Improve Your Knowledge (IYK)

Reliability and Fallibility Analysis of Complex Systems

- *Berquó, Jolan Eduardo – Electronic Eng. (ITA)*
- *Aerospace Product Certifier (DCTA/IFI)*
- *Government Representative for Quality Assurance – RGQ (DCTA/IFI)*
- *Post-graduated in Reliability Engineering and System Safety Engineering (ITA)*
- *Specialization in Systems Engineering and Analysis (Italy)*
- *Participation in the joint development program (Brazil-Italy) for the AM-X military fighter-bomber aircraft*
- *Experience of one decade as an engineer responsible for off-line maintenance of electronic systems and aircraft instruments.*

jberquo@dcabr.org.br /jberquo@gmail.com

IYK 72– May, 13 2019

In our initial steps in the study of Reliability or Fallibility or Unreliability of a system, we usually start with analyzes of simple systems, ie systems with block diagrams (units) in series or in parallel, or both, that is, with serial-parallel block diagrams. The mathematical expressions used in these diagrams are already well known to us. However, there are systems whose diagrams are not only series or parallel, nor serial-parallel; They are so-called complex systems. In these cases, we must use other resources to resolve them. This is the theme of this IYK. We must say that the subject requires reasonable attention.

Let us first recall that Reliability is the probability that a system will operate successfully for a time t, under certain conditions, being represented by the letter R.

Let us then consider, at the outset, the block or unit diagram in Fig. 1. It is a simple serial-parallel diagram.

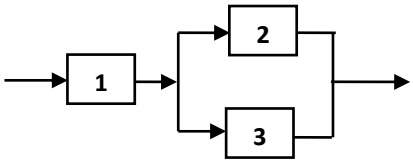

Fig. 1 - Example of serial-parallel system

To facilitate the calculation of the reliability of the system, we start with the parallel branch (2, 3), considering that (2) and (3) perform the same function, as in aviation redundancies. The failure of the entire parallel branch will only occur if there is a failure of (2) and (3). Thus, the fallibility F (t) of the parallel branch is $F_P = F_2.F_3$, where F_2 and F_3 are the fallibility of (2) and (3), respectively. A block P, in series with block (1), is then produced, as in figure 2.

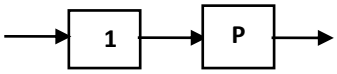

Fig. 2 - Serial system resulting from the system of Fig. 1

Taking into account that R + F = 1, the reliability of the block P will be given by $R = 1 - F_P$. Therefore, the exact Reliability of the system is:

$$R_S = R_1 . R_P = R_1 . (1-F_P)$$

Simple, right? Now, let's look at the block diagram of Fig. 3. Now, we have a complex system.

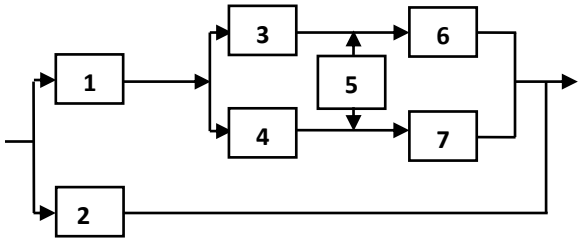

Fig. 3 – Example of Complex System

Note that if there were no unit 5, the system would be a series-parallel type with three paths from input to output, namely: (1, 3, 6), (1, 4, 7) and (2). But, with the presence of unit 5, we have 5 trajectories between those points: (1, 3, 6), (1, 4, 7), (1, 3, 5, 7), (1, 4, 5, 6) and (2).

How to determine the System Reliability? Complicated, no? Yeah, but fortunately, there are always people thinking about serious things. One of them was Shooman, M. L. (V. Ref. 1), who in 1990 presented a method to solve this type of problem. This is the so-called Path-Tracing Method.

The important entities of the method are the so-called path sets and the cut sets. A path set (PS) is a set of units that form a serial connection between the input and the output of the system, following the arrows of the path considered. (1, 3, 6), (1, 4, 7), (1, 3, 5, 7), (1, 4, 5, 6) and (2).

A minimal path set (MPS) is a set with a minimum number of units required to ensure the connection between the input and the output. In the case of Fig. 3, the MPS's are the trajectories T_1 = (1, 3, 6), T_2 = (1, 4, 7) and T_3 = (2). The sets (1, 3, 5, 7) and (1, 4, 5, 6) are not MPSs because (1, 3, 6) and (1, 4, 7) are sufficient to guarantee the two trajectories that pass by the parallel branches.

On the other hand, a cut set is a set of units that fail to interrupt all possible connections between the input and

the output. They are in the Fig. 3: C_1 = (1, 2), C_2 = (3, 4, 2), C_3 = (6, 7, 2), C_4 = (3, 5, 7, 2), and C_5 = (4, 5, 6, 2).

A minimal cut set (MCS) is the smallest set of units to ensure a flow interruption to the outlet. The MCS's are the sets: (1, 2), (3, 4, 2) and (6, 7, 2).

