Article citation info:
YANG D, REN Y, WANG Z, LIU L, SUN B. A novel logic-based approach for Failure Modes Mitigation Control and Quantitative System Reliability Analyses. Eksploatacja i Niezawodnosc – Maintenance and Reliability 2015; 17 (1): 100–106.

Dezhen YANG
Yi REN
Zili WANG
Linlin LIU
Bo SUN

A NOVEL LOGIC-BASED APPROACH FOR FAILURE MODES MITIGATION CONTROL AND QUANTITATIVE SYSTEM RELIABILITY ANALYSES

ORYGINALNA, OPARTA NA LOGICE METODA KONTROLI OGRANICZANIA PRZYCZYN USZKODZEŃ I ILOŚCIOWEJ ANALIZY NIEZAWODNOŚCI SYSTEMU

The core idea of reliability design is to mitigate the product's failure modes. However, for the cross-links among potential failure modes of a complex product, it is very difficult to establish the mapping relationship between failure modes mitigation and quantitative values of reliability, and the decision of failure modes mitigation have to be performed by virtue of experience, which always increase design period. In order to solve these problems, a novel logic-based approach for failure modes mitigation control and quantitative system reliability analyses is provided. Firstly, a hybrid of active and passive control process of reliability design is proposed. Secondly, a novel concept of failure modes correlation set (FMCS) and a determination approach based on deductive theory are presented. According to the changes in failure modes probabilities of occurrence, the reliability formulas of the components and assemblies are provided to depict the effects of failure mode mitigation on reliability of components and assemblies. And then the FMCS mitigation sequence is decided to determine reliability design activities. Thirdly, a closed control process of FMCS mitigation is provided integrated with logic decision method. By exposing the design of a helicopter fuel system, the present study demonstrates that all approaches are feasible, and the relationship between reliability parameters and qualitative design exists. Hence the failure modes mitigation could be controlled for the achievement of quantitative reliability requirements.

***Keywords**: failure, reliability, failure mitigation control, quantitative reliability analyses.*

Podstawowym problemem w procesie projektowania niezawodności jest ograniczenie przyczyn uszkodzeń produktu. Jednakże, w przypadku sieci połączeń pomiędzy możliwymi przyczynami uszkodzeń złożonego produktu, trudno jest ustalić mapę zależności pomiędzy ograniczaniem przyczyn uszkodzeń i ilościowymi wartościami niezawodności, a decyzje względem ograniczania przyczyn uszkodzeń muszą bazować na własnym doświadczeniu, co znacznie wydłuża okres projektowania. W celu rozwiązania powyższych problemów, zaproponowano oryginalną, opartą na logice, metodę kontroli ograniczania przyczyn uszkodzeń i ilościowej analizy niezawodności systemu. Na wstępie, zaproponowano mieszany proces aktywnej i pasywnej kontroli niezawodności projektu. Następnie, zaprezentowano oryginalną koncepcję zbioru korelacji przyczyn uszkodzeń (FMCS) i metodę oznaczania opartą o teorię dedukcji. Na podstawie zmian dotyczących prawdopodobieństwa występowania przyczyn uszkodzeń, określono wzory niezawodności części i układów w celu pokazania wpływu ograniczania przyczyn uszkodzeń na niezawodność części i układów. Określono następnie ograniczającą sekwencję FMCS, ażeby ustalić założenia dla projektowania niezawodności. Na koniec zaprezentowano zamknięty proces kontroli ograniczania FMCS w powiązaniu z logiczną metodą podejmowania decyzji. Analizując pod tym kątem projekt systemu paliwowego helikoptera, wykazano w niniejszej pracy przydatność wszystkich powyższych metod, jak również związek pomiędzy parametrami niezawodności a projektowaniem jakościowym. Dlatego też ograniczanie przyczyn uszkodzeń powinno być kontrolowane w celu osiągnięcia wymaganej niezawodności ilościowej.

***Słowa kluczowe**: uszkodzenie, niezawodność, kontrola ograniczania uszkodzeń, ilościowe analizy niezawodności.*

1. Introduction

Reliability plays an essential role as a major driver of life-cycle costs and has considerable influence on product performance, but its achievement is gradually, a well-defined program for the process is very important. In traditional reliability design process, the design activities are not parameter achieving oriented, they are mainly performed by virtue of experience. By using cybernetics, its process can be expressed as Fig. 1. In such way, the quantitative reliability were obtained, and the deviation could be determined by comparing them with reliability requirements by sensor unit, and then the failures could be pinpointed by execution unit. Simultaneously, designers give the improvements and apply them on product. Reliability engineers evaluate product's reliability after completing the functional design through reliability analysis [6, 12, 19], simulation [9, 18], test [2, 4] etc. The achievement of the requirements would be ensured according to the process. However, this process put the designers in a passive position as in order to meet the requirements. The development cycle is difficult to control, and designers may have to go through several iterations which may lead to enormous waste of time and money.

