Reliability Analysis of Fault Tolerant Systems with Multi-Fault Coverage

GREGORY LEVITIN¹ and SUPRASAD V. AMARI²

¹Israel Electric Corporation Ltd., P. O. Box 10, Haifa, 31000 Israel
²Relex Software Corporation, 540 Pellis Road, Greensburg, PA 15601 USA

(Received on November 26, 2006)

Abstract: Fault-tolerance has been an essential architectural attribute for achieving high reliability in many critical applications of digital systems. Automatic fault and error handling mechanisms play a crucial role in implementing fault tolerance because an uncovered (undetected) fault may lead to a system or a subsystem failure even when adequate redundancy exists. Examples of this effect can be found in computing systems, electrical power distribution networks, pipelines carrying dangerous materials etc. Because an uncovered fault may lead to overall system failure, an excessive level of redundancy may even reduce the system reliability. Therefore, an accurate analysis must account for not only the system structure, but also the system fault & error handling behavior (often called coverage behavior) as well. The appropriate coverage modeling approach depends on the type of fault tolerant techniques used. The recent research literature emphasizes the importance of multi-fault coverage models where the effectiveness of recovery mechanisms depends on the coexistence of multiple faults in a group of elements, which are also called fault level coverage (FLC) groups, that collectively participate in detecting and recovering the faults in that group. However, the methods for solving multi-fault coverage models are limited, primarily because of the complex nature of the dependency introduced by the reconfiguration mechanisms. The paper suggests a modification of the generalized reliability block diagram (RBD) method for evaluating reliability indices of systems with multi-fault coverage. The suggested method based on a universal generating function technique computes the reliability indices of complex systems with multi-fault coverage using a straightforward recursive procedure. The proposed algorithm can be easily used in the case of hierarchical structure of FLC groups. Illustrative examples are presented.

Key Words: Fault-tolerant systems; Imperfect fault coverage; Reliability; Multi-fault coverage; Universal generating function

Nomenclature

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FLC</td>
<td>fault level coverage</td>
</tr>
<tr>
<td>RBD</td>
<td>reliability block diagram</td>
</tr>
<tr>
<td>u-function</td>
<td>universal generating function</td>
</tr>
</tbody>
</table>
pmf  probability mass function
\( R_k \)  reliability of FLC group \( k \)
\( p_j \)  reliability of element \( j \)
\( c_{ij} \)  fault coverage probability in the case of exactly \( j \) failures in FLC group \( k \)
\( n_k \)  number of elements in FLC group \( k \)
\( F_\theta \)  random number of failed elements in the set of elements \( \theta \)
\( \Theta _k \)  set of elements belonging to FLC group \( k \)
\( u(z) \)  u-function representing the pmf of \( F_{(j)} \)
\( U_\theta (z) \)  u-function representing the pmf of \( F_\theta \)
\( P_{kh} \)  probability that FLC group \( k \) contains exactly \( h \) failed elements
\( \pi \)  operator incorporating the uncovered failures into u-functions of FLC groups
\( \circ \)  composition operator over u-functions

1. Introduction

Fault-tolerant system design is aimed at preventing the entire system failure even when some of its elements fail. Usually, the fault tolerance is implemented by providing sufficient redundancy and using automatic fault and error handling mechanisms (detection, location, and isolation of faults/failures). Examples of fault tolerant techniques include error correcting codes, built-in tests, replication, and fault masking [1]. However, it is difficult to make a system as 100% fault tolerant, because the fault and error handling mechanisms themselves can fail [2]. As a result, some failures can remain undetected or uncovered, which can lead to the total failure of the entire system or its sub-systems [3]. Examples of this effect of uncovered faults can be found in computing systems, electrical power distribution networks, pipe lines carrying dangerous materials etc. [4].

The systems with imperfect fault coverage have been intensively studied in [4][13]. It was shown that the system reliability can decrease with increase in redundancy over some particular limit if the system is subjected to imperfect fault coverage [5]. As a result the system structure optimization problems arise. Some of these problems have been formulated and solved for parallel systems, k-out-of-n systems [4][6] and series-parallel multi-state systems [14].

