HCRQ, Inc.

"The Key To A Safer World"

Newsletter—September 2008

Readership

There are now in excess of 1000 subscribers to this newsletter. We hope to continue to interest you in the things we {and other contributors} have to say.

Software Safety

This is sometimes referred to as "software system safety". Thus far we have said very little regarding this topic. This certainly is an area of expertise unto itself. Having specialized in this area for 22 years, we could easily make our newsletters exclusively about software safety. We will strive; however, to cover salient issues within this and subsequent newsletters.

Software Safety Engineers

The breadth and depth of the knowledge and experience of software safety engineers can vary substantially.

We know some companies which have so many active projects that the people known as "software safety engineers" only have time to move from meeting to meeting. We know DO-178B specialists who refer to themselves as software safety engineers.

Some people have experience with software DALs, others with software SILs, others with neither. There are people who have experience with the application of formal methods. Some are experienced with software fault tree analysis. Some system safety engineers, like the ones we have on board here, have expertise in software safety as well.

Software Safety Program Plans

In our July newsletter we mentioned Software Safety Program Plans. Do they always exist where necessary? No. This constitutes a serious omission. If they exist, are they separate documents? Often not—they form a section of the System Safety Program Plan which is fine.

When looking for guidance should we seek out IEEE 1228—Standard For Software Safety Plans? Our answer is no. We are not impressed by this standard. We recommend the JSSSC Software System Safety Handbook and the FAA System Safety Handbook.

There will be more to come in the future on these Plans and related issues such as Software Safety Working Groups.

Questions From Our Readers

Q. In July's issue you state that the Software Control Categories (SCCs) from MIL-STD-882C are a bad idea?
A. Our initial response to this question is that there was no companion software guideline produced (similar to RTCA DO-178B) which was SCC-driven. That said, we admit that we have issues with "level-driven" approaches such as SCCs, DALs and SILs but this discussion will have to wait until a later time.

Q. In August's issue you say that hardware means much more than electrical and electronic elements. Please expound.
A. Hardware also implies other elements such as pneumatic and hydraulic. Some people include mechanical elements as well.

Q. I would like to know what general lessons you have learned as a result of your forensic investigations.
A. We promise to provide this is. One of the lessons learned is that people need to focus more on the maintenance of their systems as problems are often introduced during this phase. We will expand upon this in a future issue.

Railroad Safety Program Plan

Some of our U.S. railroad clients have been required to comply with 49CFR236. Section 905 requires the implementation of an FRA-approved RSPP. This Plan must be enforced and updated as necessary.

We have reviewed a number of these which have been virtually identical. It is apparent that experienced system safety engineers were not used to produce the first one from which the others spawned. Had this been the case, the it would have benefited both the railroads and their suppliers.

As a further note we believe that an SSPP should also be generated for each project requiring an RSPP and that the SSPP contain a plan for software safety.

We will more to say about 49CFR236 in the future.

SAFECOMP 2008

This event is taking place September 22-25 at Newcastle upon Tyne, UK. For further information, visit http://www.safecomp2008.org.

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—September 2008

Human Error

We concluded our coverage of human error in August's newsletter with a question: "What can we do in the absence of THERP, HEART, JHEDI, etc., HFEs and field data?"

Before we answer this, we should say a bit more about field data. In some cases, pertinent data has simply not recorded. In other cases, these error rates (e.g., those associated with near misses) are known but it is not "desirable" to release this information to the outside world.

Ok, back to the question. We are assuming that there are limitations which prohibit the use of THERP, HEART, JHEDI, etc.. Perhaps the largest impediment is cost.

We could convene an expert panel from the client and, based on their experience/insight, converge on the required error rates.

There is another choice. Remember that, at this point, we have a blank sheet of paper. If we can use a logical, reasoned approach, keeping in mind the bounds of human error rates, we are much closer to where we need to be. Let's begin by using a good reference source for raw human failure rates for EOO, EOC, and CTE. Take this one step further and adjust these failure rates based on the existence of established written documentation and procedures. Adjust this again based on training and certification. Adjust this further based on the influence of a companion operator, if applicable. There are sources for this type of data. Thus far our estimates are not considering the specifics of the situation. We need to adjust our estimates considering exposure.

Ideally we need to adjust our estimates based on other factors such as lighting, the presence of cues, time of day, operator workload, task frequency, etc. but this becomes increasingly more difficult.

Remember, don't forget to list the assumptions you have made along the way. Be consistent in terms of how you apply the failure rates that you have derived. Have your data reviewed by the resources available to you.

We welcome your feedback on this article!

Standard Development

As safety engineers we need to be involved in the development of standards and regulations (e.g., MIL-STD-882E, RTCA DO-178C, CFRs). This requires sponsorship by our employers or, in the case of consultants, our customers. If you have been around long enough you will recall situations where you had to comply with a standard/regulation wishing that you had spent the effort to try to influence it before it came into play.

Face Lift

Our web site, despite a great deal of content, has been in need of a face lift for a very long time. We always seemed to be too busy in our daily routines to have the time to devote to its redesign. A decision has not been made to proceed and, before too long, you should see the net effect.

Commitment

The content of these newsletters is dependent on our freeing up the time within our busy schedules. They of course require review by others prior to their release. For this reason you are bound to see some variability in the length of the articles and of the newsletter itself from month-to-month.

Feedback

We encourage your questions, feedback, announcements and articles that you may wish to submit.

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com