Reliability Analysis of an Autonomous Underwater Vehicle Using Fault Tree

Hongli Xu  
State Key Laboratory of Robotics  
Shenyang Institute of Automation, CAS  
Shenyang, China  
e-mail: xhl@sia.cn

Guanman Li  
Institute of Information  
Shenyang Ligong University  
Shenyang, China  
e-mail: liguannan@sia.cn

Jian Liu  
State Key Laboratory of Robotics  
Shenyang Institute of Automation, CAS  
Shenyang, China  
e-mail: liuj@sia.cn

Abstract—Reliability is a very important specification for an autonomous underwater vehicle (AUV). The higher reliability can bring the shorter stop-working time and the lower maintenance cost. For a new AUV, reliability needs to be considered in advance during system design stage. This paper proposes a fault tree method for reliability analysis of the 4500m AUV. Firstly a fault tree model and its qualitative analysis are presented to determine the AUV’s bottlenecks. Then the reliability is demonstrated by the Monte Carlo simulation. Finally some experiences are discussed to improve the AUV’s reliability.

Keywords—AUV; reliability analysis; fault tree; Monte Carlo simulation

Autonomous underwater vehicle (AUV) is an automatic machine working autonomously without human intervention in underwater environment. It contains hundreds of components. Each component may fail unpredictably or even cause the AUV not to work. So it is strict on AUV’s reliability because of high expense for field trial and actual application. Reliability is a very important specification in designing a new heavy weight or large AUV. It needs to make a balance among cost, performance and maintenance. Reliability analysis method includes fault tree analysis (FTA), fault mode effect and compromise analysis (FMECA) and event tree analysis (ETA). Fault tree analysis is mainly used to find the basic causes in leading to the unexpected system failures or damaging danger events and became a common tool for fault diagnosis and reliability assessment.

Jia Zhe et al. built the fault-tree model of Dongfeng autonomous mobile robot based on the related theory of FTA and found out the checklists of faults for the timely and effective clearing faults [1]. Wang Gaiyun utilized FTA for the fault diagnosis of welding robots and gave its qualitative and quantitative analysis to improve the efficiency of diagnosis and reliability analysis [2]. For an AUV system, Bian Xinqian carried out an AUV’s fault tree and simulation model by combining FTA with Monte Carlo random sampling method [3]. Li Guoqi presented a FTA based method to evaluate runtime reliability in system level for an unmanned autonomous vehicle [4]. Cui Ying developed a database system combining with the remote monitoring, expert system, and intelligence diagnosis functions for crane and established the knowledge base with the aid of FTA [5]. Zheng Yanyi developed a fault tree automotive generation system based on decision lists [6]. Rafaul Ferdous presented a methodology for a fuzzy based computer-aided fault tree analysis tool [7]. K. Durda Rao proposed a dynamic fault tree approach using Monte Carlo simulation in probabilistic safety assessment [8].

This paper uses traditional fault tree method for reliability analysis of the 4500m AUV. Section 2 gives a brief introduction to the AUV and its components. Section 3 conducts the AUV’s fault tree model and qualitative analysis. In the following the reliability is demonstrated by Monte Carlo simulation, which shows that system design can meet the demands of reliability specification. Finally, some experiences are discussed to improve the AUV’s reliability.

I. THE 4500M AUV

The 4500m AUV is a shorter form of the deep-sea minerals autonomous exploration system, which is a 4500m rated AUV designed by Shenyang Institute of Automation, Chinese Academy of Sciences. It is equipped with many sensors including a magnetometer, side-scan sonar, a camera, CTD and a turbidimeter. The 4500m AUV will be mainly used to explore the polymetallic sulfide minerals in deep-sea hydrothermal area. The AUV system is divided into six subsystems: carrier structure, control, navigation, power and propulsion, acoustics, and detection. The whole system is composed of hundreds of components. Each component’s failure may lead to failure of its mission. So the reliability methods are necessary to grasp the bottlenecks of the whole system and take some corresponding improving measures in design and production. At the same time the methods can determine the breakdown reasons and direct the AUV’s online fault diagnosis and autonomy decision.

II. FAULT TREE MODEL AND QUALITATIVE ANALYSIS

A. Fault Tree Model

The 4500m AUV belongs to one of the complex systems. It is a complex process to assess the system state is normal or not. This paper firstly presents an AUV’s fault tree model based on

The research leading to these results has received indirectly funding from the Chinese National 863 Plan Program under the grant 2011AA09A102.
FTA shown as Fig. 1. The model maps the logic causation among the system failure and the components faults, external events, or the combination of them.

![Fig. 1. A simplified fault tree for the 4500m AUV. Rectangle means "top-level event" or "intermediate event". Bullet shape with groove tail means "or gate". Circle means "basic initiating events". Hexagon means "inhibit gate". Oval means "condition event".](image)

The destination of qualitative analysis is to determine the whole minimal cut sets.