The probability of successfully covering a fault (avoiding fault propagation) given that the fault has occurred is known as the coverage factor [2]. The models that consider the effects of imperfect fault coverage are known as imperfect fault coverage models or simply fault coverage models or coverage models [6][7]. Depending on the type of fault tolerant techniques used, the models are classified as [15]:

- Perfect Fault Coverage (PFC). The coverage factor is 1. Hence, the system can be analyzed using classical reliability analysis techniques, which do not consider the effects of coverage.
- Element Level Coverage (ELC). A particular coverage value is associated with each element. This value is independent of the status of other elements.
- Fault Level Coverage (FLC). The coverage value depends on the number of good elements that belong to a specific group (i.e., the status of other elements).
Reliability Analysis of Fault Tolerant Systems with Multi-Fault Coverage

- One-on-one Level Coverage (OLC). OLC is a special case of FLC where the coverage factor is 1 when the number of good elements in a specific group is greater than 2.

The ELC model is appropriate when the selection among the redundant elements is made on the basis of a self-diagnostic capability of the individual elements. Such systems typically contain a built-in test (BIT) capability. The FLC model is appropriate for modelling systems in which the selection among redundant elements varies between initial and subsequent failures. An example is a majority voting system among the currently known working elements. In the HARP terminology [16], ELC models are known as single-fault models, whereas the OLC and FLC models are known as multi-fault models. In the single-fault models, the effectiveness of recovery mechanisms depends on the occurrence of individual faults. A multi-element system with ELC can tolerate multiple coexisting single-faults. However, for any given fault, the success or failure of a recovery mechanism is independent of the status of other elements (or faults in the other elements). Therefore, the uncovered failures associated with single-fault models are also known as single-point failures. The multi-fault coverage models are used to accurately specify the effects of coexisting faults and effectiveness of fault & error handling mechanisms in the presence of these faults. In a multi-fault model, the effectiveness of recovery mechanism depends on the occurrence of multiple faults. Specifically, the effectiveness of recovery mechanism decreases with the increase in the number of coexisting faults. Multi-fault models have the ability to model a wide range of fault tolerant mechanisms that include the fault masking techniques that masks the effects of some non-isolated faults. Further, the probability of simultaneous presence of multiple faults is very small. Therefore, in most cases, the multi-fault models have good recovery capabilities as compared to single-fault models, hence; they have high coverage probabilities. A special type of multi-fault model is a near-coincident (critical-pair) fault model used in HARP, where the total system failure occurs as a result of two coexisting (not simultaneously occurring) faults. The near-coincident failure condition occurs when the system has already experienced one fault and is in the process of recovering from it when a second statistically independent fault occurs in another unit that is critically coupled to the unit experiencing the first fault.

Perfect fault coverage models, which are extensively studied in the literature, are actually special cases of the other three model types. Because OLC is a special case of FLC, there are effectively two classes of models (ELC and FLC) that need special attention. In the fault tolerant literature, ELC models have been studied for a long time. The landmark developments in solving these models include decomposition techniques (1983) [17], Markov chain-based solutions [16][18], multi-state combinatorial techniques [19], and a separable method called the Simple and Efficient Algorithm (SEA) [8], which uses conditional probabilities. As its name suggests, SEA provides the most simple and efficient method available for solving ELC models. Recently, several authors have extended the concepts of ELC models to account the effects of coverage in multi-state systems (MSS) [10][12][14].

Methods for solving FLC models (multi-fault models) are much more limited, primarily because of the complex nature of the dependency introduced by the reconfiguration mechanisms. Little progress has been made in analyzing multi-fault models. Time consuming Markov chain-based methods have been suggested in [16][20]. Amari [6] proposed a combinatorial method that is applicable only for k-out-of-n systems.
Recently, Myers [15] once again emphasized the need for the multi-fault models and proposed a combinatorial algorithm for their reliability evaluation. The main contribution of this algorithm is that as long as the system failure logic is represented using a combinatorial model, the inclusion of uncovered failures, resulting from either single-fault or multi-fault coverage models, does not require a complex Markov chain-based solution. Hence, one can solve both single-point failures and near-coincident failures using combinatorial models, which is another major breakthrough in the analysis of coverage models. The disadvantage of this method is its computational complexity. To produce correct results, the system reliability should be expressed in a sum of disjoint products (SDP) form that is grouped according to a specific combination of “number of good units from each FLC group”. Due to this restriction, it cannot be combined with efficient algorithms available for combinatorial reliability analysis.

