- Análise de Circuitos Ocultos (Sneak Circuits Analysis) –

Berquó, Jolan Eduardo – Eng. Eletrônico (ITA).
Certificador de Produto Aeroespacial (DCTA/IFI)
Representante Governamental da Garantia da Qualidade – RGQ (DCTA/IFI)
jberquo@dcabr.org.br

MSC 15– 04 SET 2012

O assunto deste MSC é um resumo do Capítulo 4 da apostila "Segurança de Sistemas" (Ref. 2), que produzimos para o curso de Mestrado Profissionalizante, ministrado em 2005 para profissionais do Instituto de Atividades Espaciais (IAE) do Departamento de Ciência e Tecnologia (DCTA), situado em São José dos Campos (SP).

Como indica o título, este MSC versa sobre os chamados "Circuitos Ocultos ou Fugidios" (*Sneak Circuits - SC*), para os quais reservamos a sigla CO.

Esses circuitos, quando existem, manifestam-se nos sistemas eletrônicos e elétricos, em termos de hardware, bem como nos fluxos de software. Mas ficaremos aqui apenas no nível de hardware.

A denominação "Circuitos Ocultos" vem do fato de se tratar de trajetórias elétricas ou fluxos latentes, não previstos no projeto, e que, de repente, ou seja, inesperadamente, sob certas condições, surgem num sistema, fazendo brotar funções indesejáveis ou inibindo funções previstas, podendo produzir acidentes sérios e até mesmo catastróficos.

Não se trata de falha e nem de erro de projeto. Se examinarmos um projeto com circuitos ocultos, principalmente os mais complexos, vamos concluir que ele atende aos requisitos de segurança (*safety*). No entanto, esse projeto pode conter circuitos ocultos, sem que os projetistas se deem conta disso.

O fato de terem ocorrido acidentes no programa espacial americano, provocados por esse tipo de circuitos, levou a *Boeing Aerospace Company* e *Convair Division of General Dynamics*, em 1967, a desenvolver a chamada Análise de Circuitos Ocultos – ACO (*Sneak Circuit Analysis - SCA*), para identificar essas possíveis trajetórias num projeto. Essa técnica foi aplicada, por exemplo, nos programas Apolo e Skylab.

Há cinco categorias de CO:

(1) Trajetórias Ocultas (*Sneak Paths*) – Circuitos inesperados (correntes em rotas não esperadas);
(2) Aberturas Ocultas (*Sneak Opens*) – Correntes não fluindo onde deveriam fluir;
(3) Ações Fora do Tempo Previsto (*Sneak Timing*);
(4) Indicações Ambíguas ou Falsas (Sneak Indications), levando o operador a tomar atitudes incorretas; e
(5) Etiquetas com Imprecisão (*Sneak Labels*) – fazendo o operador atuar em dispositivos de maneira errada.

Vamos apresentar um exemplo de CO do tipo (2), ou seja, "Aberturas Ocultas". Considere a figura 1.

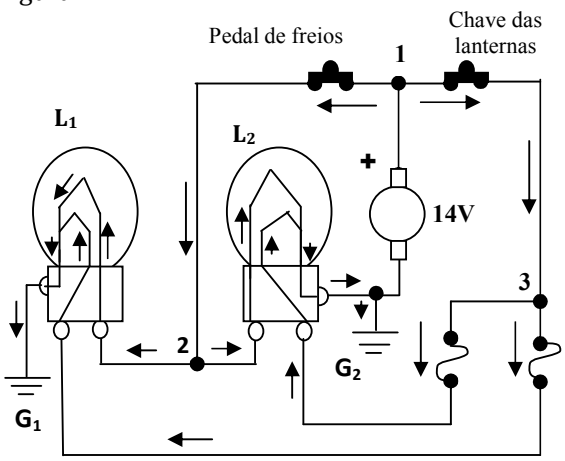

Fig. 1 – Sistema elétrico de luzes de freio e de lanternas traseiras,

A figura apresenta um sistema elétrico de luzes de freio e luzes de lanternas traseiras, na condição de operação normal.

Um dos filamentos das lâmpadas indica que o pedal de freios (chave de freios) está acionado. O outro filamento indica que a chave do painel relativa às lanternas traseiras está ligada.

Na situação da figura, o motorista está pisando no freio e a chave das lanternas traseiras está ligada.