B. Qualitative Analysis

The above fault tree is analyzed incompletely and need to further subdivide into bottom events for qualitative analysis. Taking the body equipment fault for example, its fault tree is shown in Fig. 2 and its symbols are explained in table I. The fault mode of a fault tree can be expressed by minimal cut sets. The destination of qualitative analysis is to determine the whole minimal cut sets.

The qualitative analysis process mainly includes:

- Step 1: operate the built fault tree with standardization, simplification and modularization methods.
- Step 2: calculate all of the minimal cut sets with down-to-top or top-to-down according to the fault tree structure.
- Step3: decompose the “modular minimal cut set” into “bottom-event minimal cut set” for qualitative importance comparison of the bottom events.
- Step4: On the base of the whole minimal cut set C_1, C_2, … , C_r, the top-level event can be denoted by:

\[ T = \sum_{j=1}^{r} \prod_{X_i \in C_j} X_i \]

\( \Sigma \) denotes union. \( \Pi \) denotes intersection. \( X_i \) denotes the jth bottom-level event.

![Fig. 2. The fault tree of the body equipment fault](image)
TABLE I. THE SYMBOLS IN THE BODY EQUIPMENT FAULT TREE

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>F₁</td>
<td>The power switch fault of altimeter</td>
</tr>
<tr>
<td>F₂</td>
<td>The communication fault of altimeter</td>
</tr>
<tr>
<td>E₁</td>
<td>The CTD fault with multiple reset failure</td>
</tr>
<tr>
<td>F₃</td>
<td>The power switch fault of acoustic modem</td>
</tr>
<tr>
<td>F₄</td>
<td>Acoustic modem without response</td>
</tr>
<tr>
<td>F₅</td>
<td>The leaking fault of side-scan sonar</td>
</tr>
<tr>
<td>F₆</td>
<td>The side-scan sonar fault</td>
</tr>
<tr>
<td>E₂</td>
<td>The fault continues for one second</td>
</tr>
<tr>
<td>E₃</td>
<td>Failed in turn off and reset for many times</td>
</tr>
<tr>
<td>G₁</td>
<td>The electronic cabin leaking fault of side-scan sonar</td>
</tr>
<tr>
<td>G₂</td>
<td>The control fault of the acoustic cabin power switch</td>
</tr>
<tr>
<td>G₃</td>
<td>The acoustic cabin leaking fault of side-scan sonar</td>
</tr>
<tr>
<td>G₄</td>
<td>The communication fault of the acoustic cabin</td>
</tr>
<tr>
<td>G₅</td>
<td>The acoustic power switch fault</td>
</tr>
<tr>
<td>G₆</td>
<td>The communication fault of the acoustic modem</td>
</tr>
<tr>
<td>xₙ</td>
<td>The internal fault of side-scan sonar</td>
</tr>
</tbody>
</table>

III. RELIABILITY ANALYSIS

A. Reliability Analysis

The following is focused on quantitative reliability analysis of the AUV system. At the same time the indexes of the system reliability can be calculated, the modeling and simulation can be done. When analyze the reliability, we mainly focus on three indexes of the system, namely the index \( R_i(t) \), the failure probability \( \lambda_i(t) \), and the mean time between failures (MTBF).

As can be known from above, the AUV system is a complex combination of machinery and electricity. Once damaged, the basic components cannot be fixed in the runtime. As the fault of each basic component is one of the minimum segmentation of the system faults, and the basic component failures are all independent of each other, the system can be regarded as a series one. Thus any failure of the basic components will result in the system failure.

Supposed that \( \tau_1, \tau_2, \cdots, \tau_n \) are the service lives of the \( n \) basic components, then the lifetime of the system is:

\[
\tau = \min(\tau_1, \tau_2, \cdots, \tau_n)
\]

And then the system reliability is:

\[
R_s(t) = P(\tau > t)
\]

\[
R_s(t) = P(\min(\tau_1, \tau_2, \cdots, \tau_n) > t)
\]

The failures of basic components are independent on each other, so the reliability is:

\[
R_s(t) = \prod_{i=1}^{n} P(\tau_i > t)
\]

Then it is:

\[
R_s(t) = \prod_{i=1}^{n} R_i(t)
\]

\( R_i(t) \) represents the reliability of the \( i \)th basic component.