In this paper, combining the concepts of Myers approach and a universal generating function, we propose an efficient algorithm to solve multi-fault coverage models (FLC and OLC models) using a straightforward recursive procedure. The proposed algorithm can be easily used in the case of hierarchical structure of FLC groups (any FLC group can be considered as an element of a higher level FLC group).

2. System Description

The system description and assumptions are:

- The system consists of several groups of elements (called an FLC group).
- The fault coverage (conditional probability that FLC group can recover given faults in the group occur) depends on the number of failed elements in this group.
- The uncovered failure of any element causes immediate FLC group failure, even in the presence of adequate redundancy.
- The FLC groups can compose a hierarchical structure: any FLC group can be considered as an element of a higher level FLC group, etc.
- Element failures are s-independent. The only dependency among the element failures is due to the uncovered failures caused by imperfect fault coverage mechanisms.
- An s-coherent combinatorial model (RBD) can be used to represent the combinations of covered element failures that lead to system failure (or success).

Therefore, the inputs for the reliability analysis are:

- A system reliability block diagram.
- A set of parameters describing the element reliability or time to failure behaviour.
- A set of FLC groups and corresponding fault coverage probabilities.

3. RBD Method for Multi-Fault Models

An efficient approach for reliability analysis of complex systems is based on a universal generating function (UGF) technique [21] that was first suggested by Ushakov [22]. This approach allows obtaining the performance distribution of complex multi-state systems using a generalized reliability block diagram method (recursive aggregating elements and replacing them by single equivalent ones). This paper suggests a UGF-based algorithm for evaluating reliability of arbitrary systems with multi-fault failure coverage.
3.1 Universal Generating Function (u-function) Technique

The u-function representing the pmf of a discrete random variable \( Y_j \) is defined as a polynomial

\[
u_j(z) = \sum_{h=0}^{k_j} \alpha_{jh} z^{y_{jh}},
\]

where the variable \( Y_j \) has \( k_j+1 \) possible values and \( \alpha_{jh} = \Pr \{ Y_j = y_{jh} \} \).

To obtain the u-function representing the pmf of a function of \( n \) independent random variables \( \varphi(Y_1, \ldots, Y_n) \) the following composition operator is used:

\[
U(z) = \bigotimes (u_1(z), \ldots, u_n(z))
\]

\[
= \bigotimes \left( \sum_{h=0}^{k_1} \alpha_{h1} z^{y_{1h}}, \ldots, \sum_{h=0}^{k_n} \alpha_{nh} z^{y_{nh}} \right)
\]

\[
= \sum_{h_1=0}^{k_1} \sum_{h_2=0}^{k_2} \cdots \sum_{h_n=0}^{k_n} \left( \prod_{i=1}^{n} \alpha_{h_i} z^{y_{ih_i}} \right)
\]

For example, the u-function representing the pmf of the function \( Y_1+\ldots+Y_n \) takes the form:

\[
U(z) = \bigotimes (u_1(z), \ldots, u_n(z))
\]

\[
= \bigotimes \left( \sum_{h_1=0}^{k_1} \alpha_{h1} z^{y_{1h1}}, \ldots, \sum_{h_n=0}^{k_n} \alpha_{nh} z^{y_{nh}} \right)
\]

\[
= \sum_{h_1=0}^{k_1} \sum_{h_2=0}^{k_2} \cdots \sum_{h_n=0}^{k_n} \left( \prod_{i=1}^{n} \alpha_{h_i} z^{y_{ih_i}} \right)
\]

The polynomial \( U(z) \) represents all of the possible mutually exclusive combinations of realizations of the variables by relating the probabilities of each combination to the value of function \( \varphi(Y_1, \ldots, Y_n) \) for this combination.

