HCRQ, Inc.

"The Key To A Safer World"

Newsletter - November Update 2010

Feedback - Forensic Investigations

One of our readers, actually a safety engineer that we know well and respect highly, responded to our previous newsletter as follows. We hope you enjoy his feedback as much as we did.

- In many cases, even the most exhaustive testing would not have located the scenario which led to the accident. *That has often been the case when the design is used for something other than what it was designed (and tested) for.*
- Investigative costs are dwarfed by the costs of the accidents which may have associated litigations. *Turn that around and put the effort on the other end, exchange reactive investigation with proactive analysis… "preliminary analysis costs are dwarfed by the costs of accidents". How often do we have to re-learn this lesson or do we, as safety engineers, have to bring cost analysis back into our assessments?… (that is of course until someone gets upset again because we have to actually put a figure on the value of someone's life in order to do that.)*
- Prior to the accidents, clients have often been overconfident due to extensive testing that they performed on the system or due to system's longevity in the field with no accidents. *How often do you hear "Well it passed the tests"; but no one asks "Were they the right tests?" How often does SSE fail to influence the test plan based on the analyses.*
- Often safety analyses do not match the design. *Under-funded, understaffed, and un-integrated system safety organization that's not being "kept in the loop" through development and design changes? No chance!*
- Sometimes the design documentation has not been kept current. *Geez, as though none of us have heard this: "Oh, but this change doesn't affect safety, this is just a minor hardware change, or minor a fix to make it better. We don't need to fund safety to document "no impact"."*
- Sometimes the system design is overly complex. *As long as the mitigation and controls are effective and simple, you can tolerate some excess complexity. It just means the mitigation and control systems might be working overtime. And better test the crap out of the mitigation and control to make sure they are effective and "high enough".*
- We have seen worse designs with greater potential for accidents than we saw in these investigations. *Don't tell me that; it just makes it sound so random and that we really don't have any influence anyway! And most certainly don't tell the project manager, who is looking to cut the safety budget! "We haven't had any accidents yet so it must be ok. Just design it to the same level of safety as what's currently fielded!"*
- Software Change Hazard Analysis may not have been performed. *Even those SSCA's, that have been performed, can be no better than the original analysis. Too many of the baseline software safety assessments are improperly executed (argument for another day). The SSCA will then have no more value than the baseline assessment.*
- Interesting quotes such as "we thought that couldn't happen", and "the patient did not have long to live anyhow". *How about a response to a developmental test failure… "we'll probably never know why it failed… Oh, but we have a fix in place".*

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 - November Update 2010

New Webinar A Perspective On Software Safety Assurance

Some software safety assurance techniques and guidelines effective, others are ineffective, some are quite costly to apply, some might call "nice to apply" but fail to provide significant benefit. Some lack any sort of evidence that their application is beneficial.

It is invaluable to know the effectiveness and shortcomings of these software safety assurance methods. This webinar addresses this need.

www.hcrq.com/WebinarAPOSSA.html

Question: Fault Tree Analysis Document Content

Some of you have told us that you miss our quizzes. Well, here is a question with broad appeal.

When you document an FTA, what should appear inside that document besides the fault trees and the minimal cut sets?

E-mail us with your answer or if you simply want the answer.

Australian System Safety Conference

"Managing Systems and Software Safety Risks in Emerging Technologies"

A joint conference between the Australian Safety Critical Systems Association (aSCSa) and the Systems Safety Society (SSS) Australian Chapter.

Melbourne, Australia
May 25-27 2011
http://www.assc2011.org

Full Railroad Safety Advisory Committee (RSAC) Meeting

Date: December 14
Time: 9:30AM-4:30PM
Location: Washington, D.C.
Venue: National Housing Center
Web: http://rsac.fra.dot.

Course/Webinar Price Increases

As the end of the year approaches we are preparing to transition into the new year. There are to be slight course and webinar price increases for next year.

We are going to transition each course and webinar over to their new prices as soon as the last ones for this year are underway. Since we offer so many courses and webinars, and there are so many web pages and brochures affected, this will make it easier for us rather than making all of the modifications on January 1.

Thus far we have identified the following schedule for price increases:

- Software Safety Course - Dec. 1
- System Safety Course - Dec. 7
- Hands-On FTA Course - Dec. 16

If you are planning to attend one of our offerings next year, and if you have the funds available, we encourage you to register for your Williamsburg course, webinar, or book your on-site course, as the case may be, now before the prices increases take effect.

Thank you.

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com