The service life of each basic component obeys the distribution of the indexes, and the \( i \)th component’s characteristic parameter is \( \lambda_i(t) \), so:

\[
R_i(t) = e^{-\int_{0}^{t} \lambda_i(t) dt}
\]

\[
R_i(t) = \prod_{i=1}^{n} e^{-\int_{0}^{t} \lambda_i(t) dt} = e^{-\int_{0}^{t} \sum_{i=1}^{n} \lambda_i(t) dt}
\]

For the system in this study, the formula \( \lambda_i(t) = \lambda_i \) is a constant value, so the reliability can be:

\[
R_s(t) = \prod_{i=1}^{n} e^{-\int_{0}^{t} \lambda_i dt} = e^{-\int_{0}^{t} n \lambda_i dt}
\]

Then the failure probability of the system is:

\[
\lambda_s(t) = -\frac{d}{dt} R_s(t) = \frac{1}{R_s(t)} = \frac{1}{\sum_{i=1}^{n} \lambda_i(t)}
\]

The MTBF can be calculated by the formula:

\[
MTBF = \frac{1}{\lambda_s} = \frac{1}{\sum_{i=1}^{n} \lambda_i}
\]

From the above analysis, it can be concluded that the AUV system is a series one which is constituted of components whose lifetime is exponential distribution, and the service time of the AUV system can be regarded as a component whose service life obey the same distribution. And the failure rate of the system is the sum of the failure rates of all the basic components.

B. Simulation Process

To fulfill the simulation, a simulation method need to be chosen at first to get an estimation of the service time of the system, and then repeat the test many times to get a sample of the estimations of the system’s lifetime. Finally using the statistical method to analysis the sample, we can calculate the MTBF of the system, and evaluate its reliability. So there are two important parameters need to be set properly, namely the maximum simulation time and the times of simulation. The setting of them is illustrated later.

For each simulation, we need to get the failure time of each component first. Monte Carlo method is taken to random samples of the failure times of \( n \) basic components, and we can obtain a simple sample of \( n \) basic components’ lifetime. From the results above, the failure of basic components obey the distribution of indexes, and the character parameters can be gotten by accessing to relevant data, and combing with our actual situation. The parameters are shown in table II. Based on the known failure rate, the expected lifetime of the \( i \)th basic component is:
The equation:

\[ t_i = -\frac{1}{\lambda_i} \ln(1 - r_i) \]  

In the equation:

- \( t_i \) —— the expected lifetime of the \( i \)th component
- \( \lambda_i \) —— the failure of the \( i \)th component
- \( r_i \) —— a random number between 0 and 1

For \( r_i \) is a random number between 0 and 1, so the equation can be simplified into:

\[ t_i = -\frac{1}{\lambda_i} \ln r_i \]  

Using random numbers in the range of 0 and 1, these numbers are defined as \( r_i \). Then calculate in (12) with the known parameters \( \lambda_i \) and \( r_i \), we can get the failure time of the \( i \)th component. Repeated this process, we can get all the failure times of the 38 components.

### TABLE II. CHARACTERISTIC PARAMETERS

<table>
<thead>
<tr>
<th>Basic component CP</th>
<th>Basic component CP</th>
</tr>
</thead>
<tbody>
<tr>
<td>INS fault 0.25</td>
<td>Navigation unit leaking 2.5</td>
</tr>
<tr>
<td>DVL fault 8.1</td>
<td>Side-scan sonar fault 3.3</td>
</tr>
<tr>
<td>LBL fault 13</td>
<td>LBL fault 0.5</td>
</tr>
<tr>
<td>Voltage fault of control unit 4.03</td>
<td>Voltage fault of collision avoidance &amp; detection unit 2</td>
</tr>
<tr>
<td>Acoustic communication fault 2.5</td>
<td>User voltage fault of collision avoidance &amp; detection unit 2</td>
</tr>
<tr>
<td>Gyro fault 0.35</td>
<td>CTD fault 1.15</td>
</tr>
<tr>
<td>Control unit leaking 2.5</td>
<td>Electronic leakage of control unit 0.8</td>
</tr>
<tr>
<td>OBS+ORP fault 2.29</td>
<td>Methane detector fault 2.29</td>
</tr>
<tr>
<td>Wrong navigation status 0.4</td>
<td>Magnetometer fault 2.74</td>
</tr>
<tr>
<td>Control unit software fault 4</td>
<td>Graph fault 2.29</td>
</tr>
<tr>
<td>Propulsion unit leaking 2.5</td>
<td>Propulsion unit 0.45</td>
</tr>
<tr>
<td>Insulation fault of supervision unit 2.5</td>
<td>Electronic leakage of circuit 0.8</td>
</tr>
<tr>
<td>Steering motor fault 0.08</td>
<td>Forward sonar 0.38</td>
</tr>
<tr>
<td>Trough motor fault 0.68</td>
<td>Active collision avoidance 4</td>
</tr>
<tr>
<td>Collision avoidance and detection unit leaking 2.5</td>
<td>Network fault of collision avoidance &amp; detection unit 1.25</td>
</tr>
<tr>
<td>Battery unit 1 fault 1</td>
<td>Main battery fault 0.58</td>
</tr>
<tr>
<td>Battery unit 2 fault 1</td>
<td>Load rejection device fault 0.25</td>
</tr>
<tr>
<td>Battery unit 3 fault 1</td>
<td>Emergency device fault 0.33</td>
</tr>
<tr>
<td>VA 500P fault 1.7</td>
<td>Emergency unit fault 2.2</td>
</tr>
</tbody>
</table>

In order to get the samples, we need to get a group of random numbers in the range of 0 and 1 at first, and these numbers are defined as \( r_i \). Then calculate in (12) with the known parameters \( \lambda_i \) and \( r_i \), we can get the failure time of the \( i \)th component. Repeated this process, we can get all the failure times of the 38 components.

