT to integrate the two methodologies are required.

2.3 Conversion Rules from AD to FTA

Though a FR-DP tree and a FT are complimentary, a conversion is not straightforward due to their inherent characteristics. This section provides a number of supplementary rules for achieving a conversion of a FR-DP tree and a DM to a FT.

2.3.1 Mapping to Failure Mode Domain

The objective of this study is to enable the consideration of reliability issues from an early design phase. During the early design phase, in which the synthesis process dominates, the DPs play an important role in proposing a solution. To bring reliability considerations into this design phase, it is necessary to make connections between the failure mechanism of physical parts and the DPs. This requires a proper definition for the failure of a DP. The failure of a DP refers to a situation during which the DP does not deliver its corresponding FR. This occurs when the DP is located outside its allowable range. The failure of a DP should include all of the possible cases which make the SR of the FRs move from inside a DR to outside a DR. In this context, the traditional notion of Failure Mode (FM) is customized, and an assumption is the failed DPs are always associated with the FMs.

A FM is customized as a characterization of the observable and distinguishable manner in which a DP fails. As DPs can be physical parameters while traditional FMs require the existence of physical parts, the failure of DPs should be projected to physical parts, components, or systems to properly characterize them. Failures may result from a cause either with or without functional coupling, though the same consequences appear. In order to distinguish the origin of failures, the pre-condition of a DP under which failure occurs as a FM was considered. Thus, a FM is given to a specific operation mode of the DP affecting the success of other DPs. While designing safety-critical systems, Common Cause Failures (CCFs) are an important FM. Given that CCFs take place inside a single DP or over a few DPs in terms of AD theory, there is no proper method for mapping a DP to a CCF. The management of CCFs will be addressed in a subsequent section.

2.3.2 Basic Conversion of a FR-DP Tree into a FT

Fig. 3 illustrates the method for converting a FR-DP tree into a FT. The overall structure of the FT is identical to that of a FR-DP tree due to the complimentarity. A FT uses 'OR' logic gates to represent failure logic between an upper and a lower levels, which are converted from the 'AND' gates implicitly involved in a FR-DP tree. The FMs of physical parts are then mapped into appropriate DPs. This mapping can be one-to-one, many-to-one, or one-to-many. In FTA, all of the basic events that comprise the lowest level of a FT are eventually replaced with the FMs that were extensively customized in the previous section. For uncoupled designs, all of the basic events are composed of only the primary failure of the FMs shown in Fig. 3(a). If there are off-diagonal elements in a DM, which indicate functional coupling, additional 'OR' gates are needed to add the basic events. These additional basic events represent the conditional probability of FMs. From Fig. 3(b), the failure of FR_2 occurs as a result of either the failure of the corresponding DP_2 or a specific condition of DP_1. This rule is applicable regardless of the position of the off-diagonal elements. For example, conditional failure events can be generated from the elements located between identical hierarchical levels or at different levels. In certain circumstances, a FM may be mapped onto more than two DPs when a physical part involves the DPs. In those cases, most basic events representing the conditional probability can be eliminated or ignored by a Boolean operation or by taking into account their physical validity.

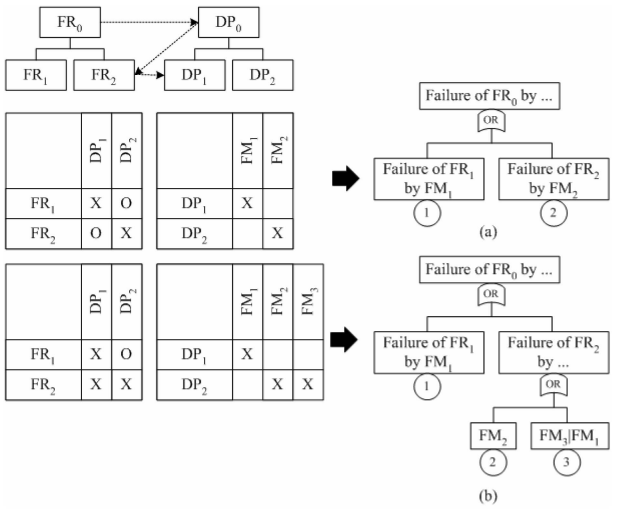


Fig. 3. Conversion of a FR-DP Hierarchical Tree into a FT (FM_A is an independent failure of a corresponding DP. $FM_B|FM_C$ indicates that FM_B is a dependent failure of a corresponding DP caused by FM_C.)

A detailed procedure for determining failure frequency using a FT follows traditional guidelines [10]. The role of failure frequency was mentioned as an approximated measure of the information content. It is a representative product of FTA. If the calculated failure frequency does not meet the given criteria, alternative DPs can be suggested, in an effort to decrease the probability of failure. Each time an alternative design is made, the FR-DP tree and the DM are updated accordingly. The modification of a FT should then follow. It is not until the given reliability criteria are fully satisfied that this interactive process is finished.