The newest reliability program standard GEIA-STD-0009 [8] proposes a new systematic process to include reliability in product design. The core idea is to progressively understand the loads and stresses of products at each level, to gradually recognize the failure

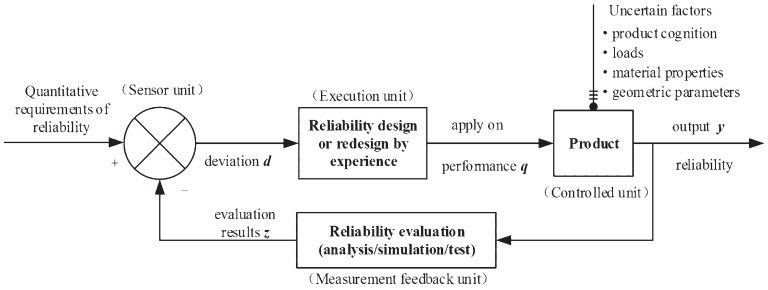

Fig. 1. The traditional reliability design process

modes and mechanism, and to actively mitigate the exposed failure modes. Therefore, mitigating the potential failure modes is the central task of reliability design. For a product with simple structure, designers should mitigate all the failure modes identified as possible. For a complex product, there are thousandths of potential failure modes. It is unrealistic to mitigate all the identified failure modes. Furthermore, cross-links exist among potential failure modes, the mitigation of a failure mode may cause occurrence of other failure modes, which make it very difficult to decide the sequence of mitigation, and have high risk to repeat the design cycle for many times. In order to control the failure modes mitigation to achieve reliability requirements quickly, it is necessary to construct a reliability design process.

In the literature about failure mode mitigation, current research mainly focused on the improvements for specific failure modes, such as run-time error mitigation in software [10], structural damage mitigation [3, 13], signal jamming [1, 14], sensor bias, drift, scaling, and dropout [5, 7]. Although these literatures show the idea of failure modes mitigation, they did not provide the control approach for failure modes mitigation on the basis of cybernetics. Furthermore, the cross-links among failure modes were often neglected when mitigating failure modes, which is unfavourable for optimized design [17].

The main purpose of this paper is to present a novel logic-based approach for failure modes mitigation control and quantitative system reliability analyses. This paper is organized as follows. Section 2 introduces the hybrid of active and passive control process based on the traditional passive reliability design process. In Section 3, an approach to determine the cross-links among failure modes and the mapping relationship between failure modes mitigation and quantitative requirements of reliability is presented in detail. The proposed approach is illustrated with the help of a fuel system example. Section 4 provides the control process of failure mode mitigation. Concluding remarks and future work are given in Section 5.

2. The hybrid of active and passive control process of reliability design

Aiming to shorten the development cycle and reduce the cost, reliability design should be carried out actively in the early stage of design. And then reliability and performance requirements could be achieved simultaneously.

2.1. The Active Process of Reliability Design

The active process of reliability design can be characterized as failure modes mitigation.

Definition 1: Failure modes mitigation [8] should be an active process, shown in Fig. 2. In this process, designers are active to identify potential failure modes of the product systematically. And then the improvements, operational compensatory provisions, diagnosis means are employed to eliminate the failure modes or reduce the failure modes' probabilities of occurrence according to their causes and severity. Furthermore, efficiency of the improvements applied should be validated.

This process is applicable to the product with sufficient prior knowledge. From the perspective of the achievement of quantitative reliability requirements, it is a problem to determine which failure modes to be mitigated. And then it is also a problem to control the achievement process of quantitative reliability requirements.

2.2. The Hybrid Control Process of Reliability Design

Integrating with the traditional process (shown in Fig. 1) and the active process (shown in Fig. 2), the paper proposes a new control process with the hybrid of active and passive one, shown in Fig. 3.

