Improve Your Knowledge (IYK)

Using Fault Tree Analysis in 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 73– Jun, 07 2019

In the last paragraph of MSC 72, we have said that the minimum cut sets (CCM's) technique is also used in the Fault Tree Analysis (FTA) tool. In fact, when we are faced with complex systems with units having various failure modes, it is difficult to use the Reliability Blocks Diagrams (RBD), so it is more prudent to adopt the CCM's technique in the FTA, or in Success Tree Analysis (STA). In addition, these two tools allow us to also include the role of the human being in the system.

From our already somewhat exhaustive considerations in previous MSCs, we know that the Fault Tree Analysis or Assessment (FTA) is a deductive analysis, that is, an undesirable event is postulated for a system, called the Top Event, deducing the possible causes of this event. It is often said that it is the method of detectives, which start from an unwanted result (homicide, for example) and search for killers (causes)

Well, let's treat FTA in this MSC using the Cut Sets methodology presented in MSC 72. Let's start with the block diagram below that was treated in Fig.1 of MSC 72. It is a simple block diagram series-parallel.

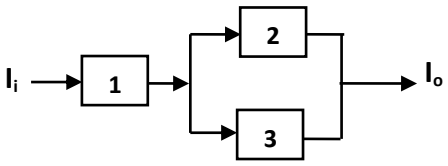

Fig. 1 – Example of a single diagram series-parallel

The current I_i is supplied to the unit 1, which processes it and forwards it to the two identical units 2 and 3.

We have the following set of cut sets: C_1 = (1) and C_2 = (2, 3). As we know, a cut set is a set of units of the system under analysis that, if they fail, cause the system to fail as a whole.

The FTA for the system, considering its cut sets, is shown in Fig. 2.

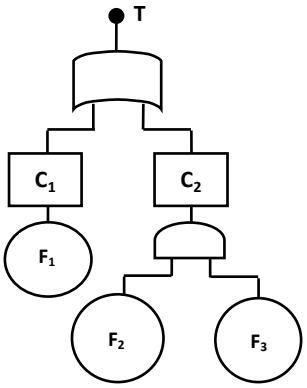

Fig. 2 – FTA of the system in Fig. 1

Notice that we have an "Or" gate, from which emerges the top event T, with the inputs C_1, which corresponds to the failure F_1 of unit 1, and the input C_2, which emerges from the "And" gate, whose inputs correspond to the failures F_1 and F_2 of units 2 and 3.

According to Boolean Algebra:

$$\boldsymbol{T = C_1 \cup C_2}$$
$$\boldsymbol{C_1 = F_1}$$
$$\boldsymbol{C_2 = F_2 . F_3}$$

. On the other hand, as we saw in MSC 72, we can write::

$$\boldsymbol{Pr(T) = Pr(C_1 \cup C_2) = Pr(C_1) + Pr(C_2),} \qquad \boldsymbol{(1)}$$

Just because C_1 and C_2 are disjoint, i.e., they have no common units..

If Pr (T) is the fallibility (or unreliability) F_S of the system, which is given by $F = \lambda t$, when t is small, which occurs if we admit, for example, t = 1h. In this way, we can write:

$$\boldsymbol{F_S = \lambda_1 . \lambda_2 + \lambda_3} \text{ with } t=1h$$

Let us assume that $\boldsymbol{\lambda_1} = 10^{-3}$ and $\boldsymbol{\lambda_2} = \boldsymbol{\lambda_3} = 2x10^{-3}$. It follows that

$$\boldsymbol{F_S = 10^{-3} + (2x10^{-3}).(2x10^{-3}).}$$

$$\boldsymbol{F_S = 10^{-3} + (2x10^{-3}).(2x10^{-3}) = 0{,}005.}$$

Since $R_S = 1-F_S$, it turns out that ***$R_S = 1 - 0.005 = 0.995$****. Now, let us consider the system of the Fig. 3.*

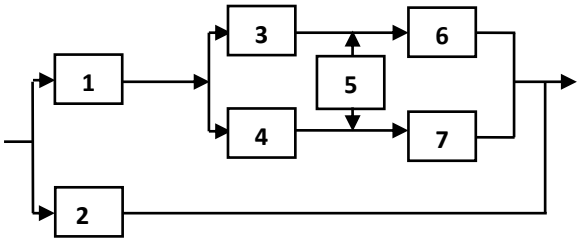

Fig. 3 – Example of Complex System

It is a complex system. We will solve it also by means of an FTA, considering the minimum cut sets (CCM's). A CCM is the smallest set of units to ensure an interruption of the flow to the output. As we saw in MSC 72, the CCM's of the above system are the sets: (1, 2), (3, 4, 2) and (6, 7, 2).