Considering initially the MPS's, we can say, strictly, that the reliability of the system is given by the relation (1), next, but only if the MPS's are disjoint .

$$R_S = Pr(T_1 \cup T_2 \cup T_3) = P_r(T_1)+P_r(T_2)+P_r(T_3), \qquad (1)$$

where ∪ is the "union" symbol of Boolean Algebra.

However, in our example, two of the MPS's, T_1 and T_2, are not disjoint because they both contain the unit 1. In this case, the exact expression is given by

$R_S = Pr\ (T_1 \cup T_2 \cup T_3)$ - $Pr\ (T_1 \cap T_2 \cap T_3)$, or more precisely:

$$R_S = [Pr(T_1)+Pr(T_2)+Pr(T_3)] - [Pr(T_1 \cap T_2) + Pr(T_1 \cap T_3) + Pr(T_2 \cap T_3)] \qquad (2)$$

Where ∩ is the "intersection" symbol of Boolean Algebra.

Note that $(T_1 \cap T_2)$ = (1), but (T1∩T3) = ( ) and $(T_2 \cap T_3)$ = ( ), i.e., there are no the intersections $(T_1 \cap T_3)$ and $(T_2 \cap T_3)$. We say then that the T_{is} are almost or highly disjoint, or that the value of (2) is very close to the value of (1). In any case, it is useful to write:

$$R_S \leq P_r(T_1)+P_r(T_2)+P_r(T_3), \qquad (3)$$

i.e. with the equality signal replaced by the inequality signal, indicating that the system reliability value does not exceed the value given by expression (1). It is a useful expression, especially for the usual mission times of commercial aircraft travel.

The approximation given by (3) is so the the lower is the reliability of the units that integrate the T_is, which is not really usual in practice, due to the current technology, which confers very high values to the reliability of the units, especially for electronic units. The approximation given by (3) is the better the lower the reliability of the units within the T_{is}

However, let us calculate the value of expression (1), assuming that the units are electronic (high reliability), which allows us to use the expression e $R = e^{-\lambda t} = Exp(-\lambda t)$[1] for the reliability of the units. Consider, for example, the following failure rates for MPS's: $\lambda_1 = 1.10^{-6}$, $\lambda_2 = 1.10^{-5}$, $\lambda_3 = 2.10^{-5}$ and $\lambda_4 = \lambda_5 = 1.10^{-4}$.

We have so with t=1h:

$R_S \leq e^{-(\lambda i)} = Exp[-(\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5) = Exp\ [-(1.10^{-6} + 1.10^{-5} + 2.10^{-5} + 1.10^{-4} + 1.10^{-4})] = Exp(-0{,}000231) \cong \mathbf{0{,}9998}$.

Well, there is another way to calculate Reliability, starting from the expression of Fallibility F. If R + F = 1, then R = 1 - F.

The F_s Fallibility, in turn, can be obtained from the minimum cut sets (MCS's) by the following expression:

$$F_S = Pr\ (C_1 \cup C_2 \cup C_3 \cup \ldots \cup C_{n-1} \cup C_n) \qquad (4)$$

As R + F =1, We have $Pr(C_1 \cup C_2 \cup C_3 \ldots . C_{n-1} \cup C_n) = 1 - 0{,}9998 = 0{,}0002 = 2{,}0.10^{-4}$.

But, as in the case of the MPS's, the expression will only be accurate if the MCS's are disjoint, which does not occur with the example of Fig. 3, since units 2, 3, 4, 5, 6 and 7 are present in more than one MCS. Thus, the expression (4) gives a value for the F_s Fallibility slightly larger than the exact value given by expression (5), below.

$$F_S = Pr\ (C_1 \cup C_2 \cup C_3 \cup \ldots . \cup C_{n-1} \cup C_n) - Pr(C_1 \cap C_2 \cap C_3 \cap \ldots \cap C_n), \qquad (5)$$

which is less than the value given by (4). Then, using (4) we have to write:

$$F_S \leq Pr\ (C_1 \cup C_2 \cup C_3 \ldots . C_{n-1} \cup C_n).$$

As R = 1 - F, we can write:

$$R_S \geq 1 - [Pr(C_1 \cup C_2 \cup C_3 \cup \ldots \cup C_5) = 1 - [Pr(C_1) \cup Pr(C_2) \cup Pr(C_3) \cup \ldots \cup Pr(C_5)] \qquad (6)$$

This time, with the inequality signal, but now indicating that the value of R_S actually surpasses the value obtained by Expression (1).

Remember that depending on the complexity of the system, the best way is to solve the problem with the help of a dedicated SW computer.

Well, let's conclude here, also stating that the Minimal Cut Sets (MCS's) technique is also applicable to FTA (Fault Tree Analysis).

On another occasion, we will discuss this.

Thank you and see you next time.

References:

1. *Modarres M., Reliability and Risk Analysis, Marcel Dekker, Inc.,1.993, NY (USA).*
2. *Shooman, M.L., Probabilistic Reliability: An Engineering Approach, 2a. Ed., Kreiger, 1.990, Melbourne.*

[1] *Where λ is the failure rate of one unit.*