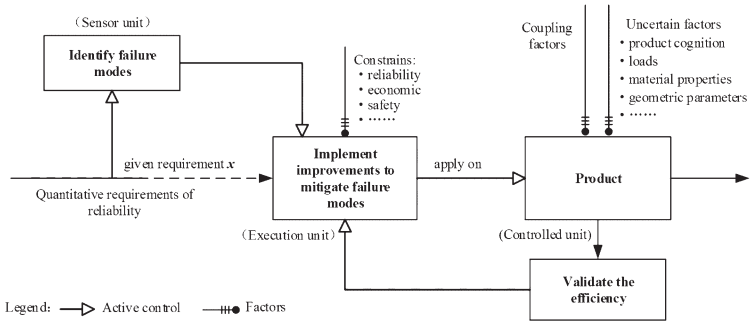

Fig. 2. The active process of reliability design

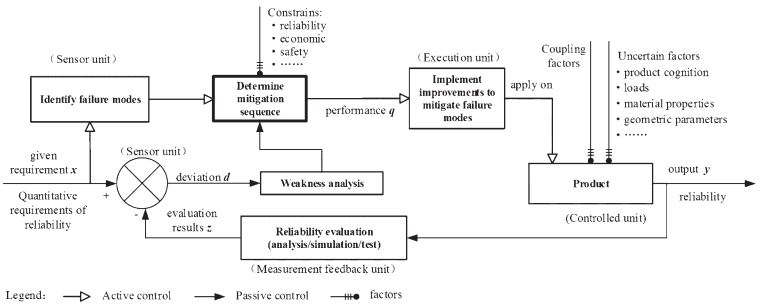

Fig. 3. The hybrid of active and passive control process of reliability design

Due to the complexity of products, failure modes would be unavoidably introduced with the design development. Therefore, designers should identify all possible failure modes through methods such as failure modes and effects analysis (FMEA), reliability simulation test. However, while designers recognize a specific failure mode, they should not take improvements to mitigate it immediately. Because different failure modes are not mutually independent - the mitigation of a failure mode may cause some others to be mitigated too, or/and may introduce some new failure modes simultaneously. And the effects of failure modes mitigation on reliability are also different. Therefore, designers must analyse the cross-links among different failure modes and determine the mitigation sequence at the outset.

Designers should be sure that the improvements are reasonable through simulation, principle analysis etc. before applying the improvements on product. After that, designers could implement the improvements on product in the order given by mitigation sequence, to eliminate the critical failure modes or reduce their probabilities of occurrence and severity.

Designers should further evaluate the product through reliability analyses, simulation, and tests. The purpose of those evaluations or revaluations is to determine the deviation between reliability achieve-

ments and its requirements under the current product configuration. If the deviation is positive (i.e., the evaluation result is greater than the required one), designers maintain the configuration, otherwise designers need to do further analysis to find out weaknesses, determine improvements and apply them on the product. In addition, there may be other disturbance factors, such as the uncertainty of product recognition, loads, material properties and geometric parameters. These factors may lead to the instability of the product. Therefore, designers should monitor the development, evaluate the product and feedback the results to the "sensor unit" in real-time.

For the hybrid process, the active process guarantees that critical failure modes will be identified timely, and the passive process can improve the product scheme exactly. Therefore, the design objective can be achieved with minimal resources and the design period would be shortened. The approaches for reliability design on the basis of the passive process have been presented. Restricted to the length, we do not give the details. The paper will focus on the active control process orienting to quantify achievement of reliability requirements.

3. Failure Modes Mitigation Sequence Decision

The determination procedure of failure modes mitigation sequence for the quick achievement of quantitative reliability requirements is as follows.

1. Identify the failure modes of the component and consider the new failure modes introduced by system integration, and the interrelationship among different failure modes, namely, to determine the failure modes correlation sets (FMCS).
2. Construct quantitative effect models of failure modes mitigation on reliability and calculate the effect of FMCS mitigation on reliability.
3. Determine the mitigating sequence of the failure modes according to the importance of reliability effect.

3.1. Determine FMCS based on Deductive Theory

To definite FMCS of f_i (the failure mode has been mitigated) proposed, we take the follows into consideration only.

1. The failure modes which are eliminated with f_i simultaneously
2. The failure modes that their probabilities of occurrence are reduced with f_i simultaneously
3. The failure modes which are introduced while f_i is mitigated

On the basis of constrains given above, the definition of FMCS can be achieved.

Definition 2: Hypothesize that there is a failure mode set $\mathbf{f}=\{f_1,f_2,\cdots,f_n\}$ for a product. Given one of the failure modes $f_i\in\mathbf{f}\left(i\in\{1,\cdots,n\}\right)$ has been mitigated by some improvements, such that $f_i\notin\mathbf{f}'$ (where $\mathbf{f}'$ is the new failure modes set for the product after failure modes mitigation) or its probability of occurrence is reduced. If $\exists\left\{f_{i_1},f_{i_2},\cdots,f_{i_m}\right\}\subset\mathbf{f}$ (m is the number of failure modes which are mitigated simultaneously with f_i), $\exists\left\{f_{j_1},f_{j_2},\cdots,f_{j_b}\right\}\subset\mathbf{f}'$ (b is the number of failure modes which are introduced with mitigation of f_i), and they satisfy following conditions:

1. $i_t\neq i\left(t=1,\cdots,m\right)$
2. $f_{i_t}\notin\mathbf{f}'$ or their probabilities of occurrence are reduced for $\forall t\in\{1,\cdots,m\}$
3. $f_{j_h}\notin\mathbf{f}\left(h=1,\cdots,b\right)$

Then the coupling set $\left\{f_i,f_{i_1},f_{i_2},\cdots,f_{i_m},f_{j_1},f_{j_2},\cdots,f_{j_b}\right\}$ is referred to as failure modes correlation set corresponding to f_i, denoted as FMCS_{fi}. Unambiguously, it can be referred to as failure modes correlation set abbreviation, denoted as FMCS.