2.3.3 Conversion of Alternative Design

It is common that multiple physical parts are installed to reliably achieve identical FRs. In reliability engineering, they are separated into two categories according to their characteristics and ability. If they have the same physical mechanism as the original or are merely duplicated, it is termed a 'redundant design'. Otherwise, it is known as a 'diverse design.' In terms of the AD theory, a redundant design corresponds to multiple physical parts delivering the role of a single DP. A diverse design is defined as design alternatives with multiple DPs to achieve the same set of FRs. In this paper, they are known as alternative design, which indicates a set of physical parts, components, or systems to achieve a single FR regardless of a redundant or diverse design. Alternative designs are usually deployed to replace failed DPs or to mitigate the consequence of failed DPs.

The system with alternative designs is described by the non-square DM in Eq. (2). Eq. (2) can be re-stated by Eqs. (3-1) and (3-2), as alternative designs are used separately at a specified time or specified condition.

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = \begin{bmatrix} X & O & X \\ O & X & X \end{bmatrix} \begin{Bmatrix} DP_{alt1} \\ DP_{alt2} \\ DP_2 \end{Bmatrix} \quad (2)$$

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = \begin{bmatrix} X & O \\ O & X \end{bmatrix} \begin{Bmatrix} DP_{alt1} \\ DP_2 \end{Bmatrix} \quad at \quad t = t_1 \quad (3\text{-}1)$$

$$\begin{Bmatrix} FR_1 \\ FR_2 \end{Bmatrix} = \begin{bmatrix} X & O \\ O & X \end{bmatrix} \begin{Bmatrix} DP_{alt2} \\ DP_2 \end{Bmatrix} \quad at \quad t = t_2 \quad (3\text{-}2)$$

Here, *alt1* and *alt2* are the first and second alternative design for FR_1, respectively.

Fig. 4 illustrates the method for drawing the FT with alternative designs. All of the DPs are mapped into relevant FMs. The difference from a basic conversion is that 'AND' gates are needed to combine the failure logic of the alternative designs. In some cases, a fractional number is assigned to the gates to indicate a voting scheme. For example, in Fig. 4, DP_1 has three alternatives. If a single DP for achieving FR_1 at a specified condition is necessary (1-out-of-3 voting gate), the FT is drawn as shown in Fig. 4(a). If at least two alternatives are desirable (2-out-of-3 voting gate), the proper FT is Fig. 4(b).

One of the most important concerns while deploying alternative designs is a CCF. A DM does not have an appropriate method to show CCFs, as CCFs happen inside a single DP, which is the minimum resolution in the decomposition or over a few DPs under the same external influence. Therefore, the representation of CCFs is not involved in the conversion process from a FR-DP tree to a FT. If it is necessary to complete the FT involving CCFs, the branches of the representative CCFs could be appended at the appropriate locations, similar to manner in which the traditional FTA manages CCFs. The dotted portion in Fig. 4 shows an example for adding the failure modes caused by a CCF.

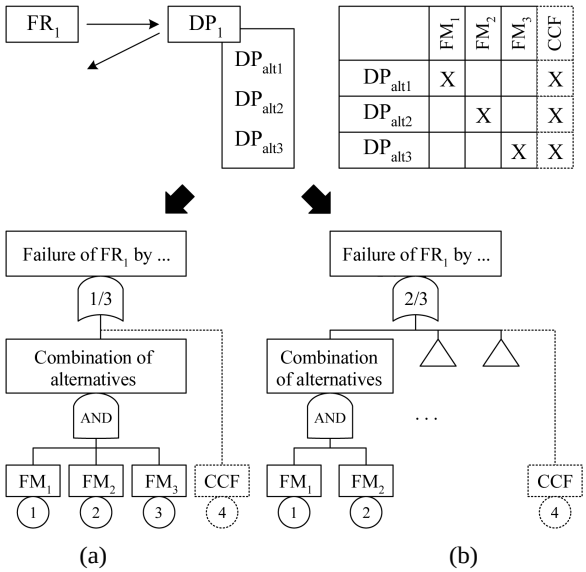


Fig. 4. Conversion of Alternative Designs into a FT (The node for CCFs (dotted line) can be appended.)

