Hazards: A Constant Threat (II) -

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

IYK 23 – DEC 3, 2012

In continuation of the theme, we treat here the dangers embedded in the development of operational processes and procedures.

As mentioned in the MSC 22, the best we can and must do is identify hazards and assess the risks arising, according to their consequences and probability of occurrence (qualitative and/or quantitative), trying, as much as possible and economically supportable, avoid them or minimize their effects.

But when we talk about risk, most people think immediately in physical systems designed and operated by human beings, such as bridges, aircraft, rockets, missiles, etc.

This reminds us the accident investigation of the Brazilian launcher VLS-1, V03 prototype, which occurred at approximately 13:30, 22/08/2003, whose Committee of Investigation for the Material Factor we had the honor of chairing. That investigation lasted 172 days, ending in February 2004.

But our committee investigated just the material factor and drew conclusions that can be seen in the Final Report or, in more detail, in the Report of Material Factor.

Based on the reports of the various committees (Material, Operational, Meteorological and Human Factors), the Final Report made several recommendations.

One of them recommended to use the Sneak Circuit Analysis, for the next designs, a type of analysis widely practiced in american space projects. But it was recommendation thinking just on the design of the launch vehicle, although this type of analysis can also to be perfectly practiced in the operational processes.

Subsequently, we suggested that a risk analysis was also performed on the operational processes performed on the ground, before launch, using, for example, a PFMEA (Process Failure Mode and Effects Analysis). It seemed right to us to suggest such a thing, considering the evidences recorded in the report of the operational factor about the accident.

The suggestion was well received; however, we do not have information on the real use of this analysis.

Nevertheless, what is necessary to have in mind, all the time, is that accidents can occur when we use wrong procedures or when we follow them incorrectly, even though they are correct. This is basic.

We must remember that a process is composed of tasks, but may be that the tasks of a process have different levels of risk in their implementation; so, the risk rating for the process is that attributed to the task with the highest risk.

Sometimes, the accident can occur because the operator does not use security devices or use them incorrectly, or there is a device failure. Other times, the danger is in a task or in a tasks sequence.

A hazard can, for example, be present, at the time in which a person, responsible for performing a particular task, fails to carry it out, by imposition of superiors. Unfortunately, we can not say that this is unusual.

Anyway, there are several considerations to be made when designing or analyzing a process with its tasks and security devices.

Let's list a few.

But first, for illustration, let's talk about the famous "Murphy's Principle" (which some call "Murphy's Law"). We have information that Murphy was an USAF Sergeant, dedicated to test in flight activities. He was part of the team that handled the instrumentation connected to the acceleration test.

At the end of one of these tests, the Major who had participated as pilot told Murphy he had beat the record for acceleration. Promptly, they went to see the records in the instrumentation and they noticed that the same indicated

acceleration "zero". After analyzing what had occurred, they concluded that the mechanic who had prepared the instrumentation had reversed the connections of the accelerometer. Consequence: the instrument pointer remained static.

So, the Major would have spelled out the so called "Murphy's Law": “If the task or procedure can be performed incorrectly, it eventually will be done that way”. This is a proper example of error in execution of an operational process, which may have occurred because one or more possible reasons, as we will see later.

We present now the list (not exhaustive) of considerations to be taken into account.

When a procedure is lengthy, tedious, strenuous, and uncomfortable or requires patience, the operator may tend to skip steps or take shortcuts.

Procedures that require intense concentration, for a long period of time must be minimized, modified or eliminated, since any distraction can follow an unexpected trajectory (“sneak circuit”).

The checklists are examples of procedures that must be clear, concise and easy to follow.

Must be eliminated all the steps that can be eliminated, but without being lost the clarity and effectiveness of the procedure.

The way we use any device can be more dangerous than the use of a defective device.

The feeling of "**I know very well that**" can lead to disdain for checklists and lead to errors and accidents. The driver starts to hit the car after that he considers himself to be a good driver. (Perhaps this was the case when the Major enunciated the "Murphy Law").

Procedures that seem very simple and quiet, can lead to a false sense of safety.

The procedures must clearly identify all devices and equipment that an operator will need to perform a task, and the operator must be trained to use them.

Interrupting a task to find some device that was forgotten, can lead the operator to make mistakes in the continuations of the task

If a procedure has been started, it should run until the end. This is an advice that can save lives (unfortunately, we have examples of this).

Procedures that require a lot of communication should be avoided or eliminated, mostly by faults in communication devices or difficulty understanding of interlocutors, due to electromagnetic interference.

The theoretical and practical training shall, as far as possible, be supplemented with "on-the-job-training".

Finally, lack of energy or excess of some energy (electrical, chemical, mechanical, thermal, etc.) must be considered and simulated, but paying attention to the risks

Well, we have presented here some alerts, which we can use when we will intend to design and analyze processes; but of course we could still increase this list.

See you

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

(2) MIL-HDBK-764(MI). **System Safety Engineering Design Guide For Army Materiel**. USA: DoD, 1990.