3.1.1. The types of failure modes interrelationship

Assume that all the failure modes mitigation actions are reasonable and effective, the condition that one eliminated failure mode increasing some other failure modes' probabilities of occurrence are not under consideration. Based on this assumption, the interrelationship among different failure modes could be divided into the following types:

1. Type I (a failure mode is eliminated with another introduced): Although the failure mode f_1 is eliminated, some new failure modes $f_1^{eN},f_2^{eN},\cdots,f_{te}^{eN}$ are introduced, and the corresponding probabilities of occurrence are denoted by $\bar{\beta}_1^{eN},\bar{\beta}_2^{eN},\cdots,\bar{\beta}_{te}^{eN}$. Let type I FMCS be denoted as $\mathrm{FMCS_I}=\left\{f_1,f_1^{eN},f_2^{eN},\cdots,f_{te}^{eN}\right\}$.
2. Type II (concurrently eliminated): The failure mode f_1 is eliminated, and the failure modes $f_1^{ee},f_2^{ee},\cdots,f_E^{ee}$ are eliminated simultaneously. Denote type II FMCS as $\mathrm{FMCS_{II}}=\left\{f_1,f_1^{ee},f_2^{ee},\cdots,f_E^{ee}\right\}$, and the corresponding probabilities of occurrence are denoted by $\beta_1^{ee},\beta_2^{ee},\cdots,\beta_E^{ee}$. Note that the failure modes mitigated not necessarily belong to the same product (hereinafter the same, will not go into details).
3. Type III (one eliminated with another reduced): The failure mode f_1 is eliminated, and the failure modes probabilities of occurrence $f_1^{ed},f_2^{ed},\cdots,f_{De}^{ed}$ are reduced from the original $\beta_1^{ed},\beta_2^{ed},\cdots,\beta_{De}^{ed}$ to $\bar{\beta}_1^{ed},\bar{\beta}_2^{ed},\cdots,\bar{\beta}_{De}^{ed}$ respectively. Let type III FMCS be denoted as $\mathrm{FMCS_{III}}=\left\{f_1,f_1^{ed},f_2^{ed},\cdots,f_{De}^{ed}\right\}$.
4. Type IV (one reduced with another introduced): Although the failure mode probability of occurrence f_1 is reduced, some new failure modes $f_1^{dN},f_2^{dN},\cdots,f_{td}^{dN}$ are introduced, and the corresponding probabilities of occurrence are denoted by $\bar{\beta}_1^{dN},\bar{\beta}_2^{dN},\cdots,\bar{\beta}_{td}^{dN}$. Let type IV FMCS be denoted as $\mathrm{FMCS_{IV}}=\left\{f_1,f_1^{dN},f_2^{dN},\cdots,f_{td}^{dN}\right\}$.
5. Type V (concurrently reduced): The failure mode probability of occurrence f_1 is reduced, and meantime one of failure modes $f_1^{dd},f_2^{dd},\cdots,f_{Dd}^{dd}$ is also reduced from the original $\beta_1^{dd},\beta_2^{dd},\cdots,\beta_{Dd}^{dd}$ to $\bar{\beta}_1^{dd},\bar{\beta}_2^{dd},\cdots,\bar{\beta}_{Dd}^{dd}$ respectively. Let type V FMCS be denoted as $\mathrm{FMCS_V}=\left\{f_1,f_1^{dd},f_2^{dd},\cdots,f_{Dd}^{dd}\right\}$.
6. Type VI (one integrated with another introduced): Considering the interface failure modes, and the failure modes with high severity rank introduced by system integration, the corresponding probabilities of occurrence are denoted by $\bar{\beta}_1^{IN},\bar{\beta}_2^{IN},\cdots,\bar{\beta}_{tI}^{IN}$. Let type VI FMCS be denoted as $\mathrm{FMCS_{VI}}=\left\{f_1^{IN},f_2^{IN},\cdots,f_{tI}^{IN}\right\}$.

Since the interrelationships among failure modes are not identical, the FMCS is the union of Type I, II and III FMCS, namely $\mathrm{FMCS}=\mathrm{FMCS_I}\cup\mathrm{FMCS_{II}}\cup\mathrm{FMCS_{III}}$, denoted by $\mathrm{FMCS^E}$, or the union of Type IV and Type V FMCS, namely

$\mathrm{FMCS} = \mathrm{FMCS_{IV}} \bigcup \mathrm{FMCS_V}$, denoted by $\mathrm{FMCS^D}$. The Type VI FMCS is introduced by system integration, denoted by $\mathrm{FMCS^I}$, which is independent of Type I and Type V. It should be noted that designers should deeply analyze the mitigation of $\mathrm{FMCS^I}$. Therefore it could be further divided into two subsets: $\mathrm{FMCS^E}$ and $\mathrm{FMCS^D}$.