Vamos então partir do terminal positivo do gerador de 14VDC. A corrente que parte desse gerador bifurca-se no nó 1, passando uma parte pela chave de freios e a outra pela chave das lanternas traseiras.

A parte que passa pela chave de freios também se bifurca no nó 2, passando uma parte por um filamento da lâmpada L_1 e a outra por um filamento análogo da lâmpada L_2 (são os filamentos de indicação das luzes de freio) . Ambas as partes, após passarem por esses filamentos, dirigem-se aos respectivos pontos de massa (terra) G_1 e G_2. Acendem-se as luzes de freio.

A parte que sai do gerador e passa pela chave das lanternas traseiras bifurca-se no nó 3, passando uma parte por um dos fusíveis e a outra pelo outro fusível. Essas correntes vão passar cada uma por filamentos análogos das lâmpadas (os filamentos das luzes de lanterna), encaminhando-se para os respectivos pontos de massas (terra) G_1 e G_2. Acendem-se as luzes das lanternas traseiras.

O leitor é convidado a verificar o que ocorre, quando, por exemplo, a chave de freios está aberta (o motorista não está pisando no pedal de freios). Existem outras possibilidades. Verifique-as.

Numa primeira análise do sistema apresentado na Figura 1, pode-se dizer que o projeto está funcionalmente perfeito. Não há nada que aparentemente não o recomende. Seria difícil, para um cliente normal, recusá-lo.

Mas um analista de CO o veria com outros olhos. Ele se preocuparia, de pronto, com dois tipos de trajetórias: (a) as que resultam, quando um ou mais pontos de alimentação distintos são removidos; e (b) as que resultam, quando um ou mais pontos de massa distintos são removidos.

Suponhamos, por exemplo, que a ligação ao ponto de massa G_1, por algum motivo (p. ex.: movimento involuntário na manutenção, vibração etc.) seja removido. O circuito ficaria como na figura 2.

O que ocorre é que, nessa configuração, a diferença de potencial elétrico entre os nós 2 e 3 é praticamente nula (o fusível, na trajetória entre o ponto 3 e a lâmpada L1, é praticamente um curto circuito, não produzindo queda de tensão).

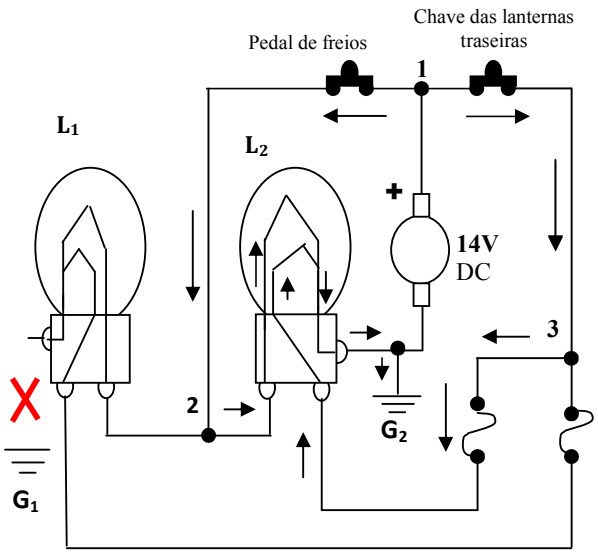

Fig. 2 – Sistema elétrico de luzes de freio e de lanternas traseiras.

Desse modo, em sendo nula a diferença de potencial entre esses pontos, nenhuma corrente fluiria nos filamentos da lâmpada L1, e ela simplesmente permaneceria apagada. A lâmpada L_2 se acenderia (com os dois filamentos acesos).

Imagine agora que o pedal de freios não estivesse acionado (chave de freios aberta), e a chave das lanternas traseiras, fechada. O que aconteceria? Verifique!

O circuito que examinamos é simples. Se fosse um sitema complexo, como aquele da Apolo, seria quase impossível fazer uma análise com a simplicidade da que fizemos. Aí é que entraria o computador.

Se o leitor quiser se aprofundar, consulte o Capítulo 4 da Ref. 2. Cópia em PDF desse Capítulo poderá ser enviada ao leitor, a pedido do mesmo, por meio de e-mail endereçado a treinamento@dcabr.org.br.

Ali está incluída a metodologia de preparação dos dados para inserção no computador.

Referências:

(1) DoD: MIL-STD-882E. System Safety. EUA: 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. EUA, John Wiley & Sons Inc., (2005).

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