Power Production Uncertainty Using Common-cause Failure Method

R. MEZIANE, M. AMARA, H. AMAR and S. BOUFALA
Electrotechnical Engineering Laboratory
University of MoulayTahar UMTS
BP 138 En Nasr Saida
ALGERIA
meziane22@yahoo.fr

Abstract: -Modern technology has generated a tendency to design and manufacture equipment’s and system of greater sophistication complexity and capacity. Serious implications of unreliable equipment behavior and systems have led to the desire for higher reliability. Thus, reliability has become one of the vital ingredients in system planning, design, development and operation. A dominant role in increasing a system’s reliability is played by common-cause failure, especially where the system must be working without interruption. The contribution of common cause failure to uncertainty in power production unavailability is discussed in this paper, with particular emphasis on the evaluation of common cause failure probabilities. A new computer program has been developed which models common cause failure for normally identical components by a specialization of multivariate exponential probability distribution which is characterized by a binomial failure rate. A program called Sim_CCF is developed with the consideration of the constant and binomial failure rate. The objective is to estimate the unavailability level of the system.

Key-Words: -CCF, Unavailability, Reliability, Binomial failure rate.

1 Introduction
In classical reliability modeling, it is assumed that the units fail independently. However, in a many systems, the occurrence of common-cause failures easily violates the assumption of independent failure of units [1]. A common-cause failure is defined as any instance where multiple units fail due to a single underlying effect [2] [3]. When this type of failures occurs, all other failures are triggered to constitute a complete system failure. Some of the reasons for the occurrence of common-cause failures are design deficiencies, operator and maintenance errors, operating environment, and external catastrophe [4]. A reliability analysis of system components which does not take into consideration the occurrence of common-cause failures may lead to optimistic prediction [5].

Generally, in the reliability analysis of any complex engineering systems an often significant and sometimes dominant aspect is a phenomenon that commonly known as “Common-cause Failure”. The term common-cause failure is widely employed by the technical community to describe events involving multiple failures that are the result of the same (single) cause. An important feature that makes common-cause failures to guard against is that the original connection between the particular units that failed almost in unison may not obvious at first sight [6]. The fundamental defect that brought about the common cause failure of two or more units may have arisen in the design phase of the equipment or the system. It may be due to unsuspected interdependence between various subsystems or components in a system where safety was sought by building in redundancy. Due to this uncertainty there is a definite requirement for further study of this reliability aspect, which has become more onerous as the need of systems having high reliability has increased. We have seen an explosive trend in technological evolution and complexity (e.g. space crafts, computerization, power production etc.) where the consequences of failures can become catastrophic and create international concern [9]. One facet of this problem has received considerable attention by this paper. This is the possibility that product or mission failure may occur due to some form of “common-cause failure” that is the simultaneous loss of multiple components paths in the electric generation system due to an underlying common mechanism, fault, or phenomena. In such instances the avoidance measures may be the very victims of such occurrence. Power system using redundancy techniques can tolerate a certain number and/or type of failure while continuing to maintain the required situation between the input and output conditions [8]. This is so when failures of individual components are independent. However, since the assumption of statistically-independent failure of redundant units is easily violated in practice, it is
necessary to include the occurrence of common-cause failures in the reliability analysis.

This paper describes the use of common-cause failure method to solve the unavailability problem involve the power production system, the main aim is to evaluate the system reliability using two popular method in the reliability field. The first one is based on the constant failure rate; the second one is based on the binomial failure rate. A combination of two methods is used in the last for more general cases.

2 Common-cause Failure Analysis

The probability of failure or unavailability of complex redundant system such as those found in the power generation may be seriously underestimated if contributions from “non random” failures sources are ignored. These common-cause (or common mode) contributions represent the dependent failure of more than one component (occurrence of more than one basic event) due to a single failure cause. Such dependent failures are termed secondary failures and are not quantifiable by the methods discussed previously for dependent failures.“A common cause failure is the result of events which because of dependencies, causes a coincidence of failure states of components in two or more separate components of a redundancy system failing to perform its intended function”.

Fussel[12] proposed the following four convenient classifications for common cause failures:

1- Failure of identical components,
2- Entire system rendered unavailable for any reason,
3- Failure of two or more “lines of defence”,
4- Loss of protection resulting in need for lost protection system (due to operator errors).