3.1.2. The determination of FMCS

In practical projects, it is very difficult to determine FMCS. The determination should be made according to the products working principles and fault propagation etc. The paper proposes an approach based on deductive theory [16] to determine the FMCS. It consists of two steps:

Step 1: Construct a logic tree of failure mode mitigation to determine the FMCS of a specific failure mode. In this step, a logic tree of the specific failure mode mitigation will be achieved. An example is shown in Fig. 4. It contains four layers, as follows:

1. Layer 1 (the mitigation object layer): specify mitigation object, namely choose the specific failure mode for mitigation.
2. Layer 2 (the mitigation procedures layer): according to Definition 1, classify the procedure of failure modes mitigation into two categories: the eliminated failure mode; and the reduced failure mode. Therefore, construct the layer by the logic "OR" between elimination of the failure mode and reduction of its occurrence probability.
3. Layer 3 (the improvements layer): according to the detailed failure mitigation procedures, including the reasons that lead to the occurrence of failure mode, determine the procedures and methods to construct the third layer. Namely, this layer is the relationship of AND, OR, CONDITION et al.
4. Layer 4 (failure modes correlation layer): according to the procedures and methods to improve the product, integrating product's functional principle and interrelationship, analyze all possible associated failure modes at the forth layer. In the logic tree, the paper adds a logic gate "failure modes correlation gate", denoted by "⩾". It not only denotes the AND logical relationship, but also shows the mitigation sequence of failure modes, namely from left to right.

Step 2: Determine FMCS. Identify the FMCS through descending method or ascending method according to the logic relationship implicated in the figure:

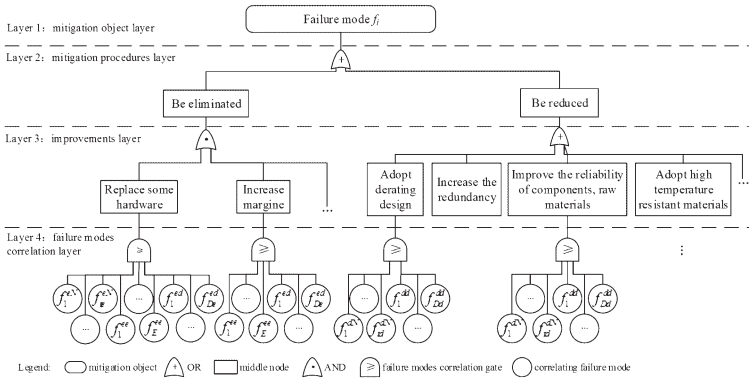

Fig. 4. An example of logic tree

3.2. Construct quantitative impact models of failure modes mitigation on reliability

The impact model shows the mapping relationship between failure modes mitigation and reliability parameter. It indicates the product's reliability after mitigation of a specific failure mode. According to the characteristic of Type II and Type III FMCS, they will be considered as the same type when constructing the impact models.

The common reliability parameters for complex products can be summarized as shown in Table 1.

Table 1. The common reliability parameters for complex products

Name	Applicable scope	
	assembly	component
failure rate	√	√
mean time between failures (MTBF)	√	√
mean time to failure (MTTF)		√
mean time between critical failures (MTBCF)	√	
mission reliability	√	

Notation: √ represents "applicable".

Considering the interrelationship types of failure modes, the impact models can be divided into two categories:

1. The impact models of the component-level reliability
2. The impact models of assembly-level reliability

3.2.1. The impact models of the component-level reliability

Let t denote a component. Assume its life is subjected to exponential distribution, namely its failure rate is a constant, and the failure mode probability of occurrence f_i is β_i. If f_i was mitigated, let $\bar{\beta}_i I_i \left(I_i = \begin{cases} 1 & f_i \text{ probability of occurrence was reduced} \\ 0 & f_i \text{ was eliminated} \end{cases} \right)$ denote the probability of occurrence. Then the failure rate of product t is given by:

$$\begin{aligned} \bar{\lambda}_t &= \lambda_t - \left(\beta_i - \bar{\beta}_i I_i\right) \\ &+ \left(1 - I_i\right)\left(\sum_{j=1}^{te} \bar{\beta}_j^{eN} - \sum_{j=1}^{E} \beta_j^{ee} - \sum_{j=1}^{De}\left(\beta_j^{ed} - \bar{\beta}_j^{ed}\right)\right) \\ &+ I_i\left(\sum_{j=1}^{td} \bar{\beta}_j^{dN} - \sum_{j=1}^{Dd}\left(\beta_j^{dd} - \bar{\beta}_j^{dd}\right)\right) \end{aligned} \tag{1}$$

If there are some failure modes contributing to other products, it should be calculated in accordance with the products respectively. The same is to the following equations.

MTBF of the product t is given by:

$$\mathrm{MTBF}_t = 1/\bar{\lambda}_t \tag{2}$$

3.2.2. The impact models of the assembly-level reliability

Suppose that the product P is comprised of H devices and does not take failure modes introduced by system integration into consideration, then the model of the assembly-level reliability influenced by component-level failure modes mitigation should be established first.