In our case u-functions can represent the pmf of random number of failed elements in any subsystem (FLC group). For subsystem consisting of single element \( j \) the number of failed elements \( F_{\{j\}} \) can be either \( 0 \) (with probability \( p_j \)) or \( 1 \) (with probability \( 1-p_j \)). This can be represented by the following u-function:

\[
u_j(z) = p_j z^0 + (1-p_j) z^1
\]

For a subsystem consisting of two elements \( j \) and \( h \) the total number of failed elements is \( F_{\{j,h\}} = F_{\{j\}} + F_{\{h\}} \). The pmf of this random number can be represented by u-function obtained using the following operator:

\[
U_{\{j,h\}}(z) = u_j(z) \bigotimes u_h(z) = [p_j z^0 + (1-p_j) z^1] \bigotimes [p_h z^0 + (1-p_h) z^1]
\]

\[
= p_j p_h z^0 + [p_j (1-p_h) + p_h (1-p_j)] z^1 + (1-p_h)(1-p_j) z^2
\]
Applying the following recursive procedure one can obtain the u-function representing the pmf of random number of failed elements in any subsystem (set of elements):

**Procedure 1.**

1. Find any pair of system elements belonging to the subsystem and obtain u-function of this pair using the composition operator \( \otimes \) over two u-functions of the elements.
2. Replace the pair with a single element having the u-function obtained in step 1.
3. If the system contains more then one element, return to step 1.

### 3.2 UGF Representation of Uncovered Failures

By applying the recursive procedure one obtains the u-function in the form

\[
U_{\theta_k}(z) = \sum_{h=0}^{n_k} P_{kh} z^h,
\]  

that represents the distribution of the number of failed elements in FLC group \( k \) consisting of \( n_k \) elements. Here \( P_{kh} \) is the probability that FLC group \( k \) contains exactly \( h \) failed elements. The unconditional probability that the subsystem with \( h \) failed elements can work is

\[
P_{kh} r_{kh} = P_{kh} \prod_{j=0}^{h} c_{kj},
\]

where \( c_{kj} \) is the fault coverage probability in the case of exactly \( j \) failures (\( r_k c_0 = 1 \), \( c_{nk} = 0 \) by definition) in FLC group \( k \). One can consider the case of uncovered failure as total failure of the FLC group in which all its \( n_k \) elements cannot work. The uncovered failure in the case of \( h \) failed elements occurs with probability \( P_{kh}[1-r_{kh}] \). Therefore this failure adds a term \( P_{kh}[1-r_{kh}] z^n \) to the u-function describing the distribution of failed elements in the subsystem. To incorporate the uncovered failures into the u-function one has to apply the following operator \( \pi \):

\[
U^{*}_{\theta_k}(z) = \pi(U_{\theta_k}(z)) = \pi(\sum_{h=0}^{n_k} P_{kh} z^h)
\]

\[
= \sum_{h=0}^{n_k} P_{kh} z^h + z^n \sum_{h=0}^{n_k} P_{kh} (1-r_{kh}) = \sum_{h=0}^{n_k} P_{kh}^* z^h.
\]

This u-function represents the unconditional distribution of number of failed components in FLC group \( k \). In order to obtain the subsystem reliability one has just to calculate the sum of coefficients corresponding to working states. For example, for \( m_k\)-out-of-\( n_k\):F subsystem, its reliability is equal to

\[
R_k = \sum_{h=0}^{m_k-1} P_{kh}.
\]
Reliability Analysis of Fault Tolerant Systems with Multi-Fault Coverage

Observe that the term $P_{kn}$ is never used in determining FLC group reliability because it corresponds to total group failure. The coefficients $P_{kh}$ for $h<n_k$ can be obtained using the following recursive procedure in accordance with (7) and (8):

$$P_{kh}^{*} = P_{kh}^{*} ; \quad P_{kh}^{*} = P_{kh}^{*} - \frac{P_{kh}}{P_{kh-1}} \forall h=1,\ldots,n_k-1$$ (10)

Now one can obtain the entire system reliability using the following procedure:

**Procedure 2.**

1. Define the $u$-functions $u_j(z)$ for each system element $j$ according to (4).
2. For any FLC group $k$:
   2.1 Apply Procedure 1 using composition operators $\otimes$ over $u$-functions $u_j(z)$ of the elements belonging to the FLC group and obtain $u$-function of the equivalent element representing this group in the form (6).
   2.2 Apply operator $\pi$ (8) over the FLC group $u$-function.
   2.3 Calculate the FLC group reliability $R_k$ using (9).
   2.4 Obtain the $u$-function representing random number of total failures of FLC group $k$ in the form $R_k^{*}z^0 + (1-R_k)z^1$.
3. Apply the same algorithm over $u$-functions of FLC groups belonging to higher level FLC group.

