HCRQ, Inc.

"The Key To A Safer World"

Newsletter—October 2008

Forensic Investigations

The following is the follow-up to a question asked by a reader in the September issue.

We have had the opportunity to perform post-accident analyses for companies whose systems have failed catastrophically, often resulting in death. This work has been insightful from ethical, moral, legal (both corporate and professional), and technical standpoints.

Accidents, related to software failures, were very insightful. We have noted that it took periods of months and sometimes years (4 years in one case) for the problems to surface. This is consistent with available literature on the subject. In these situations, where the period was years, prior to the accidents, companies had a false sense of security regarding the integrity of their software.

We have noted that the problems would have been very difficult, if not impossible, to locate in the presence of even the most rigorous testing regime. This is consistent with a statement we recall reading years ago: "problems, which are discovered by testing, are usually of the type which do not typically cause future accidents."

We have noted that some of the problems were introduced during software maintenance.

We also noted one case where, had the requirement been written mathematically, instead of in English, it is very unlikely that the accident would have occurred.

FTA Software

There are a number of FTA programs on the market; however, it is our opinion that there are only a few which are good. Analytically, they are all very similar. Some are weak though when it comes to printing especially paginating, and linking pages. Some utilize OTS databases which is advantageous when attempting to ensure consistency in notation and probabilities. Some suppliers offer FTA software integrated with other analytical software.

PHL

We have seen confusion over what constitutes a Preliminary Hazard List (PHL). The PHL is a line item inventory of system hazards. There is no evaluation of severity or probability and no controls/ mitigations suggested. Sometimes PHLs are created by system safety engineers during the preparation of a responses to RFPs. One analyzes the system concept and preliminary requirements and specs. A list of potential hazards is created from this, hazard analyses and lessons learned from similar systems, generic lists of hazards, and accident/ incident reports. A PHL may or may not be specified. If one is created, it forms the primary input to the PHA. Task 201 of MIL-STD-882C specifies the requirement for a PHL.

PHA

Since the PHL is not always specified, the Preliminary Hazard Analysis (PHA) is often referred to as the hazard identification task. (Note: For those of you that use HAZOP analyses, don't worry, we will be covering these in a future issue.)

Note that in the case of both PHL and PHA, the first word is "Preliminary". These documents are of passing interest. You can see how the PHL fades away after it becomes swallowed up by the PHA. Similarly, the PHA fades away after it becomes swallowed up by the Hazard Log which becomes the evolving/maintained document.

Neither the PHL nor the PHA is intended to be perfect, after all they are created early in the development cycle. For instance, some, all or none of the controls/mitigations listed in the PHA may be ultimately adopted.

A coordinated, multidisciplinary group approach is required. The team may consist of domain experts, system safety engineers, software safety engineers, system engineers, software engineers, hardware engineers, human factors analysts, operators/users, QA, and test & evaluation personnel.

The process of performing a PHA may be based on hazard type, function, operational phase, system/subsystem, energy source, or geographic location.

Two things sometimes become very clear when creating a PHL or PHA. The first is that some people do not understand what constitutes a hazard and what does not. The second is that often the first cut of the PHL/PHA contains a mixture of hazards and contributors to hazards.

Task 202 of MIL-STD-882C specifies the requirement for a PHA.

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com

HCRQ, Inc.

"The Key To A Safer World"

Newsletter—October 2008

Questions From Our Readers

Q. I understand the need for independence of system safety from the development group. Has it been your experience that this is a common practice?
A. You are probably familiar with the table within IEC 61508 which recommends various degrees of independence based on SIL. Independence is necessary period; however, it has been our experience that in many cases this practice is not followed. There can be practical or economic reasons for this. Often there is no distinct/separate safety group. In many cases we see engineers who, depending on the day, will either have a developer's hat on or a system safety one.

Q. I am looking for insight regarding hazards associated with touch potential.
A. Electric shock becomes a consideration when the voltage exceeds 50 VDC. It is a consideration on 3 rail light rail systems where the return path for the high voltage DC is through the car body and running rails. Ordinarily constant exposure to 50 VDC is not hazardous. As the voltage increases, the maximum time one should be exposed to this decreases. There is a published curve of voltage versus time we believe in an IEEE Standard (80?). Perhaps one of our readers has the reference handy.

MIL-STD-1629A

Question: What is the commercial replacement for this FMECA standard?

Answer: SAE ARP5580 although 1629A continues to be specified.

Why Are We Doing These Things?

Have you ever leaned back in your chair, examined what safety analyses, guidelines, tools and processes you are being forced to use or what safety documentation you are being forced to create and asked yourself "Why?" "Does this make sense?"

Perhaps you are being forced to do so because of a SOW/DID. We are sure that you have seen some pretty terrible SOWs and DIDs—some that resemble snippets from a safety engineer's trash can thrown into a document. Perhaps it is due to a governing standard. Just because it is a standard doesn't mean it necessarily makes sense. Perhaps it is your company's policy.

Is there a rationale, scientific/ mathematical justification for doing these things? Is there proof that they are effective? If so, to what degree? Do you know that safety will be enhanced by doing so? Are you filling rooms with documentation for which you know there is no budget to maintain?

Are you spending too much time on things of questionable significance? In doing so, is this burning project budget dollars that would be better spent on things which safety engineers know contribute much more significantly to system safety?

As safety engineers, these are questions that we need to constantly ask ourselves. We need to question the originators. We need to discuss this in forums. We need to analyze the situation and propose more effective measures. There are times when we need to push back!

Corporate Safety Policy

We mentioned this document in the July issue.

In order to achieve safety, commitment by management is crucial. The System Safety Management Plan (SSMP) or safety management section of the System Safety Program Plan (SSPP) usually articulates the Corporate Safety Policy.

This Policy conveys the importance of safety efforts both internally within the company as well as externally to clients and safety authorities.

The Corporate Safety Policy is much more than a sentence or a paragraph from a marketing brochure; it contains specific elements, details and commitments. For instance, who maintains the Policy? Who ensures its distribution? Who ensures its adoption? What mechanism is in place to support recommended changes?

This is more than a "nice to have". It is a corporate essential!

Webinar—SSPPs

The next webinar on this topic is scheduled for November 3.

Further information is available at www.hcrq.com/WebinarSSPP.html.

System & Software Safety

Courses to be held in Willamsburg, VA in 2009 will be announced shortly.

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com