Epler[16] notes that notes that while many in the nuclear industry (and regulatory agency) have assumed that class 1 common cause failures predominate, actual operating experience, cumulating with the Tree Mile Island Unit #2 accident, have been mainly of the class 4 variety. Current regulatory philosophy is to minimize common cause failure susceptibility by periodic test and maintenance. While this may reduce common-cause failure contribution from classes 1, it has essentially no effect on power plant. Thus common-cause failure susceptibility in power plant safety systems may not be reduced as much as some have been led to believe.

Selections of the appropriate methods to be used in common-cause analysis depend on several factors including:

1- Size and scope of the problem,
2- Availability of experts (e.g. in human factor),
3- Type of analysis required,
4- Intrinsic modelling difficulties,
5- Accessibility to super computers,
6- Budgetary constraints.

A decision tree indicating available choices and methods has been developed by Xie[15]. Structured approaches to the quantitative evaluation of common cause failure analysis were first developed concertedly by Vaurio [8] and Espiritu[11]. Their methodologies considered only those common-cause failures which result in system failure. The future requirement that all min cut sets be known, a task essentially impossible for a large complex system, limited the application of these methodologies for relatively small systems. These methodologies are discussed below.

The following terminology is associated with common-cause failure analysis [10]:

1- A “significant common cause event” is a cause of secondary failure common to all basic events contained in a cut set,
2- A “common cause candidate” is a minimal cut set which contains a significant common cause event and all basic events contained in the cut set share a common physical location or susceptibility (i.e. no means exist to isolate the components from the failure cause). Note that a common location may exist for several components of the distance which physically separate the. If the components in the cut set share a common susceptibility (e.g. exposure to fire hazards or having a common manufacturer) then their physical location are inconsequential,
3- A “domain” represents that physical area in the plant within a common-cause failure may exist. Each domain is delineated by natural physical barriers, such as walls. Note that a barrier for one common failure cause may not be a barrier for some other (e.g. earthquake and fires).

Since many specific causes could result in a secondary component failure, generic failure causes categories have been implemented [20]:

1- Mechanical/thermal,
2- Electrical/radiation,
3- Chemical/miscellaneous.

These generic causes of failure are then assigned time-dependent occurrence rates in each domain where they may exist. Since each cause of secondary failure, when it occurs, may not cause the system to fail, a ranking system is used to determine the fraction of occurrence of the particular secondary failure cause which results in system failure. The common cause event may then be represented by a one element min cut set with failure rate determined as above and with an associated repair rate for the secondary failure. Common susceptibilities, such as common manufacturer, cannot be modeled by occurrence of repair rates; rather it is often assumed that a constant probability of failure is associated with such affected components. The multivariate exponential approach described in this paper offers method of assessing the contribution to unavailability from such factors.

Common-cause failure analysis consists of the following necessary steps:

1- Determine all the minimal cut sets for the system under study,
5- Obtain the qualitative secondary failure characteristics for every component (basic event) in each minimal cut set,
6- Automated search of the list of minimal cut sets to determine the common -cause failure candidates,
7- Perform quantitative analysis based on a probabilistic representation of the common-cause candidates,
8- Use the results of the qualitative and quantitative evaluation to make decision and conclusion regarding the system reliability and availability.

Consequently, while adopting the procedure of estimating

### 3 Common-cause Failure Approach

A more pertinent approach to system reliability is that of Vesely[13], who has developed techniques for estimating the parameters of Marshall-Olkin multivariate exponential distribution for modeling repairable common-causes. This model is specialized to allow the efficient estimation of parameters from sparse data and is discussed in detail below. An alternate approach[8] is the use of Markov models for repairable redundant systems, but will not be discussed here. Other methods for evaluating the reliability of systems (fault trees) which contain dependent components (basic events) may be found in [4]. The Marshall-Olkin model [13] is based on the following considerations:

1- Assume that each of a group of n components can fail from various causes,
2- Associate a vector \( v^* \), of order n with a specific failure cause. The elements of \( v^* \) have the value of one corresponding to those components which are simultaneously failed by the cause and the value of zero otherwise. A vector with only one non-zero entry therefore represents an “independent” failure cause,
3- A total of \( 2^{n-1} \) possible failure causes exist, each described by vector \( v^* \) with time to failure distribution:

\[
f_{v^*}(t) = \lambda_{v^*} e^{-\lambda_{v^*}t}
\]

(1)

Where: \( \lambda_{v^*} \) is the failure rate associated with \( v^* \). All possible failure causes are assumed to be competing, with observed failure due to the first failure cause which occurs.