3. CASE STUDY: CONTAINMENT HEAT REMOVAL SYSTEM

The previous chapter described the proposed interactive design framework based on AD and FTA, and explains

the conversion scheme. This chapter demonstrates the application of this interactive design framework using a well-known example, a Containment Heat Removal System (CHRS) which was analyzed by WASH-1400, US NRC [2]. The purpose of the case study is to illustrate the process of designing the CHRS with an interactive design framework from the outset of the design to the point where it is quantified as a converted FT. This study is not intended to produce a better CHRS design. It is assumed that the information shown in the FTA by the US NRC is identical to that in a synthesis process. Therefore, the end result of the interactive design framework should be identical to the current CHRS. CHRS is one of the safety features in nuclear power plants. Fig. 5 shows a simplified flow diagram of the existing CHRS. In Fig. 5, all of the multiple trains were merged into a single path, but the name tags state how many multiple trains are installed.

The first step is to determine the top FR for the CHRS. The function of CHRS is to cool the containment sump water being re-circulated through the Containment Spray Recirculation System (CSRS). Therefore, it was decided to 'remove sufficient heat from the spray fluid' as a top FR, FR_0 and a CHRS was designated as a top DP, DP_0. To implement DP_0, the following four sub-FRs are necessary under a solution-neutral environment: 1) FR_1; coolant inventory, 2) FR_2; coolant driving force, 3) FR_3; coolant delivery path, and 4) FR_4; heat transfer mechanism. As the simulation of the design process of the existing CHRS is carried out, the corresponding DPs are taken to be: 1) DP_1; the river water in the intake canal, 2) DP_2; the head difference, 3) DP_3; the piping network, and 4) DP_4; the indirect heat transfer. Each DP is then decomposed in detail. For example, to implement DP_1, which requires transporting river water up to the intake canal located on higher ground, a pump and power source for the pump are needed. For DP_3, which arranges a coolant flow path, it is necessary to suggest the FRs for the inlet condition, air venting, and piping. This decomposition process is repeated until all of the DPs are decomposed to the desired level. The first three columns in Table 1 show the results of the FR-DP decomposition for a CHRS as a whole. The FR-DP decomposition in Table 1 enables the sketching of a preliminary design of a CHRS, as shown in Fig. 5. The fourth column in Table 1 is a list of the physical parts necessary for realizing

