

Journal of  
System  
Safety
eEdition

A publication of the System Safety Society

Home
Subscriptions & Memberships
Contact
About eJSS
System Safety Society



## From the Editor's Desk

[Download printable PDF of this page](#)

### To DAL or Not to DAL?

by **Clif Ericson**

President's Message

From the Executive Vice President

From the Editor's Desk

Outside the Lines

In the Spotlight:

- The Use of Safety Cases in Certification and Regulation
- Safety Implications of Software in Safety-Critical Devices

System Safety in Healthcare

- Swiss Cheese Model for Investigating the Causes of Adverse Events

Announcements

Gains from Losses:

- Facts, Fiction and Public Perception

Book Review:

- Murder by Electrocution, by David MacCollum

Unintended Consequences:

- TWA Flight 800 Accident

Opinion (MacCollum)

Upcoming Conferences/Calls for Papers

Chapter News

Mark Your Calendar

About this Journal

Advertising in eJSS

Contact Us

Puzzle

As many readers know, DAL refers to "design assurance level" — or is it "development assurance level?" I have seen both. Either way, the DAL concept is a nifty idea whereby a system, subsystem or software item is built to a specified DAL. There are typically five DALs, where level one (or level A) requires the most stringent development rigor, while each lower level requires less rigor. This methodology presupposes that the more rigor applied, the safer the resulting design; however, there does not seem to be evidence supporting this theory. ARP-4754A now has multiple DAL levels; there is the Functional DAL (FDAL) and the Item DAL (IDAL). Does this strike anyone else as confusing? My concern is: Do DALs replace or ignore the proven system safety process? ARP-4754A does not even call out or discuss hazard analysis, hazard risk or hazard elimination/mitigation. What am I missing here?

The first technical paper in this issue, "The Use of Safety Cases in Certification and Regulation" by Dr. Nancy Leveson, discusses the certification of safety-critical systems using safety assurance cases and global methods, including the impact of regulations. This paper uses the term "assurance cases" in general and limits the use of the term "safety case" to a specific definition as an argument for why the system is safe. It also examines the use of safety cases and some dangers associated with their use.

The second technical paper in this issue, "Safety Implications of Software in Safety-Critical Devices" by Amber Schauf, discusses three specific cases in which a software error was the culprit in a safety-critical device. While discussing software errors, this paper elucidates the relationship between electronics and software.

In his "System Safety in Healthcare" column, Dev Raheja discusses the "Swiss Cheese Model for Investigating the Causes of Adverse Events." He expands upon Reason's Swiss Cheese model for human error and describes how it is used in the healthcare industry.

In his "Gains from Losses" column, John Livingston delves into how the Tennessee Valley Authority (TVA) has made a significant impact on the Huntsville, Alabama area during the last 80 years. He discusses some myths, misperceptions and truths regarding commercial nuclear power safety.

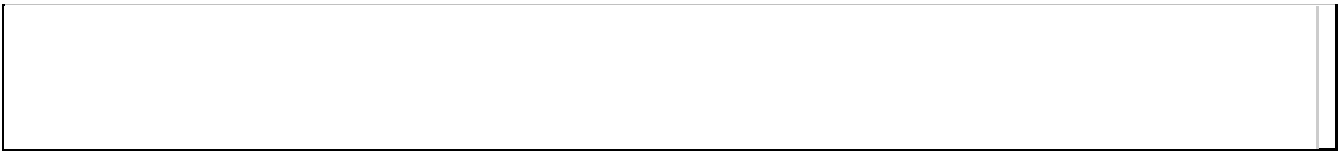
In his "Unintended Consequences" column, Terry Hardy describes a past mishap and the lesson learned from that mishap. The mishap in this issue is the TWA Flight 800 accident, which occurred on July 17, 1996. In case you have forgotten, this is a significant lessons learned regarding ignition of fuel in the center wing fuel tank, where the tank was regarded as being ignition source-free.

In their Outside the Lines Column, Benner and Rimson discuss the state of the International System Safety Society. They suggest that the ISSS has never subjected itself to an analysis similar to those its members apply to the hazards and risks, and that perhaps we should. In their column, they present a system safety analysis of the ISSS. In order to understand concerns and challenges to the ISSS, they have developed a short questionnaire they would like readers to respond to. They will devote a future column to the results of this survey, so please participate.

Remember, if you wish to opine, send me an email at [journal@system-safety.org](mailto:journal@system-safety.org).

Until next time,  
Clif





Copyright © 2011 by the System Safety Society. All rights reserved. The double-sigma logo is a trademark of the System Safety Society. Other corporate or trade names may be trademarks or registered trademarks of their respective holders.