Letting:

\( T_i: \) The time to first failure for component i;

\( g_i(t) : \) The exponential distribution for component I with failure rate \( \lambda_i \);

\( g_{ij}(t) : \) The exponential distribution for the time to simultaneous failure of component i and component j with failure rate \( \lambda_{ij} \);

Then:

\[
F(t_1, t_2, ..., t_n) = 1 - \Pr[T_i > t_1, T_j > t_2, ..., T_n > t_n]
= \prod_{i=1}^{n} \Pr[ g_i(t_i) = 0; g_{ij} \left( \max(t_1, t_2) \right) = 0; \ldots; g_{i,n} \left( \max(t_1, t_2, ..., t_n) \right) = 0] \tag{2}
\]

For all: \( i=1, ..., n; l \leq j \leq k \leq n \). This may be equivalently expressed as:
If the components are identical then this expression becomes:

$$F(t) = 1 - e^{-\left(\sum_{i=1}^{n} \lambda_i t - \sum_{i=2}^{n} \lambda_i \max(t_i, t_2) - \cdots - \max(t_1, \ldots, t_n)\right)}$$

(3)

For example, the probability of failure by time $t$ for two identical components is:

$$F(t) = 1 - e^{-\left(-\lambda_1 t - \lambda_2 t\right)}$$

(4)

This correspond to the failure cause vectors $v = [0,0]$; $v = [0,1]$; $v = [1,1]$. This expression may be simplified by using the first order approximation for the exponential reliable components (assuming no repair):

$$F(t) \approx Q(t) = (\lambda_1 t)^2 + \lambda_{12} t$$

(5)

For reparable components, the average unavailability $U$ is:

$$U = \left(\lambda_1 \mu_1\right)^2 + \lambda_{12} \mu_{12}$$

(6)

Where $\mu_1$ and $\mu_{12}$ are the average repair times for the individual component failure and the common-cause failure respectively.

Veseley[17] developed two techniques for estimating the parameter $\lambda_1$, $\lambda_{12}$ and $\lambda_i$ in general. These techniques are based on the following assumptions:

1. Common-cause failure occur at the same time,
2. Whenever failures occur they are repaired immediately and reoccur with identical time to failure distribution,
3. That the component population has been selected such that the failure rate $\lambda_{v\cdot}$ depend only on the number of components failed:

$$\lambda_{v\cdot} = \lambda_v \quad v = 1, \ldots, n$$

(7)

Where:

$v$ is the total number of components simultaneously failed by the cause. This implies that the components are similar and subject to similar failure causes. Veseley terms this assumption for the homogeneous model and notes that identical components in the same environment or whose failures are caused by the same maintenance error constitute a population for which such a model applies.

For this homogeneous model, Veseley developed the following expression for the failure rate corresponding to $I$ specific components failing and $I$ specific component not failing without restrictions on the remaining $n-i-j$ components:

$$\lambda_{ij} = \sum_{k=0}^{n-i-j} \binom{n-i-j}{k} \lambda_{i+k} \quad 1 \leq i + j \leq n$$

(8)

If only specific components failures are of interest, then this expression becomes:

$$\lambda_{i0} = \sum_{k=0}^{n-i} \binom{n-i}{k} \lambda_{i+k} \quad 1 \leq i \leq n$$

(9)

Two methods for estimating $\lambda$ are then given by Veseley assuming:

1. A constant common failure rate,
2. Binomial failure rate.

The first one assumes that common cause failure rates are independent of failure numbers: $\lambda_i = \lambda$ when $v \geq v_i$ and without restriction on $\lambda_i$ for $v < v_i$. This equality applies when common causes are equally likely to affect any combination of components. The most frequently observed number of failures under this assumption is approximately $n/2$.