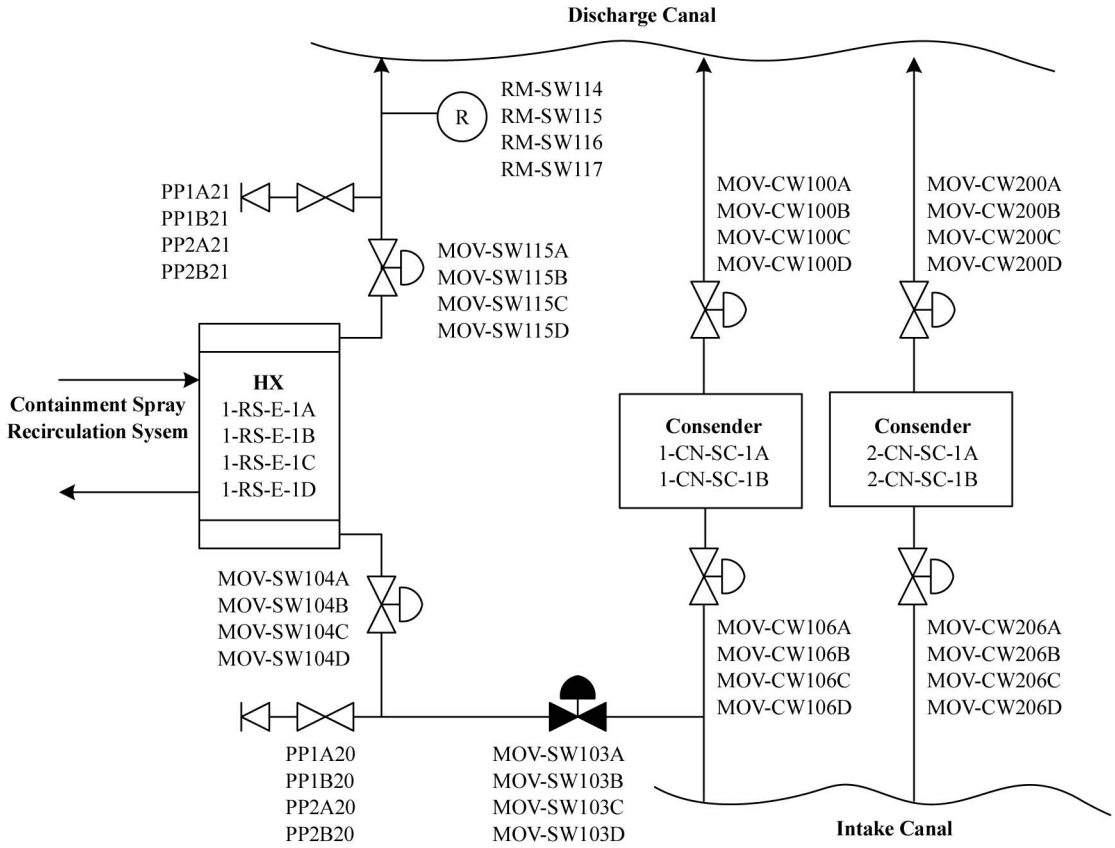


Fig. 5. Simplified Flow Diagram of a CHRS

Table 1. Preliminary Results for Designing a CHRS

	FRs	**DPs**	**Physical Parts**	**FMs**
0	Remove sufficient heat from spray fluid	Containment Heat Removal System		
1	Provide sufficient service water inventory	River (intake canal)		
1.1	Provide pumping equipment	Circulating water pump	Pump	1. Fail to run
1.2	Provide operation source for pumping	Power circuit by off-site power	Power bus	1. Loss of power
2	Provide service water driving force	Flow induced by head difference		
2.1	Provide higher head at intake	Higher intake canal position	Canal	N/A
2.2	Provide lower head at drain	Drain pumping	Pump	1. Fail to run
3	Provide proper configuration for service water	Piping network for service water		
3.1	Provide the inlet of service water	Inlet on/off mechanism	Motor Operated Valve (MOV)	1. Fail to open, 2. Inadvertent close
3.2	Provide air venting to make injection possible	Air vent on/off mechanism		
3.2.1	Provide air vents at inlet	Air venting on/off line at inlet		
3.2.1.1	Provide air vent equipment	Inlet air vent valves	MOV	1. Inadvertent open, 2. Fail to open
3.2.1.2	Provide operator	Human operator	Operator	1. Human error
3.2.2	Provide air vents at outlet	Air venting on/off line at outlet		
3.2.2.1	Provide air vent equipment	Outlet air vent valves	MOV	1. Inadvertent open, 2. Fail to open
3.2.2.2	Provide operator	Human operator	Operator	1. Human error
3.3	Provide flow path	Piping network	Pipe	1. Break
4	Provide the way for heat transfer from spray fluid to service water	Heat transfer by indirect contact		
4.1	Provide proper structure for indirect contact heat transfer	Shell & tube type heat exchanger	Heat exchanger	1. Break
4.2	Supply spray fluid to either side of heat transfer surfaces	Containment Spray Recirculation System pumping		
4.2.1	Provide pumping equipment	CSRS pumps	Pump	1. Fail to run
4.2.2	Provide proper configuration for spray fluid	Piping network	Pipes	1. Break
4.2.3	Provide power source for pumping equipment	460 Volts AC	AC bus	1. Insufficient volts
4.2.4	Provide power source for control	125 Volts DC	DC bus	1. Insufficient volts
4.3	Prevent leakage from spray fluid to service water	Drain isolation by monitoring radioactivity		
4.3.1	Provide radioactivity monitoring equipment	Radiation monitoring sensor	Sensor	1. Sensor trouble
4.3.2	Provide the way to isolate service water leaking to environment	Isolation valves		
4.3.2.1	Provide the isolation valves at inlet	Inlet isolation on/off mechanism of heat exchanger	MOV	1. Fail to close, 2. Inadvertent close
4.3.2.2	Provide the isolation valves at outlet	Drain isolation on/off mechanism of heat exchanger	MOV	1. Fail to close, 2. Inadvertent close

the preliminary design of the CHRS. It was assumed that all of the physical parts were feasibly selected and can supply all of the lowest level of DPs. Though it is possible to advance to a lower level, for easier demonstration the process is halted at this point and the next level is addressed.

The second step is to populate a DM to determine if there exists functional coupling of the preliminary design of a CHRS. The schematic flow diagram of the preliminary design in Fig. 5 provides insight into a method for populating the DM, and Fig. 6 displays the results. In this study, Acclaro™ facilitates the AD process [11]. It facilitates the classification of designs; coupled, decoupled, or uncoupled. Most functional couplings are present in the DPs related to heat transfer. For example, FR_{41}, 'provide the proper structure for indirect contact of service water' is closely related to the configuration of the fluid path inside as well as outside heat exchanger, as DP_{41}, 'shell & tube type heat exchanger' was chosen as a solution. DP_{31} and DP_{32} are noted as potential causes that may affect the satisfaction of FR_{41}. As power-operated equipment such as pumps are

