Reliability and Safety: Curiosities

Berquó, Jolan Eduardo – Electronic Eng. (ITA)
Aerospace Product Certifier (DCTA/IFI)
Government Representative for Quality Assurance – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

IYK 34 – MAR 12, 2013

Can a System be reliable, but unsafe? Can a System be safe, but not reliable? These issues were placed by a friend. It was an opportunity that we had for dealing with curious things in the field of Reliability and safety. But in this field there are many others curious things. From these questions, we thought it would be very interesting, occasionally, to present others "curiosities" in this our space.

But the answer, at once, to the above questions is "yes", that is, a System can be reliable but unsafe, or a System may be safe but not reliable. But sometimes the System is reliable and secure, or is unreliable and unsafe.

But let's say that the above possibility is because Safety is a relative term. Further, we will show that.

But, just to be clear, let's present the thesis which we want to demonstrate:

"In the field of Reliability and Safety of a System, can exist the following set of pairs of possibilities:

$S = \{(C, S), (C, I), (N, S), (N, i)\}$ (1)

where C: Reliable, S: Safe; U_R: Unreliable; and U: Unsafe".

To demonstrate the thesis, we have to know three concepts: Safety, Reliability, and Severity of Failure Conditions[1]. Let us start with Safety:

"**Safety** - Absence of those conditions that can cause (an accident with) death, injury, occupational illness, damage to or loss of property or equipment, or damage to the environment".

Observe that People, equipment, properties and environment are the "patients", i.e. those who suffer the adverse effects from the "failure agent."

These "conditions"' of this concept are termed "fault conditions" because they are caused by failures. Failure conditions can induce adverse effects on patients.

Note then that safety is a state, and this is relative, that is, there are several possibilities for this State, depending on these failure conditions.

Let us look at the concept of reliability.

"Reliability-Probability that a System meets its mission successfully, at a particular time and under certain conditions".

Promptly, we see that the reliability is a mathematical concept which does not represents a state, but a probability of success of a mission.

When we say that a System is reliable, we mean that there is a good probability of fulfillment of the mission. A System can fulfill its mission, but during the same might occur, for example, one or more deaths. In this case, for the failure that led patients to death, the System is unsafe. Here we have a case of reliable System, however unsafe.

We think that, at this time, it would be enough to realize that the two concepts are quite distinct; they do not necessarily walk in the same direction and sense. But let us dive more to prove the thesis.

Let us now see the concept of Severity:

"Severity (Severity) - Are the potential adverse effects of failure conditions."

As we have seen in the IYK 06, failure conditions are classified according to the severity of its effects.

Let's then consider the severity scale contained in MIL-STD-882 (Ref. 1), presented in table 1. This table also appears in the FAA document: System Safety Handbook, Chapter 3 (Principles of System Safety -Ref. 2).

Table 1 - Categories of Severity

Description	Category	Effects
Catastrophic	**1**	Death, and/or System loss, and severe environmental damage..
Critical	**2**	Severe injury, severe occupational, illness, major System damage and

		environmental damage.
Marginal	**3**	Minor injury, minor occupational illness, minor System damage and environmental damage.
Negligible	**4**	Almost no effects to patients.

We have to understand that it is enough that a failure condition has just one of the effects foreseen to certain failure condition to be considered inserted in such level.

With these established premises, we can see through an ingenious artifice that was developed by safety engineers to establish a relationship between System safety and Reliability. This artifice has received the designation of "Risk Analysis". The risk concept is as follows:

"**Risk-** is a combination of the severity of failure condition and the likelihood that the same occurs".

The risk measures the level of safety provided by the System. High risk, unsafe System; low risk, safe System.

We are getting there. Let's continue.

We will present, then, in table 3, the Risk Acceptability Matrix, extracted from the referenced documents.

Table 3 – Risk Acceptability Matrix

Severit. / Probab.	Catastr. (1)	Crítical (2)	Marginal (3)	Negligible (4)
Frequent (A)	**High**	**High**	**High**	**Medium**
Probable (B)	**High**	**High**	**Serious**	**Medium**
Occasional (C)	**High**	**Serious**	**Serious**	**Low**
Remote (D)	**Serious**	**Serious**	**Medium**	**Low**
Improbable (E)	**Medium**	**Medium**	**Medium**	**Low**

In the first column, we have the levels of probability of failure, from the most probable to the less probable; In the first line are inserted the severity levels, from the most severe to the less severe.

Note that the reliability is not mentioned in this table; however, there is a relationship between the probability to fail (also called fallibility F) and the probability of not fail (Reliability R), that is:

$$R = 1 - F \qquad (2)$$

In the several cells we have the risk levels: high, serious, medium and low, defined by the binomial "Probability of Failure vs. Severity"

These designations "high", "serious", etc., depend on the requirements of the Authority.

The authority may consider unacceptable the High and Serious Risks, considering low the safety of the System. This is the case of the binomial "Catastrophic" and "Remote", despite good reliability. The binomial "Negliguible" and "Frequent" would be considered safe, despite having a very low reliability.

Anyway, we present a possible configuration accepted by the Authority:

(N, I): A1, A2, A3, B1, B2 e B3.
(C, I): C1, C2, C3, D1 e D2.
(N, S): A4 e B4.
(C, S): C4, D3, D4, E1, E2, E3 e E4.

That is, all possibilities contained in the expression 1.

Therefore we believe it is now possible to understand why we have said that the answer to the questions in the first paragraph of this MSC would be "yes".

Finally, we can say that reliability and safety go together in the same direction, but not necessarily in the same sense.

Again, thanks for your attention.

See you.

References:

(1) DoD, **MIL-STD-882E, System Safety**. DoD, USA, 2012.

(2) FAA, **System Safety Handbook**. FAA. USA, 2000.

(3) DAU (Defense Acquisition University). **Systems Engineering Fundamentals**. Fort Belvoir, VA, USA. 2000.