Then, combined with reliability theory, the expression of the P's failure rate is as follows:

$$\lambda_s = \sum_{t=1}^{H} \bar{\lambda}_t + \sum_{j=1}^{tI} \bar{\beta}_j^{IN} \tag{3}$$

In general, the assembly-level products are repairable. Correspondingly, the MTBF is given by:

$$\mathrm{MTBF}_s = 1/\lambda_s \tag{4}$$

The MTBCF is given by:

$$\mathrm{MTBCF_s} = \frac{\lambda_s}{\sum_{i=1}^{k}\beta_{CFi}} \times \mathrm{MTBF_s} \tag{5}$$

where $\frac{\lambda_s}{\sum_{i=1}^{k}\beta_{CFi}}$ denotes critical failure factor. β_{CFi} denotes the occurrence probability of the critical failure mode i after mitigation. k denotes the total number of critical failure modes.

If the lifetime of the complex product follows an exponential distribution, then its mission reliability is given by

$$R_s = e^{-T/\mathrm{MTBCF}_s} \tag{6}$$

where T denotes the mission duration.

In fact, new failure modes will be introduced by system integration, which could be mitigated by the designers. The impact models of reliability could be established according to the approach applied in components.

3.3. Order the FMCS mitigation sequence

Combining the impact models established above, designers can calculate the impact on reliability of different FMCS. According to the principle of maximization, designers can determine the failure modes mitigation sequence.

Theoretically, we should take all relevant reliability parameters into consideration. However, it can be seen from the equation (1) to (6) that reliability parameters are mutually dependent on each other. All other reliability parameters could be directly obtained from failure rate. Based on the attribution simplification rule [11], the mitigation sequence could be directly determined by failure rate. It is given by:

$$\left\{f_1, f_1^{eN}, f_1^{ee}, f_2^{ee}\right\} \succ \left\{f_2, f_1^{ed}, f_2^{ed}\right\} \succ \cdots \tag{7}$$

where $\succ$ denotes order relation, namely $\left\{f_1, f_1^{eN}, f_1^{ee}, f_2^{ee}\right\}$ should be mitigated prior to $\left\{f_2, f_1^{ed}, f_2^{ed}\right\}$.

3.4. Illustrative example

Here, a fuel system of a native helicopter was taken as an example to verify the feasibility of the approaches and models. The failure rate of the fuel system is 0.00000224(10^{-6}/h), and the failure rates of its components under current configuration are shown in Table 2.

Table 2. The failure rates of components of fuel system (section)

Components	Failure rate (10^{-6}/h)	Components	Failure rate (10^{-6}/h)
1 fuel tank	0.22	5 fuel supply hose assemblies	0.18
2 fuel boost pump	0.45	6 one-way valve	0.45
3 suction port assembly	0.25	7 drain valve	0.24
4 fireproof fuel supply hose assemblies	0.45		

Table 3. The results of fuel system's FMEA (section)

Components	Failure modes	S	β (10^{-6}/h)	After mitigation β (10^{-6}/h)	…
fuel tank	f_{11}: fuel tank wall leakage	IV	0.15	0.08	…
	f_{12}: fuel leakage after crash	II	0.07	0.04	…
fuel boost pump	f_{21}: fuel booster pump not working	II	0.12	0.08	…
	f_{22}: no flow	II	0.15	0	…
	f_{23}: pressure pulsation	II	0.18	0	…
suction port components	f_{31}: blocking	II	0.12	0	…
	f_{32}: leakage	II	0.13	0	…
fireproof fuel supply hose components	f_{41}: fuel leakage at inter faces	I	0.45	0	…
fuel supply hose components	f_{51}: fuel leakage at inter faces	II	0.18	0	…
one-way valve	f_{61}: blocking	II	0.15	0	…
	f_{62}: leakage	III	0.18	0.18	…
	f_{63}: seepage	II	0.12	0	…
drain valve	f_{71}: cannot open	III	0.12	0.08	…
	f_{72}: cannot turned off	IV	0.12	0.08	…

Notation: S denotes severity rank. β denotes a failure mode probability of occurrence.

By using FMEA, all possible failure modes can be identified, some of which are shown in Table 3. If a failure mode was mitigated, then its probability of occurrence (shown in column 5) could be predicted on the basis of NPRD 2011 [15] and experiment data.

1. Determine FMCS based on the deductive method

Since the severity rank of "f_{23}: fuel boost pump pressure pulsation" is II as in Table 3, and the correctness "optimization of inlet filter pore diameter" is feasible in technology and economy, so take it to be eliminated. According to the functional model of fuel system, failure modes "f_{22}: the fuel boost pump no flow", "f_{31}: suction port components blocking" and "f_{61}: one-way valve blocking" were eliminated simultaneously. According to the steps in section 3.1.2, the mitigation logic tree was achieved, as shown in Fig. 5. Furthermore, FMCS of f_{23} was then deduced. It was $\{f_{23}, f_{22}, f_{31}, f_{61}\}$. Similarly, other FMCSs were $\{f_{32}, f_{41}, f_{51}, f_{63}\}$, $\{f_{11}, f_{12}\}$, $\{f_{21}, f_{71}, f_{72}\}$.