$\lambda$ is then evaluated form the following expressions:

$$\hat{\lambda} = \frac{N_n}{KT}$$

(10)

Where: $T$ is the total time operational.

$$K = \sum_{k=0}^{n-1} \binom{n}{k}$$

(11)

This yield the following expression for $\hat{\lambda}_{i0}$:

$$\hat{\lambda}_{i0} = \hat{\lambda} 2^{i-j} \quad i \geq v_i$$

(12)
These estimates apply to single population of components, although they may be extended to m populations of similar common-cause which are removed from one another. Random maintenance errors which could equally affect any specific components and manufacturing defects which could be present equally any specific components are examples of common-mode failures causes for which common failure rate is applicable.

The second assume that the common-cause failure rate can be factored into an overall occurrence rate and “detailed effect” probability. From the assumption that given a common-cause failure has occurred, the probability of failing from the common-cause is a constant \( p \) yields the following expression for the common-cause failure rate:

\[
\lambda_v = \frac{\hat{\lambda}}{C} p^v (1-p)^{n-v} \quad v \geq v_i
\]  

(12)

Where:

\[
\hat{\lambda} = \sum_{i=v}^{n} \binom{n}{v} \lambda_v
\]

And:

\[
C = \sum_{i=v}^{n} \binom{n}{v} p^i (1-p)^{n-v}
\]

Theses equations yields the following estimate for \( \lambda_{i0} \):

\[
\lambda_{i0} = \frac{\hat{\lambda}}{C} p^i
\]  

(13)

Where:

\( \hat{\lambda} \) is estimated form the following expression:

\[
\hat{\lambda} = \frac{N_v}{T} \quad \text{or more simultaneous failures}
\]

(13)

Two approaches are used for estimating the binomial parameter:

1- Standard maximum likelihood techniques,
2- Poisson approximation to the binomial distribution.

5 Illustrative Example

Let consider the western Algerian power generation system characterized by the following:

1- Terga: Three groups of 400 Mw,
2- Ravin Blanc: Two groups of 168 Mw,
3- Mersa El hadjaj: five groups of 168 Mw,
4- Tiaret and Naama: Contains the equivalent sum of four groups of 168 Mw.

Unfortunately some data have been used to specify the scenario of the common-cause failure.

1- Failure rate model to be evaluated = 0.2,
2- The number of simultaneous failures considered = 20,
3- The generic component population size = 11,
4- The number of population in which common-cause failure information is to be input = 1,
5- The number of simultaneous failures for which parameter are to be maximized = 3,
6- The maximum number of simultaneous failures considered = 2,
7- The maximum number of simultaneous failures provided in output calculation = 20,
8- The population number = 1,
9- The operational time considered = 6840,
10- The mean time between tests = 720.

The followings results are obtained:

1- Common-cause failure occurrence rate = 0.1157.10^{-3},
2- Constant failure parameter = 1.1050. 10^{-3},
3- Constant failure rate = 1.047. 10^{-7},
4- Binomial failure parameter = 2.2872. 10^{-7},
5- Binomial failure rate normalisation parameter = 7.3575. 10^{-1}.

The common-cause failure rates and availability for different constant failure rate case are the following tables:
Recent Advances in Energy, Environment and Development

TABLE I. COMMON-CAUSE FAILURE RATES AND AVAILABILITY FOR THE CONSTANT FAILURE RATE CASE

<table>
<thead>
<tr>
<th>Failures</th>
<th>Failure rate per hour</th>
<th>Unavailability per demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5.363.10⁻⁶</td>
<td>1.931.10⁻⁶</td>
</tr>
<tr>
<td>2</td>
<td>2.681.10⁻⁶</td>
<td>9.653.10⁻⁷</td>
</tr>
<tr>
<td>3</td>
<td>1.341.10⁻⁶</td>
<td>4.827.10⁻⁷</td>
</tr>
<tr>
<td>4</td>
<td>6.704.10⁻⁷</td>
<td>2.041.10⁻⁷</td>
</tr>
<tr>
<td>5</td>
<td>3.352.10⁻⁷</td>
<td>1.207.10⁻⁷</td>
</tr>
<tr>
<td>6</td>
<td>1.676.10⁻⁷</td>
<td>6.033.10⁻⁸</td>
</tr>
<tr>
<td>7</td>
<td>8.379.10⁻⁸</td>
<td>3.017.10⁻⁸</td>
</tr>
<tr>
<td>8</td>
<td>4.190.10⁻⁸</td>
<td>1.508.10⁻⁸</td>
</tr>
<tr>
<td>9</td>
<td>2.095.10⁻⁸</td>
<td>7.541.10⁻⁸</td>
</tr>
<tr>
<td>10</td>
<td>1.047.10⁻⁸</td>
<td>3.771.10⁻⁸</td>
</tr>
</tbody>
</table>