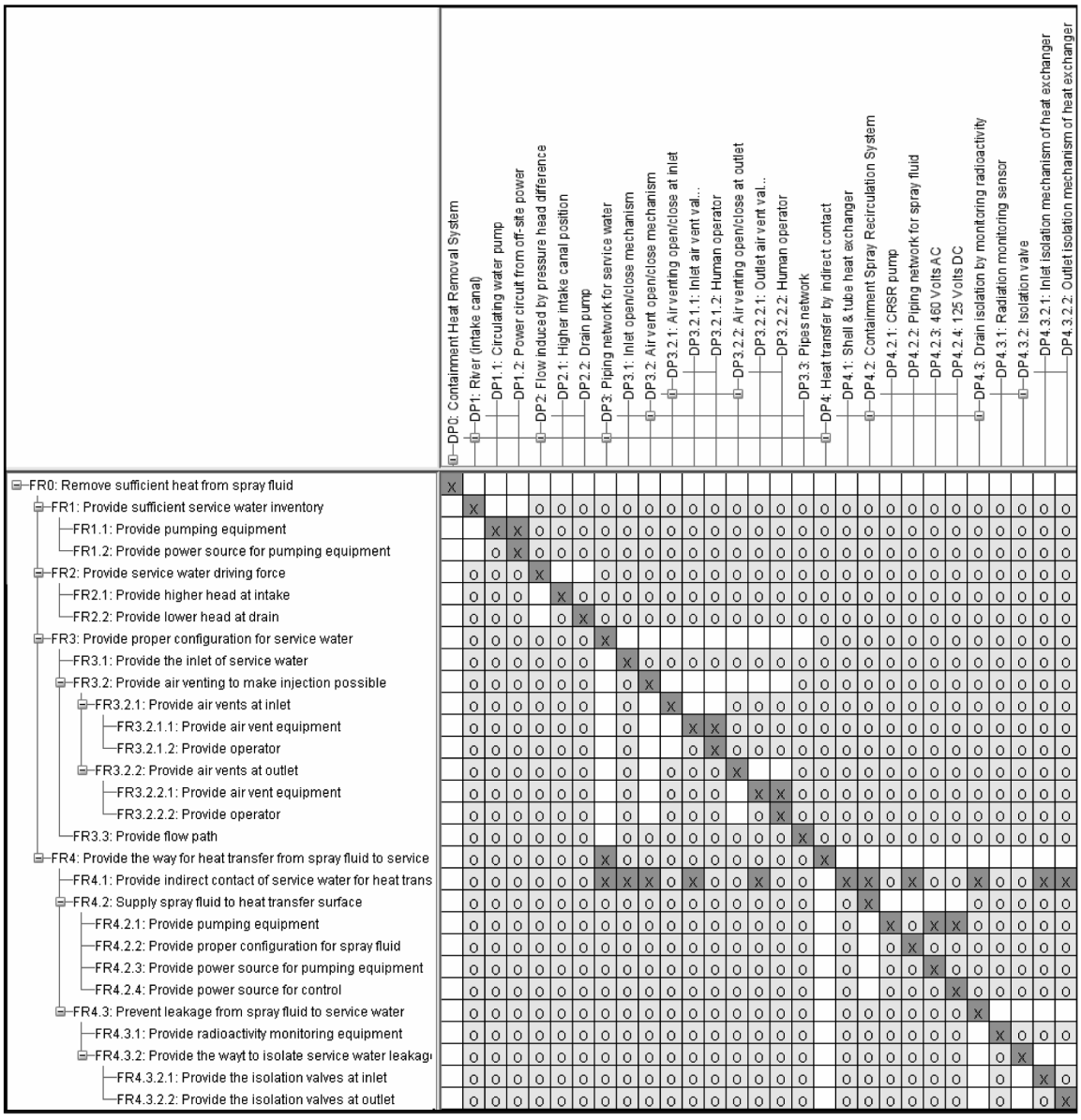


Fig. 6. Populated DM for Designing a CHRS

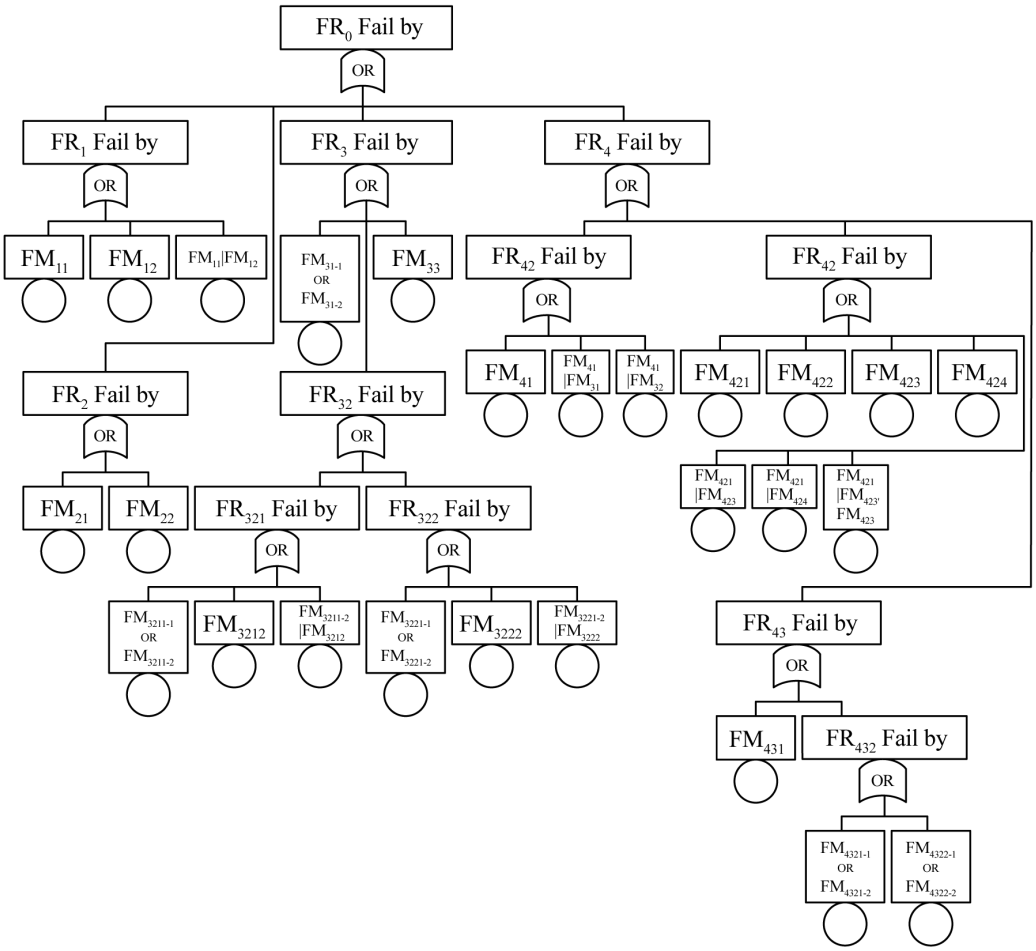


Fig. 7. Preliminary FT Converted from the Design Products by AD

typically coupled with a power source or a controller, additional couplings are disclosed in FR_{11}, FR_{3211}, FR_{3221}, and FR_{421}.

The third step is to map FMs into DPs and to generate a FT. It was assumed that the design information involved in the synthesis and analysis process is equal. In other words, the FMs that are generative while implementing DPs should be identified in a similar approach as are the FMs provided by WASH-1400. Therefore, the DPs of the lowest levels are mapped into the FMs provided by WASH-1400 considering the pipes, valves, control circuit components, electric power, and human error - without addressing their validity. The fifth column in Table 1 shows a list of the FMs that exist in the preliminary design of a CHRS. Using the FM and the conversion rules described earlier in this paper, a preliminary FT was constructed, as shown in Fig. 7. The structure of the FT is identical to that of the FR-DP hierarchical tree. The FT is composed of the FMs which replace DPs. Additionally, several FMs caused by functional coupling are suspended. By taking into account the duplication among the precursors resulting in functional coupling-induced failures, a number of of them are eliminated. If all of the FMs are quantifiable, it is possible to obtain the probability of failure at the top event, 'the failure of FR_0.'

The fourth step is to determine if the probability of failure at the top event is acceptable in terms of the customers' criteria. If it does not meet this criteria, either a redundant or diverse design may be chosen in an effort to improve the reliability of the preliminary design. Table 2 lists the redundant designs deployed in the design of the CHRS as well as the assumptions when calculating the failure frequency, as provided by WASH-1400. The failure frequency of several FMs is regarded as a negligible quantity; however, this does not imply they are eliminated. On the basis of these lists, redundant designs to the bare-

