

## June? Newsletter

We are expecting to ramp up quickly to fully-loaded in June. For this reason we are issuing June's newsletter early.

## New Webinar Estimating Probabilities of Human Failures

If you are curious, please follow the link on our home page.

## System Safety Course Updated Course Outline

One of the updates includes coverage of GEIA-STD-0010.

## Software System Safety Course Announcement

In the March 2010 issue, we mentioned that we would be extending this course from 3 days to 5 days. No wonder—the slide count is now 800.

After further deliberation, we concluded that 4 days would be the most optimal length for this course. This change is now in effect.

## Questions From Our Readers

**Q.** What, in your experience, is often poor in SSPPs?

**A.** Two things come to mind: 1) no software safety section given that there is no separate software safety program plan, and 2) poorly defined hazard severities, hazard risk assessment matrix, and risk classes. There are other areas as well.

**Q.** In a previous issue you asked the question "The target probability of catastrophic failure of  $10^{-9}$  originated from aviation. What is the basis for using the same target in rail systems?"; however, I did not see your answer.

**A.** Unlike its derivation in the field of aviation, we are not aware of a reasoned justification for its use in the rail industry.

**Q.** Have you encountered safety "engineers" who do not have university degrees yet are adept in system safety?

**A.** Yes. Although it has been our experience that the bulk of safety engineers do have university degrees, there are two people that immediately come to mind who are utterly amazing and it has been our pleasure to have met them.

**Q.** Do you plan to offer "Applying EN50126, EN50128 and EN50129 To Existing Systems" as a webinar?

**A.** Yes. Likely within the next two weeks. An announcement will be placed on our home page.

**Q.** What was the most stressful safety contract that you worked on?

**A.** With no hesitation, even though this was years ago, the THERAC-25. We were performing safety analyses on this system which had delivered fatal overdoses of radiation; however, the machines continued to be used while we were analyzing. It was a race to analyze, document, and "fix" before the next accident took place and another person lost their life.

**Q.** We know the definition of a hazard; however, we continue to struggle with the hazard descriptions for our system. Are we alone or do other people have the same difficulty?

**A.** You are definitely not alone. This is quite common. We have helped many people in this regard. We would add that people also experience trouble with the usage of terms such as safety-critical, vital, software hazard, etc. This problem was mentioned in the March 2010 issue.

## Spring Special

The month of June remains as a customer appreciation month for our valued repeat clients

Lockheed Martin  
Raytheon

Discounts are available to them on all courses and webinars.

Telephone :  
757-564-7703

Fax :  
757-564-7704

Email :  
info@hcrq.com

Web :  
www.hcrq.com