HCRQ, Inc.

"The Key To A Safer World"

Newsletter—February 2009

Quizzes

Just how well did you fare on our first two quizzes? Well, to paraphrase Emeril Lagasse, it is time to "kick it up a notch".

We left you with a question in the last newsletter: "Just How Important Is The Selection Of The Programming Language in a Safety-Related System?" Any guesses? Well, prior to providing you with the answer, let's give you Quiz #3 in its entirety.

Good luck!

Quiz #3

1. Just How Important Is The Selection Of The Programming Language in a Safety-Related System?
2. How Do You Analyze The Safety Of Functional Changes To A System When No Safety Analysis Exists?
3. Should You Consider Software Sneak Analysis?
4. I Am A Safety Engineer. I Have Too Many Active Projects. Additional Safety Engineers Are Not Available. The Bean Counters Make It Difficult Just To Order Books And Standards. What Can I Do?
5. The Target Probability Of Catastrophic Failure Of 10^{-9} Originated From Avionics. What Is The Basis For Using The Same Target In Rail Systems?
6. Are Development Assurance Levels From SAE ARP4761 Equivalent To Safety Integrity Levels?
7. When Preparing A Minimal Equipment List (MEL - Avionics) Do I Repeat My Safety Analyses Considering Various Unavailable Equipment?

Now check the answers on the next page.

Questions From Our Readers

Q. Do you have plans to offer your 3-day courses as webinars?
A. Prior to this recession, the answer was no. People prefer to see the instructor and certain things are more optimal in a classroom environment. However, training budgets these days are either non-existent or very lean, and travel budgets are also tight. You can't argue with cost—no travel costs, reduced tuition fee, and you can opt to remain at home for the training. We will be making announcements!!

Q. Has it been your experience that PHAs are requested as final deliverables?
A. Yes, unfortunately. PHAs are intended to be delivered early in the development cycle and never later. It is illogical to provide PHAs either late in the development cycle or as final deliverables. The client really needs to be educated about the difference between the PHA and the hazard log and should be requesting the hazard log. Would you consider requesting a PHA for a legacy system—we hope not. For further insight into PHAs, refer to the October newsletter.

Q. How do we avoid cost overruns in system safety?
A. This is a very good question. Cost overruns in system safety are very common. Here are a few ideas:
(a) Verify that your client's SOW and DIDs are well written, unambiguous, and not disjointed. Involve your best system safety engineers as early as possible. Use them to vet these items and to prepare a PHL to assist in the cost estimation process.
(b) Beware of overzealous client representatives leading to excessive iterations. Use your best/most aggressive system safety engineer as a liaison with the client on all safety issues. It is preferable if the safety expertise of this person exceeds that of the client.
(c) Try to encourage client use of an experienced system safety engineer. The road ahead will be much less bumpy.
(d) Reuse formats, analyses, documentation, and databases from other projects as much as possible. Obtain templates for analyses and documentation if you do not already have them.
(e) Use good software tools (e.g., FTA programs) that are easy to use, maximize analysis and minimize operator involvement.
(f) Use safety engineers to analyze and alleviate them from work that can be performed by less skilled people.
(g) Try to minimize interrupting your safety engineers. Both productivity and accuracy (due to loss of context) tend to suffer.
(h) Be very careful writing SOWs for subcontractors. It is not uncommon for system integrators to get stuck performing system safety work which should have been performed by the subcontractors.

No doubt we could come up with other ideas but this will get you started in the right direction.

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—February 2009

Answers to Quiz #3

1. The selection of programming language is important as is the definition of a language subset and the provision of coding guidelines. Some guidance is provided in IEC 61508 although there are other sources as well. This said, let's put this into perspective. Very successful safety-related systems have been developed using languages that are not strongly typed or object oriented. It is important to note that we do not have field data that correlates programming language to failures/hazards/accidents. One of the questions that needs to be asked is "How important is the programming language relative to many other aspects of system safety (e.g., requirements hazard analysis)?"
2. This is a real life dilemma. There are many existing safety-related systems, in probably all sectors, for which no system safety analyses were performed. It would be eye-opening to discover just how many systems fit into this category! In the ideal world we would analyze the safety of the entire system including the new functions, implement safeguards where needed, and ensure that the addition of the new functions did not negatively impact the overall safety of the system. However, this is usually impractical and cost-prohibitive. Imagine the system is a missile! End of story! The first step is to identify the hazards associated with the complete system so that one will know the significance of the end effects of failure modes associated with the new functionality.
The next step is to perform safety analyses (e.g., FMEA, FTA) of the new functionality while taking advantage of the insight of the engineers who are most knowledgeable of the existing system design. In addition, utilize the knowledge of these people to help define new test procedures and to refine the current ones.
3. Our advice is no. Sneak Circuit Analysis, yes although one should understand what one is getting into by undertaking this. Use a good static code analyzer instead of Software Sneak Analysis.
4. This is another real life dilemma. Too many projects, too few safety engineers. Sometimes the situation is so severe, one does not have time to perform safety analyses as one moves from meeting to meeting. Anyone who has performed FTA before realizes that it takes a certain amount of uninterrupted time just to resume where one left off, let alone to progress the analysis further. This situation is sometimes driven by the company's client who expects more but expects to pay less. Safety budgets are slashed to the point where even ordering books and standards requires an act of congress. An obvious solution might be to transfer into another department or simply resign. One suggestion is to increase the system safety and software safety awareness of the system and software designers. Another idea is to focus on the techniques that offer the "biggest bang for the buck". System safety and software safety analysis techniques, guidelines, etc. do not weigh the same (e.g., requirements analysis).
5. There does not seem to be an analytical justification for using this target in rail systems. There is a justification in avionics (however crude) based on accident rate, contribution of aircraft failures to accidents, and an estimate of the number aircraft hazards.
6. No they are not equivalent. SAE ARP4761 development assurance levels are derived based on hazard/failure condition severity alone. Safety integrity levels are derived based on hazard risk. Thought must be given to this situation when preparing SOW and DID text as one bidder may be using SAE ARP4761 while another may be using MOD 00-56. The one using SAE ARP4761 will map nicely to DO-178B. The one using safety integrity levels needs to give some thought to mapping to DO-178B.
7. As safety engineers, we would like to say yes. Practically though, this is cost-prohibitive. For this reason, it has been our experience that qualitative safety assessments are performed when assembling an MEL.

Our Face Lift

At long last, we are now days away from having our new web site uploaded!! What a relief!!

Update—Technical Writing

Last month we announced a new offering for us — technical writing.

Perhaps it is the economy that has resulted in a very healthy response as everyone is cost-conscious these days and it is easy to save money this way.

Thus far, the bulk of the interest shown has been in scrubbing down documents (e.g., SOWs, white papers, SSPPs, SARs).

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com