Table 2. Improved Design of a CHRS Using Redundant Designs

	DPs	**Modified FMs**	**Redundant Physical Parts**
0	Containment Heat Removal System		
1	River (intake canal)		
1.1	Circulating water pump	1. Negligible	8 trains
1.2	Power circuit by off-site power	1. Loss of power	
2	Flow induced by head difference		
2.1	Higher intake canal position	N/A	
2.2	Drain pumping	1. Negligible	1-SW-P-5A~D
3	Piping network for service water		
3.1	Inlet on/off mechanism	1. Negligible, 2. Negligible	MOV-SW103A~D
3.2	Air vent on/off mechanism		
3.2.1	Air venting on/off line at inlet		
3.2.1.1	Inlet air vent valves	1. Negligible, 2. Fail to open	PP1A20, PP1B20, PP2A20, PP2B20
3.2.1.2	Human operator	1. Human error	
3.2.2	Air venting on/off line at outlet		
3.2.2.1	Outlet air vent valves	1. Negligible, 2. Fail to open	PP1A21, PP1B21, PP2A21, PP2B21
3.2.2.2	Human operator	1. Human error	
3.3	Piping network	1. Break	Common head
4	Heat transfer by indirect contact		4 trains
4.1	Shell & tube type heat exchanger	1. Break	1-RS-E-1A~D
4.2	Containment Spray Recirculation System pumping		
4.2.1	CSRS pumps	1. Fail to run	1-RS-P-1A, B; 1-RS-P-2A, B
4.2.2	Piping network	1. Break	
4.2.3	460 Volts AC	1. Insufficient volts	Bus 1A, B
4.2.4	125 Volts DC	1. Insufficient volts	Bus 1J, H
4.3	Drain isolation by monitoring radioactivity		
4.3.1	Radiation monitoring sensor	1. Sensor trouble	RM-SW114~117
4.3.2	Isolation valves		
4.3.2.1	Inlet isolation on/off mechanism of heat exchanger	1. Negligible, 2. Inadvertent close	MOV-SW104A~D
4.3.2.2	Drain isolation on/off mechanism of heat exchanger	1. Negligible, 2. Inadvertent close	MOV-SW105A~D