The FTA for the system is shown in Fig.4.

Note that the CCM's are not disjoint because the unit 2 is in all of them. In this way, we must rigorously write:

$$F_S=Pr(T)=Pr(C_1\cup C_2\cup C_3)-Pr(C_1\cap C_2\cap C_3) =$$

$$Pr(C_1)+Pr(C_2)+Pr(C_3) - Pr(C_1.C2.C3) \qquad (2)$$

We have: $C_1=F_1.F_2;\ C_2=F_3.F_4.F_2;\ C_3=F_6.F_7.F_2.$ **(3)**

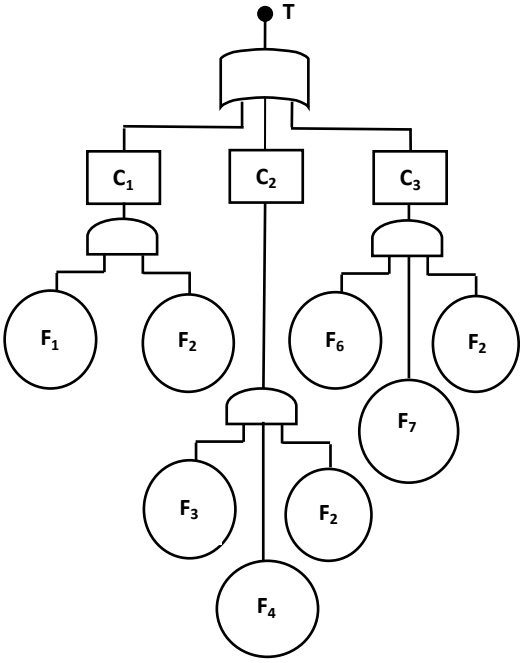

Fig. 4 – FTA of the system of Fig.3

Substituting in expression (2), we obtain:

$$F_S=Pr(T)= Pr(F_1.F_2)+Pr(F_3.F_4.F_2)+Pr(F_6.F_7.F_2)- Pr(F_1.F_2.F_3.F_4.F_2.F_6.F_7.F_2),$$ *ou seja:*

$$F_S=Pr(T)= Pr(F_1.F_2)+Pr(F_3.F_4.F_2)+Pr(F_6.F_7.F_2)- Pr(F_1.F_2.F_3.F_4.\ F_6.F_7) \qquad (3)$$

Notice that in (3) F_2 appears only once in the subtrahend. In fact, according to the idempotent property of Boolean Algebra, $F_2\cap F_2\cap F2\cap \ldots = F_2.F_2.F_2 \ldots = F_2$.

To simplify the operations of expression (3), we consider that the time is small, something like t = 1h, the same way we did in the previous example. Thus, we have the expression $F = \lambda$.

Therefore, the expression (3) is as follows:

$$Fs = (\lambda_1.\ \lambda_2+\lambda_3.\ \lambda_4.\ \lambda_2+\lambda_6.\ \lambda_7.\ \lambda_2)-(\lambda_1.\lambda_2.\lambda_3.\lambda_4.\lambda_6.\ \lambda_7)$$

Additionally, suppose that $\lambda_1=10^{-3}$, $\lambda_2=\lambda_3=2x10^{-3}$, $\lambda_4=10^{-4}$, e $\lambda_6=\lambda_7=10^{-2}$.

The addition of the first three terms give us the value $2{,}2x10^{-6}$, and the subtrahend, $4x10^{-16}$, meaning in this context that the subtrahend is almost "0". Therefore, we can affirm that

$$F_S = 2.2x10^{-6},$$

Given that R + F = 1, we can write $R_S = 1 - F_S = 1 - 2.2x10^{-6} = 1 - 0{,}0000022 \therefore$

$$\therefore \quad R_S = 0{,}999$$

Finally, it is important to note that the subtrahend in equation (2) is generally very small, allowing us, often, only consider parts of the sum, in this case $Pr(C_1) + Pr(C_2) + Pr(C_3)$ *.*

Thank you very much

References:

1. *O'Connor, Patrick D. T., Practical Reliability Engineering, John Wiley & Sons, Ltd, 2010, England.*
2. *Modarres M., Reliability and Risk Analysis, Marcel Dekker, Inc., 1993, NY (USA).*
3. *Shooman, M.L., Probabilistic Reliability: An Engineering Approach, 2a. Ed., Kreiger, 1990, Melbourne.*