TABLE II. COMMON-CAUSE FAILURE RATES AND AVAILABILITY FOR THE BINOMIAL FAILURE RATE CASE

<table>
<thead>
<tr>
<th>Failures</th>
<th>Failure rate per hour</th>
<th>Unavailability per demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>8.229.10⁻⁶</td>
<td>2.963.10⁻⁷</td>
</tr>
<tr>
<td>2</td>
<td>1.882.10⁻⁶</td>
<td>6.776.10⁻⁷</td>
</tr>
<tr>
<td>3</td>
<td>4.305.10⁻⁶</td>
<td>1.550.10⁻⁷</td>
</tr>
<tr>
<td>4</td>
<td>9.846.10⁻⁷</td>
<td>3.545.10⁻⁸</td>
</tr>
<tr>
<td>5</td>
<td>2.522.10⁻⁷</td>
<td>8.107.10⁻⁸</td>
</tr>
<tr>
<td>6</td>
<td>5.151.10⁻⁸</td>
<td>1.854.10⁻⁹</td>
</tr>
<tr>
<td>7</td>
<td>1.178.10⁻⁸</td>
<td>4.241.10⁻⁹</td>
</tr>
<tr>
<td>8</td>
<td>2.694.10⁻⁹</td>
<td>9.700.10⁻¹⁰</td>
</tr>
<tr>
<td>9</td>
<td>6.163.10⁻¹⁰</td>
<td>2.219.10⁻¹⁰</td>
</tr>
<tr>
<td>10</td>
<td>1.409.10⁻¹¹</td>
<td>5.074.10⁻¹¹</td>
</tr>
</tbody>
</table>

TABLE III. UNAVAILABILITY CHARACTERISTICS FOR ALL COMBINATIONS

<table>
<thead>
<tr>
<th>Failures</th>
<th>Failure rate per hour</th>
<th>Unavailability per demand</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>4.372.10⁻³</td>
<td>1.574.10⁻²</td>
</tr>
<tr>
<td>2</td>
<td>3.889.10⁻³</td>
<td>1.400.10⁻²</td>
</tr>
<tr>
<td>3</td>
<td>2.307.10⁻³</td>
<td>8.304.10⁻³</td>
</tr>
<tr>
<td>4</td>
<td>9.576.10⁻⁴</td>
<td>3.447.10⁻⁴</td>
</tr>
<tr>
<td>5</td>
<td>4.733.10⁻⁵</td>
<td>1.704.10⁻⁵</td>
</tr>
<tr>
<td>6</td>
<td>1.719.10⁻⁶</td>
<td>6.187.10⁻⁶</td>
</tr>
<tr>
<td>7</td>
<td>1.593.10⁻⁷</td>
<td>5.733.10⁻⁷</td>
</tr>
<tr>
<td>8</td>
<td>2.449.10⁻⁸</td>
<td>8.816.10⁻⁸</td>
</tr>
<tr>
<td>9</td>
<td>5.228.10⁻⁹</td>
<td>1.882.10⁻⁹</td>
</tr>
<tr>
<td>10</td>
<td>1.409.10⁻¹⁰</td>
<td>5.074.10⁻¹⁰</td>
</tr>
</tbody>
</table>

6 Conclusion

In this paper we formulated the problem of common-cause failure for power generation system. In this work we focussed on the evaluation of unavailability for selected failures where the common-cause probability is an essential part of complete reliability of risk assessment. The sim CCF computer programs developed facilitate theses evaluations. It is more useful for estimation of generic common-cause failure probabilities.

These output results can be used as an input for uncertainties analysis for the bounds determination in the case of simultaneous failures for a future research work. Many cases do exist, however, where Sim CCF will be useable and provide important quantitative results for common-cause failure evaluation.

References:


