HCRQ, Inc.

"The Key To A Safer World"

Newsletter—April 2009

Update

You likely noticed the absence of the March issue of this newsletter. This was due to the effects of the recession on our business. We simply could not justify the allocation of resources to it.

We are doing our best to keep these newsletters coming; however, there may be additional gaps along the way and/or terser newsletters until the economic climate improves.

Readership is continuing to increase.

With Gratitude

We would like to acknowledge the supportive comments and feedback that we receive from Bill Harrison of Sikorsky Aircraft. Thank you Bill!

Bill provided us the following comments regarding the February issue:

1) Development Assurance Levels (DAL) are covered in SAE ARP4754 not in 4761. DALs are addressed in 4761 in the bottom section of Table-1, as well as Section 3.3 (PSSA) and 3.4 (SSA) which refer back to 4754. Additionally, 4761 is considered subordinate/supplemental to 4754.
2) MOD 00-56 is not the correct reference and should be replaced by DEF STAN 00-56. The Ministry Of Defence (MOD) is the responsible authority; whereas, Defence Standards (DEF STANs) are their actual publications.
3) DEF STAN 00-56 also refers to RTCA DO-178B as does SAE ARP4754.

Questions From Our Readers

Q. Is there a published comparison between RTCA DO-178B Software DALs and MIL-STD- 882C SCCs?
A. None of which we are aware. DALs are defined by the severity of the failure conditions. SCCs are defined by the degree of control software exercises over the hardware.

Seasoned Safety Engineers

This sounds like we are taking safety engineers, adding gourmet spices (perhaps a little saffron, tarragon, etc.), simmering them over low heat while enjoying fine Chianti.

These types of engineers are indeed a rare breed. It is frequently the case that either ourselves or our clients are dealing with customers who lack what we call "seasoned" safety engineers. Ludicrous requirements are being levied while other, more important, issues are being ignored.

Safety engineers may be experienced, knowledgeable or both; however, this does not mean that they are "seasoned". Let's consider an example.

Experienced safety engineers may have only worked in light rail safety (e.g., no aviation safety experience, no experience with DALs). There are also safety engineers who have spent most of their time reviewing other's analyses but considerably less time performing analyses. Some have performed PHAs but not a HAZOP. Some have performed SSHAs but not PSSAs. Some have never performed CCA. Some have never prepared a safety case. Some have no software safety experience.

Knowledgeable safety engineers may have published books or papers. They may have an abundance of sector-specific knowledge, standards, and know a great deal concerning the various analytical approaches and safety documents. They may be knowledgeable of both system safety, software safety, and reliability.

Seasoned safety engineers have broad and in-depth experience and knowledge. They can review or produce any kind of safety or reliability analysis or related document, applicable and acceptable to any sector. Large projects and large system safety programs are second nature to them. So is working with system engineering, project management, quality assurance, configuration management, software engineering, human factors engineering, and subcontractors. They quickly focus on what is missing and what is wrong. They hit the ground running. They are very pragmatic and productive. They know when "enough" safety assurance has been provided. They have a good sense of "bang for the buck". Ideally, they have a solid foundation in software safety.

Industry is sadly lacking these unique people and they are necessary. In their absence, safety can be compromised, money wasted, and very poor SOWs, DIDs, and standards produced.

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—April 2009

We close this article with a note from one of our most respected industry contacts.

"There can be an even further problem when you have the situation characterized so well by Will Rogers: *The problem in America isn't so much what people don't know; the problem is what people think they know that just ain't so.*"

Questions For You

Ok, now it is your turn. With only a very few exceptions we have not heard from you.

Here are two questions for you. E-mail us your answers. We promise to keep your identity confidential.

1. How do you identify a good fault tree versus a bad one?

2. When you transition from dual redundancy to triple is safety increased?

Announcements

NFPA Conference & Expo
June 8-11
Chicago
www.nfpa.org/categoryListWSCE.asp?categoryID=1600

ASSE Safety 2009
June 28-July 1
San Antonio
www.asse.org/education/pdc09/index.php

ISSC 2009
August 3-7
Huntsville
www.system-safety.org/~issc2009/

SAFECOMP 2009
September 15-18
Hamburg
www.safecomp.org/

International Conference on System Safety
October 26-28
London
conferences.theiet.org/system-safety/index.htm

Readers: We would appreciate your additions to this list!

Webinar, Course Cancellations

Our suspicions regarding the recession's effects on training budgets have been confirmed. Due to cutbacks, we are not seeing sufficient interest in the public offerings of our courses.

For this reason, the SSPP Webinar, scheduled for March 23, was cancelled. Furthermore, our Software Safety Course, scheduled for April 20-22, and our System Safety Course, scheduled for May 18-20 were also cancelled.

We will not be scheduling future public offerings until the economic situation improves.

Still available as an option for interested parties (with intact training budgets) are on-site courses which require a minimum of 5 attendees.

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com