According to the simple sample of the basic components’ lifetime, we can get an estimation of the system’s lifetime in each simulation. Analyzing the fault tree, we can find out that the failure of any component will result in the failure of the system. So in the \( j \)th simulation, the estimation of the system’s lifetime is:

\[ T_j = \min_{\kappa \in \{1, n\}} (t_{ij}) \]

\( T_j \) —— life estimation of the system in the \( j \)th simulation

\( t_{ij} \) —— failure time of \( i \)th component in the \( j \)th simulation

Sorting the failure time of all the basic components, we should take the minimum of them as the failure time of the system in this simulation. If the expected time is larger than the maximum simulation time, the maximum simulation time is considered as the failure time of the system. Based on the proper simulation time, we can ensure that this situation will happen really rarely, and this approximate treatment will not lead to a distortion of the simulation result.

Repeat the above process for \( m \) times, and we will get \( m \) life estimations of the system.

Use interval statistics to process the \( m \) data. Setting the maximum simulation time as \( T_{\text{max}} \), and divide it into \( k \). Then estimate \( m(T_r) \), which represents the number of times for \( T_j \) fell into \( (T_{r-1}, T_r) \), \( r = 1, 2, \ldots, k \)

Based on the simulation results, the index of the reliability is calculated.

The mean-time-between-failure, namely MTBF:

\[ MTBF = \sum_{T_r=0}^{\infty} [T_r \cdot p_s(T_r)] \]

\[ p_s(T_r) = \frac{m(T_r)}{m} \]

For in the range of \( T_r > T_{\text{max}} \), \( p_s(T_r) \) is very small, so the equation can be approximated as:

\[ MTBF = \sum_{T_r=0}^{T_{\text{max}}} [T_r \cdot p_s(T_r)] \]

When MTBF is gotten, we can get \( \lambda_s \) according to (10). So the reliability of the system is \( t \):

\[ R_s(t) = e^{-\lambda_s t} \]

Failure rate of the system is \( F_s(t) \):

\[ F_s(t) = 1 - R_s(t) \]

The number of simulation times, namely \( m \), should not be too small; otherwise the accuracy of simulation result will be too low to ensure the result is convergent. But if \( m \) is too big, it will prolong the simulation time. After many times of test, it turned out that 1000 is the proper number.

\( T_{\text{max}} \), the maximum simulation time, should cover the estimations of the system’s lifetime. Analyzing the performance of all the basic components, we find out that LBL
system has the shortest life expectancy, which is 769 hours. So basically, $T_j$ is inside 1000 hours, and we set $T_{\text{max}}$ as 1000.

Setting $k$ as 10, the simulation result can meet the requirement.

According to the method, we carry out the simulate running. The simulating program flow chart is Fig. 3.

![Flow chart](image)

**Fig. 3. The flow chart of the simulation process**

C. Result of Simulation

After simulating for 1000 times, MTBF of the AUV is 180 hours. Compared to the designed runtime which is 100 hours, we can make sure that the system design satisfies its reliability requirement. The vehicle is designed to work for 30 hours, and at most 10 hours can be added in case of emergency, so it will be 40 hours in total. We evaluated its possibility for working for 40 hours continually, and the result is 0.8007, which is big enough for such a vehicle. At last, we draw the reliability distribution, as is shown in Fig. 4, and the distribution of failure probability, as is shown in Fig. 5. With their help, we can evaluate the vehicle’s reliability at anytime within 1000 hours.

![Reliability distribution](image)

**Fig. 4. The reliability distribution in the simulation**

![Failure probability](image)

**Fig. 5. The failure probability in the simulation**

IV. CONCLUSION AND DISCUSSION

Through qualitative and quantitative analysis we can make a conclusion that the 4500m AUV design can satisfy its reliability requirement. there are some experiences to discuss, including: 1) considering the AUV easy to use and easy to operate in software and structure design and improve design reliability; 2) take the software process control independently and testing fully for a long time to ensure the robustness of the software; 3) employ mature technology, off-the-shelf components and simpler structure for easy maintenance; 4) add appropriate redundancy and independent emergency unit for the AUV’s safety.

ACKNOWLEDGMENT

The authors would like to thank the 4500m AUV project group for providing the related data and pictures.

REFERENCES