2. Calculate the fuel system's failure rate after mitigation

After mitigation of FMCS, the failure rate of the fuel system was arrived according to Equation (1) and the data shown in Table 2 and 3, shown as follows:

1) $\{f_{23}, f_{22}, f_{31}, f_{61}\}$: 0.00000164
2) $\{f_{32}, f_{41}, f_{51}, f_{63}\}$: 0.0000013
3) $\{f_{11}, f_{12}\}$: 0.00000202
4) $\{f_{21}, f_{71}, f_{72}\}$: 0.00000212

According to the failure rates above, the failure modes mitigation sequence was determined as follows:

$$\{f_{32}, f_{41}, f_{51}, f_{63}\} \succ \{f_{23}, f_{22}, f_{31}, f_{61}\} \succ \{f_{11}, f_{12}\} \succ \{f_{21}, f_{71}, f_{72}\}$$

By adopting the proposed process to control the failure modes mitigation of the fuel system, the reliability objective was achieved through iterations, and the development cycle was greatly shortened.

4. The control process of failure modes mitigation

In line with the mitigation sequence, designers can mitigate the failure modes. A specific logic-based control process is proposed to guide the mitigation of FMCS, as shown in Fig. 6.

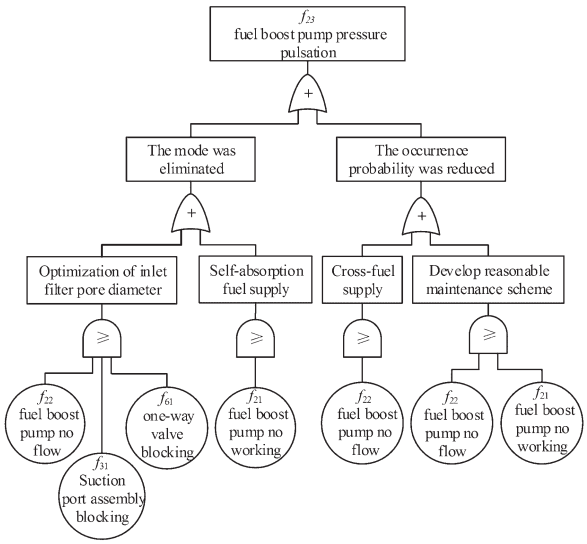

Fig. 5. The logic tree of fuel boost pump pressure pulsation mitigation

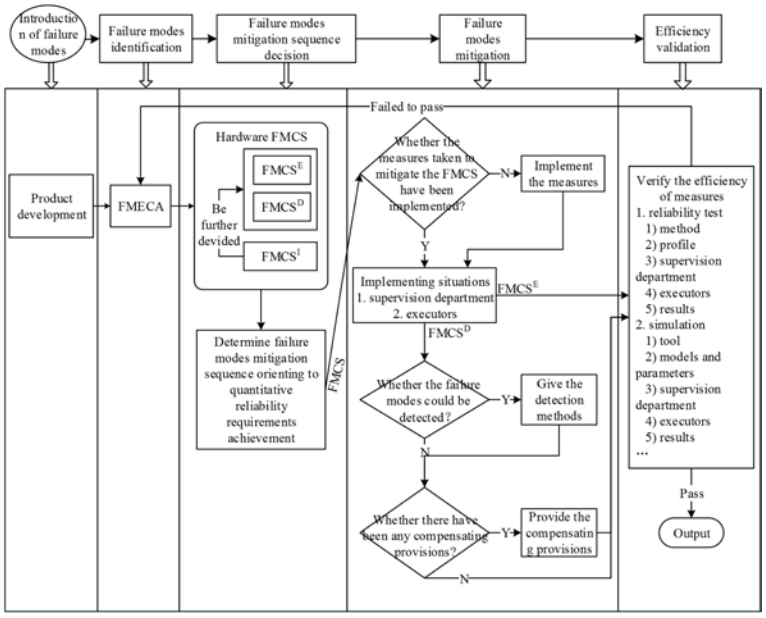

Fig. 6. The hardware FMCS mitigation process based on logic decision

For the FMCS, designers determine whether the improvements taken to mitigate the failure modes have been implemented. If the answer is "Yes", designers should record the implementing situations including supervision department and executors. If the answer is "No", designers should take the mitigating improvements, and track the process to make sure the failure modes are mitigated.

For the FMCS^{D}, designers should further determine whether the failure modes can be detected. If the answer is "Yes", designers should give the detection methods. Then, designers should determine whether there have been any compensating provisions. If the answer is "Yes", designers should also provide the compensating provisions.

Furthermore, designers should verify the efficiency of the mitigation improvements, detection methods and compensating provisions through reliability tests, simulation etc. Certainly, designers should also verify their final efficiency during operation stage, and make it guidance of the similar products design.

