HCRQ, Inc.

"The Key To A Safer World"

Newsletter—July 2008

Our first newsletter met with success with us receiving thanks and requests for additions to our distribution list.

It is now time to make things a wee bit more interesting. This can be a challenge due to a diverse audience but we promise to provide you with both information applicable to all safety-related sectors as well as to specific sectors.

SMP, SSPP, et al

Remember the days when only SSPPs were required? Not too long ago we saw the emergence of the requirement for Safety Management Plans (SMP). The SMP describes the overall safety effort within the contractor's organization. Its role is to emphasize the management aspect of system safety but not the technical /analytical aspect (leaving that up to the SSPP which is project-specific). However, we sometimes see SMPs with embedded SSPPs, and we sometimes see comprehensive SSPPs which include it all.

Sometimes we see Integrated System Safety Program Plans (ISSPP) which are required when we have large complex systems involving multiple subcontractors. In some cases we have distinct plans covering product development, construction, T&C, and O&M. Sometimes there are unique safety plans such as FRA's Railroad Safety Program Plan (RSPP). More about the latter will be forthcoming. Software Safety Program Plans? We'll save this for future discussion.

An important element of safety management is the Corporate Safety Policy. The safety plan should reference this policy an/or include salient elements of it.

SMPs and SSPPs should be solid documents, written with a great deal of care. For one thing, they can be an immediate target of lawyers should an accident occur. HCRQ offers a comprehensive Webinar on SSPPs.

Historical Data

As system safety professionals we all understand the significance and the importance of historical data (lessons learned) from previous systems. A number of companies have developed databases which are accessible by all employees. Unfortunately, often these are not used—either people neglect to input information or they do not review its contents during new product development with the net result being the same flaws being introduced into the new product.

Hazard Severity

If you use MIL-STD-882C as a guideline, you no doubt are familiar with the definitions provided for the various hazard severity levels. It is a fundamental mistake though to use them verbatim. For example: What is "severe injury"? What is "major system damage"? Your SSPP should use explicit definitions.

Safety Levels

Let's ignore software control categories within MIL-STD-882C (this is not a bad idea anyhow). This leaves 2 approaches: the first being Safety Integrity Levels (SILs) per IEC 61508 for instance, and the second being Development Assurance Levels (DALs) per SAR ARP4761. SILs range from 4 to 1 with 4 being the highest. DALs range (essentially) from A to D with A being the highest. Does this imply that SIL 4 is equivalent to DAL A. No. For one thing, SILs and DALs are derived differently. This is one of the reasons why DefStan 00-56 changed the way that it did—it removed SILs in an attempt to eliminate "SIL wars". It is worthwhile mentioning that MOD and DOD are discussing ways of reducing the difference between 00-56 and 882.

Forensic Engineering

We have had the opportunity to perform post-accident analyses for companies whose systems have failed catastrophically.

Our first analysis was performed on the THERAC-25. Each of these analyses was not only challenging but very sobering. We learned some valuable lessons along the way. We also gained insight into corporate litigation and professional liability.

We promise to provide you with useful insight in the future but, suffice to say for now, these designs are not the worse we have seen.

A Personal Note

When we first began specializing in safety in 1986, we did so because we had a desire to benefit mankind. Life is a gift. It is precious. And it is often too easily taken from us. We wish you, your families and loved ones well.

Telephone :
757-564-7703

Fax :
757-564-7704

Email :
info@hcrq.com

Web :
www.hcrq.com