**4. Illustrative Example**

Consider a data storage system (Fig. 1) using Redundant Arrays of Inexpensive/Independent Disks (RAID) [23][24]. The disks have different reliabilities. Disks 1-5, 6-9, 10-12, 13-16, 17-20 and 21-24 compose arrays 1, 2, 3, 4, 5 and 6 respectively. The arrays have m-out-of-n reliability configuration and can be viewed as voting networks with perfectly reliable voters. Arrays 1-3 and 4-6 compose groups 7 and 8 respectively. Group 7 has parallel configuration, whereas group 8 has 2-out-of-3 configuration. The data storage system is available if both groups 7 and 8 are available (series configuration). The disk arrays and the groups of arrays are subject to uncovered failures of FLC type. The disks' probabilities as well as group configurations and coverage probabilities are presented in Table 1 (note that in m-out-of-n system $ckj=0$ by definition for any $j>n-m$ since the system cannot tolerate failure of more than $n-m$ elements).

The entire data storage reliability obtained for the given parameters using the algorithm presented above is $R=0.839474$. The reliability obtained for the same system with perfect fault coverage within arrays of disks (FLC groups 1-6) is $R=0.986336$. The reliability obtained for the system with perfect fault coverage in all FLC groups is $R=0.999904$. 
Gregory Levitin and Suprasad V. Amari

The presented algorithm can be easily used for finding bottlenecks in system fault detection/coverage mechanisms. For this purpose one can evaluate the relative influence of fault coverage probabilities in different FLC groups on the entire system reliability. The functions \( R(c_k) \) are presented in Fig. 2 (the rest of parameters take the values from Table 1). Having the values of \( R \) for different \( c_k \) one can easily calculate the slope of linear functions \( R(c_k) \).

One can see that the improvement of the coverage probability of FLC group 7 (group of arrays) has the greatest effect on the entire data storage system reliability \( \left( \frac{\partial R}{\partial c_7} = 0.347 \right) \). Among the arrays of disks the most beneficial is the improvement of the coverage probability of FLC group 6 \( \left( \frac{\partial R}{\partial c_6} = 0.124 \right) \). The least improvement of \( R \) can be achieved by increase of the coverage probability of FLC group 3 \( \left( \frac{\partial R}{\partial c_3} = 0.075 \right) \).
Table 1: Reliability Parameters of a Data Storage System

<table>
<thead>
<tr>
<th>FLC group (of arrays)</th>
<th>GC</th>
<th>CP</th>
<th>Array: FLC group (of discs)</th>
<th>Array configuration</th>
<th>No of disks</th>
<th>CP Disk reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3:5</td>
<td>5</td>
<td>C1:0.770</td>
<td></td>
<td></td>
<td>p1=0.857</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p2=0.847</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p3=0.836</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p4=0.826</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p5=0.816</td>
</tr>
<tr>
<td>7</td>
<td>1:3</td>
<td>4</td>
<td>C2:0.742</td>
<td></td>
<td></td>
<td>p6=0.866</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p7=0.861</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p8=0.853</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p9=0.848</td>
</tr>
<tr>
<td>3</td>
<td>1:3</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td>p10=0.866</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p11=0.857</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p12=0.848</td>
</tr>
<tr>
<td>4</td>
<td>2:4</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>p13=0.866</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p14=0.861</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p15=0.853</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p16=0.853</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p17=0.848</td>
</tr>
<tr>
<td>8</td>
<td>2:3</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>p18=0.866</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p19=0.857</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p20=0.848</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>p21=0.848</td>
</tr>
</tbody>
</table>

GC: Group Configuration, CP: Coverage Probability

Fig. 2: Functions R (c_{k1}) for the Data Storage System
5. Conclusions

The paper suggests a reliability block diagram method for evaluating reliability indices of systems with multi-fault coverage. This method based on a universal generating function technique computes the reliability of complex systems with multi-fault coverage using a straightforward recursive procedure. The proposed algorithm can be easily used in the case of hierarchical structure of FLC groups with series-parallel and $k$-out-of-$n$ configuration.

The approach allows reliability analysts to find bottlenecks in system fault detection/coverage mechanisms and to enhance the system reliability by improving the fault coverage in the most sensitive groups.

References