5. Conclusions

Failure modes mitigation is the core of reliability design process and should be well programmed. The pilot study had proposed a novel logic-based approach for failure modes mitigation control, the failure modes correlation sets (FMCS) had been defined and the links between qualitative and quantitative realization of reliability had been established. The approach takes the cross-links among failure modes into consideration and makes the novel hybrid control process, which constructs a bridge between the quantitative reliability parameters and the design and redesign activities, and would shorten the development cycle time. Hence, the provided approach is efficient for solving the decision problem of failure modes mitigation sequence.

The failure modes mitigation was illustrated for a fuel boost pump pressure pulsation, focusing on its typical failure modes. The study revealed that the proposed approach is efficient in this typical condition. In the future, more examples should be considered. Also, it is reasonable to develop correlation sets of coupled failure modes and impact model of its mitigation. And it is necessary for the authors to apply the approach repeatedly in more practical projects to provide sufficient evidence. The assumption that life of product is subjected to exponential distribution makes it easy to calculate the effect of failure mitigation on reliability. Nevertheless, the assumption may not reasonable, and the failure rates of the components of fuel system are not constant in fact. More work will be done to optimize the approach in the future.

References

1. Bhuiyan M Z H, Zhang J, Lohan E S, Wang W, Sand S. Analysis of multipath mitigation techniques with land mobile satellite channel model. Radioengineering 2012; 21(4): 1067-1077.
2. Chen Y X, Zeng Z G, Kang R. Validation methodology for distribution-based degradation model. J Syst Eng Electron 2012; 23(4): 553-559.
3. Chimpalthradi R A, Dattaguru B, Iyengar N G R. Adaptive control for structural damage mitigation. Global journal of researches in engineering: D aerospace engineering 2011; 11(5): 13-19.
4. Cotroneo D, Pietrantuono R, Russo S. Combining operational and debug testing for improving reliability. IEEE T Reliab 2013; 62(2): 408-423.
5. da Silva J C, Saxena A, Balaban E, Goebel K. A knowledge-based system approach for sensor fault modeling, detection and mitigation. Expert Syst Appl 2012; 39(12): 10977-10989.
6. Dui H Y, Si S B, Cai Z Q, Sun S D, Zhang Y F. Importance measure of system reliability upgrade for multi-state consecutive k-out-of-n systems. J Syst Eng Electron 2012; 23(6): 936-942.
7. Fong X Y, Kim Y S, Choday S H, Roy K. Failure mitigation techniques for 1T-1MTJ spin-transfer torque MRAM bit-cells. IEEE T VLSI Syst 2014; 22(2): 384-395.
8. GEIA-STD-0009, Reliability program standard for systems design, development, and manufacturing. ITAA 2008.

9. Johansson J, Hassel H, Zio E. Reliability and vulnerability analyses of critical infrastructures: comparing two approaches in the context of power systems. Reliab Eng Syst Saf 2013; 120: 27-38.
10. Jozef H, Teun H. Models in Software Engineering. Lecture Notes in Computer Science 2008; 5002: 225-236.
11. Komorowski J, Polkowski L, Skowron A. Rough sets: a tutorial. rough-fuzzy hybridization: a new method for decision making, Singapore: Springer-Verlag 1998; pp. 36-45.
12. Michael P. Product Reliability, Maintainability, and Supportability Handbook. 2nd ed. New York: Taylor & Francis Group, LLC, 2009.
13. Nayfeh A H, Hammad B K, Hajj M R. Discretization effects on flutter aspects and control of wing/store configurations. J Vib Control 2012; 18(7): 1043-1055.
14. Park D B, Shin D H, Oh S H, Kim H S. Velocity aiding-based anti-jamming method for GPS adaptor kits. T JPN Soc Aeronaut S 2011; 54(184): 130-136.
15. Reliability Information Analysis Center (RIAC). Nonelectronic Parts Reliability Data (NPRD-2011), 2011.
16. Tarski A. Introduction to logic and to the methodology of deductive sciences, 4th ed. NY: Oxford University Press, pp. 24-45, 1994.
17. Wang J W. Mitigation strategies on scale-free networks against cascading failures. Physica A 2013; 392(9): 2257-2264.
18. Xu S W, Wu X Y. Simulation method for reliability of TT&C mission with high redundancy and small time horizon. J Syst Eng Electron 2012; 23: 943-948.
19. Yang Q Y, Zhang N L, Hong Y L. Reliability analysis of repairable systems with dependent component failures under partially perfect repair. IEEE T Reliab 2013; 62(2): 490-498.

Dezhen YANG
Yi REN
Zili WANG
Linlin LIU
Bo SUN
School of Reliability and Systems Engineering
Beihang University
Xueyuan Rd., 100191 Beijing, China
E-mail: muyidz@126.com, renyi@buaa.edu.cn, wzl@buaa.edu.cn, liullcn@163.com, sunbo@buaa.edu.cn