- Sneak Circuits Analysis -

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

IYK 15 – SET 04, 2012

The subject of this MSC is a summary of Chapter 4 of the book "Segurança de Sistemas" (System Safety) - (Ref. 3), we write for engineers of the Professional Master Course, offered in 2005 to the "Instituto de Atividades Espaciais - IAE" (Institute of Space Activities) of the Departamento de Ciência e Tecnologia Aeroespacial – DCTA" (Department of Science and Technology), located in São José dos Campos (SP).

As the title indicates, this MSC is about the so called "Sneak Circuits" (SC) or "Hidden Circuits". These circuits, when they exist, can manifest themselves in the electronic and electrical systems, in terms of electrical currents in hardware and flows in software. But we'll treat here just of electrical currents in hardware..

The name "Sneak Circuits" comes from the case of electrical paths or dormant flows, not foreseen in the design, and that suddenly, or unexpectedly, under certain conditions, arise in a system, making arise unwanted functions or inhibiting existent functions, what can lead to serious accidents and even to catastrophic accidents.

It is neither a failure nor a design error. If we examine a design with sneak circuits, mainly the most complex, it is possible that almost always we conclude that it meets the functional and safety requirements. However, such design can contain sneak circuits, which unfortunately are not perceived by the designer.

Accidents in the U.S. space program, caused by this type of circuits, took the Boeing Aerospace Company and Convair Division of General Dynamics in 1967 to the development of the so-called Sneak Circuit Analysis (SCA) to identify these possible paths in a design. That technique was applied, for example, to the Apollo and Skylab programs.

There are five categories of SC:

(1) Sneak Paths - currents in unexpected routes;

(2) Sneak Opens - current not flowing where it should flow;

(3) Sneak Timing - actions out of the expected time;

(4) Sneak Indications - ambiguous or false Indications, leading the operator to take wrong attitudes; and

(5) Sneak Labels or Sneak Procedures - leading the operator to operate devices in the wrong way.

We will present an example of SC of the type of 2, ie "Sneak Opens". Consider Figure 1.

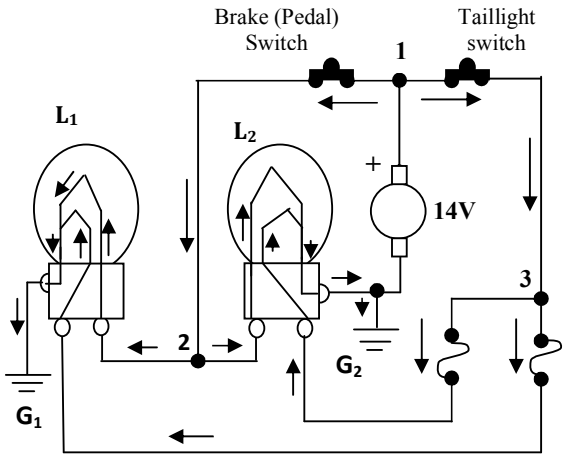

Fig. 1 – Electrical System of Brake Lights and Taillights in normal operation.

The figure shows an electrical system used in a car with a DC generator, two lamps with two filaments each one, brake (pedal) switch, taillight switch and fuses, in normal operating condition.

One of the filaments in both lamps indicates that the brake pedal is pressed. The other filament,

also in both lamps, indicates that the taillights key in the panel is turned on.

In the situation of the figure, the driver is stepping on the brake pedal and the taillights switch is turned on.

Let us go then from the positive terminal of the 14VDC generator. The current from this generator bifurcates at node 1, passing a part through the brake pedal switch and the other part through the taillight switch.

The part that goes through the brakes switch also bifurcates at the node 2, passing part through similar filaments in the lamps L1 and L2, that is, the filaments of the brake lights. Both parties, after passing through these filaments, forwarding to the respective points of mass (ground) G1 and G2. So, turn on the brake lights.

The part that comes out from the generator and passes through the taillight switch bifurcates at the node 3, passing a part through one of the fuses and the other part through another fuse. These currents will pass each one by similar filaments of the lamps L1 and L2 (the filaments of the taillights), forwarding to the respective points of masses (ground) G1 and G2. So, turn on the taillights.

The reader is invited to check what occurs when, for example, the brakes switch is open (that is, the driver is not stepping on the brake pedal). There are other possibilities. Check them.

In one first analysis of the system shown in Figure 1, we can say that the design is functionally perfect. Apparently, there is nothing that does not recommend such design. It would be difficult for a normal customer refuse it.

But a SC analyst would see it with other eyes. Immediately, he would worry with two types of paths: (a) one that would result when one or more distinct power points were removed; and (b) one that would result when one or more discrete mass points were removed.

Suppose, for example, that the connection to the point of mass G1, for some reason (e.g. involuntary movement in maintenance, vibration etc.) is removed. The circuit would be as in Figure 2.

In such a situation, the electric potential difference between nodes 2 and 3 is virtually null (the fuse, in the path between the point 3 and the lamp L1, is practically a short circuit, not producing voltage drop).

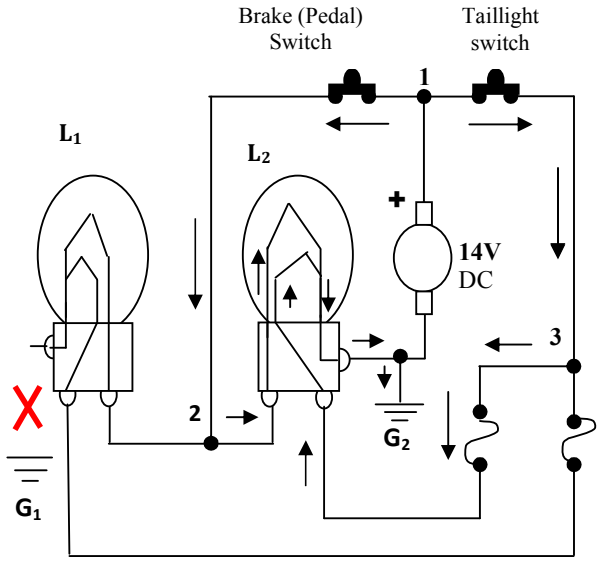

Fig. 2– Electrical System of Brake Lights and Taillights with the point G1 removed

Thus, no current would flow in the filaments of the lamp L1, that is, the lamp L1 simply would remain off. On the other hand, the Lamp L2 would be activated, with both filaments turned on.

Now, suppose that the brake pedal was not pressed (brake switch opened), and the switch of taillights is closed. What would happen? Check!

The circuit that we have examinated is simple. If it were a complex circuit, like one of a rocket, would be almost impossible to make an analysis like that we did. In this case, we would have to use a computer.

If the reader wants to know more details, see the references. The Chapter 4 of the Ref. 2, which treats the Sneak Circuit Analysis, may be requested by e-mail. Use the e-mail treinamento@dcabr.org.br.

There it is included the methodology for preparation of the data for insertion into the computer.

References:

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

(2) BERQUÓ, Jolan Eduardo. Segurança de Sistemas, São José dos Campos (SP) – Brasil, Apostila 5ª. Rev, (2006).

(3) ERICSON II, Clifton A. Hazard Analysis Techniques for System Safety, USA, John Wiley & Sons Inc. (2005).

(4) AIR FORCE SAFETY AGENCY, Air Force Safety Handbook. USA: HQ AFSC/SEPP, Kirtland AFB, NM 8117-5670, (2000).