bone CHRS were considered, as was a modification of the voting scheme of the DPs. It is of interest that DP_4 has four train redundant mechanisms, but the electric sources of a CSRS, DP_{423} and DP_{424} have only two trains. The voting scheme of DP_4 is 3/4, which indicates a CHRS required three out of four trains to meet a performance criterion. In addition to redundant designs, a diverse design for DP_1 is involved as an alternative design. The level in the intake canal is maintained by eight circulating water pumps that take water from the river. These pumps are powered by off-site power. If off-site power is lost, half of these pumps stop, as emergent diesel power is insufficient for supplying electricity. Table 3 provides a modified FR_1 and DP_1 to represent the alternative design of the original DP_1. New decisions for all of the sub-FRs and sub-DPs are needed for the alternative design. For the new DPs, it is necessary to analyze the FMs. The finalized FMs are given in Table 3.

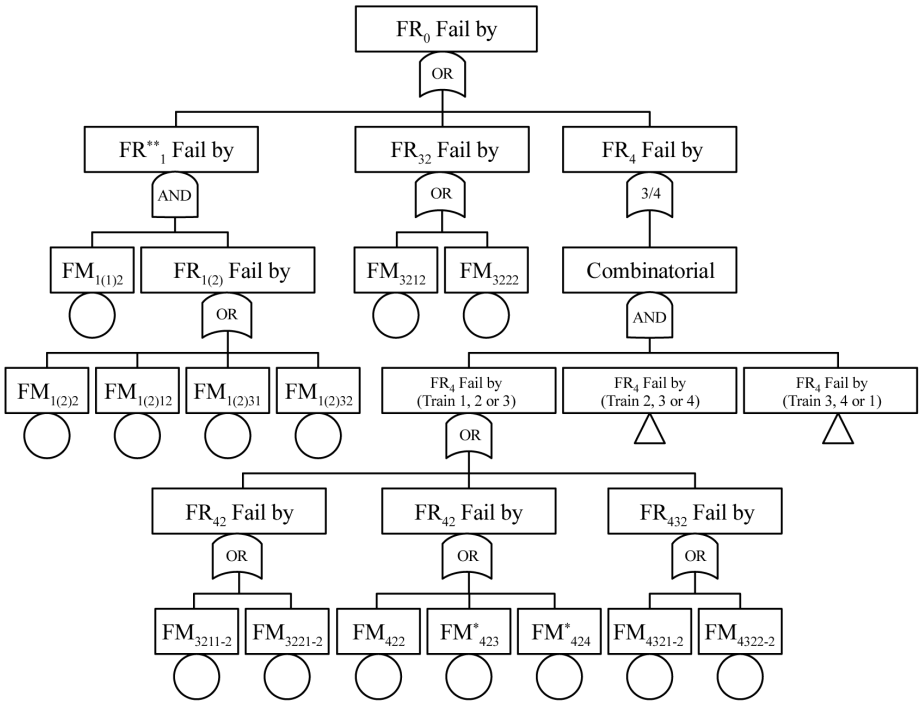
Table 3. Improved Design of a CHRS Using a Diverse Design

	FRs	**DPs**	**Modified FMs**	**Redundant Physical Parts**
1	Provide sufficient service water inventory	River		
1(1)		River (intake canal, Normal operation)		
1(1).1	Provide the force to pump up from river to higher canal	Circulating water pumping		8 trains
1(1).1.1	Provide pumping equipment	Circulating water pump	1. Negligible	
1(1).1.2	Provide pump driving source	Power circuit by off-site power	1. Loss of off-site power	
1(2)		River (intake canal, Drain operation)		
1(2).1	Provide the force to pump up from river to higher canal	Circulating water pumping		4 trains
1(2).1.1	Provide pumping equipment	Circulating water pump	1. Negligible	
1(2).1.2	Provide pump driving source	Power circuit by diesel power	1. Insufficient power to bus	Single unit
1(2).2	Monitor the level of intake canal	Level sensor	1. Sensor failure	
1(2).3	Isolate unnecessary service water	Condenser isolation		
1(2).3.1	Isolate the inlet of service water to condenser	Inlet on/off mechanism	1. Failure in power circuit, 2. Fail to close, 3. Failure in control circuit	MOV-CW-206A, C
1(2).3.2	Isolate the outlet of service water to condenser	Outlet on/off mechanism	1. Failure in power circuit, 2. Fail to close, 3. Failure in control circuit,	MOV-CW-200B, D

The final step is to generate a FT for the CHRS with alternative designs. Fig. 8 shows the final FT converted from the modified FR-DP decomposition incorporating the results in Table 2 and Table 3. The FT in Fig. 8 provides an identical minimal cutset to that analyzed in WASH-1400. It is clear, as the equality of design information while synthesizing or analyzing the CHRS was hypothesized. The essence of the proposed design framework is to share design information from an early design phase by making the synthesis and reliability check-up more interactive. The case study conceptually shows a technique that achieves this mission.

4. CONCLUSIONS

The purpose of this study is to propose a framework to enable close interaction between the synthesis and analysis processes, particularly a reliability analysis, in order to efficiently design safety-critical systems. It is believed that AD and FTA play indispensable roles during the design of safety-critical systems. While designing nuclear power plants, FTA is a mandatory requirement during the design processes. This study does not suggest FTA has to be induced from the products of AD; however, it was found that integrating AD and FTA into a single framework is a viable solution, as they compliment each other with their unique advantages. The synthesis process driven by AD involves much available information, thus it is possible to carry out FTA with less effort. In addition, it should be possible to obtain the same amount of insight from an FTA converted from AD as that from the FTA traditionally performed. The interactive design framework integrates the two methodologies. In contrast, FTA during the synthesis process allows a more feasible opportunity to discover



* 1 and 3, and 2 and 4 trains share the same physical parts respectively.
** See Table 3

Fig. 8. Final FT Converted from the Modified FR-DP Decomposition

design vulnerabilities by observing a system from the viewpoint of a failure domain. A survey on failure domain may be useful to complete missed sets of FRs and DPs.

ACKNOWLEDGEMENT

This work was supported by the Korea Research Foundation Grant (No. M01-2005-000-10048-0).

REFERENCES

[1] N. P. Suh, *Axiomatic Design: Advances and Applications*, Oxford University Press, USA (2001).
[2] US Nuclear Regulatory Commission, Reactor Safety Study, "An Assessment of Accident Risks in U.S. Nuclear Power Plants," WASH-1400, NUREG-75/014, USA (1975).
[3] US National Aeronautics and Space Administration, Probabilistic Risk Assessment of the Space Shuttle, "A Study of the Potential of Losing the Vehicle During Normal Operation," NASA-CR-197808, USA (1995).
[4] J.L. Herrmann and P.J. Wood, "The Practical Application of PRA: An Evaluation of Utility Experience and USNRC Perspectives", *Reliability Engineering and System Safety*, **24**, 1, 167 (1989).
[5] G.E. Apostolakis, "How Useful Is Quantitative Risk Assessment", ESD-WP-2003-05, Massachusetts Institute of Technology (2003).
[6] Axiomatic Design Solution, Inc., "The Axiomatic Design Decomposition Process, Internal Report," PN 60-10-002, USA (2004).
[7] S. Rudolph, "On a Mathematical Foundation of AD," *Proceedings of ASME Design Engineering Technical Conference and Computers in Engineering Conference*, Irvine, USA, August 18-22, 1996.
[8] J. Trewn and K. Yang, "The Relationship between System Functions, Reliability and Dependent Failures," *Proceedings of IEEE International Conference on System, Man, and Cybernetics*, San Diego, USA, September, 1998.
[9] J. Trewn, and K. Yang, "A Treatise on System Reliability and Design Complexity," *Proceedings of International Conference on Axiomatic Design*, Boston, USA, June 21-23, 2000.
[10] G. S. Shin, S. I. Yi, G. J. Park, J. W. Yi, Y. D. Kwon, "Calculation of Information Content in AD," *Proceedings of International Conference on Axiomatic Design*, Seoul, Korea, June 21-24, 2004.
[11] H. Kumamoto and E. J. Henley, *Probabilistic Risk Assessment and Management for Engineers and Scientists*, 2nd edition, IEEE press, USA (1996).
[12] US National Aeronautics and Space Administration, "Fault Tree Handbook with Aerospace Applications," USA (2002).
[13] Axiomatic Design Solution Inc., Acclaro™ DFSS, http://www.axiomaticdesign.com