

— Some Common Errors in Analysis — Independent Reviews Uncover Flaws

P. L. Clemens, P.E., CSP
Safety Engineering and Analysis Center, APT Research, Inc.

Background / Introduction

In the practice of system safety, competent and well-intentioned analysts often commit errors that defy discovery by those who make them. Once an analysis has been completed and a solution has become evident, analysts often succumb to a mind set that precludes further consideration. Acquiring independent third-party reviews is a practice that reduces the likelihood of analytical errors, thereby endowing analyses with heightened credibility. Performing external reviews forms an arena of system safety practice that now enjoys increasing popularity, driven in part by the ever-increasing complexity of systems and in part by the need to be prepared for the eventuality of litigation.

This paper describes three kinds of errors that are often encountered in conducting independent reviews. In the first, the analyst has both miscounted failure opportunities and neglected to sum partial risks, the latter for an instance in which they are individually acceptable although their unseen total may far exceed a rational tolerance threshold. In the second example, an analytical method has been misapplied leading both to a faulty result and to a vain and costly attempt to reduce risk. And in the third, an error is made in moving from the reality of the system to the conceptual model that is then analyzed. The result is a flawed understanding of system vulnerability. In all three examples presented here, system designs and their applications have been altered to disguise ownership.

Unsummed Partial Risks

Figure 1 shows an air cargo tie-down system. Its integrity is critical. Three straps and six floor-bolted brackets restrain the load. To determine whether risk is acceptable, the analyst has performed a Preliminary Hazard Analysis (PHA). Results appear in Table 1. There, one of the three tie-down assemblies has been analyzed as being typical of the three. The potential failure modes available to each assembly element have been recognized individually as hazards. This approach is not uncommon. A failure at any one of the line items shown in the analysis is scored as leading to a severity-level II, “Critical,” mishap. Failure probability for each is judged at the “D” or “Remote” level for the anticipated interval of use. (Hazard severity and probability levels are taken from MIL-STD-882D.) Risk assessed as II/D is customarily regarded as acceptable. By many, risk would be seen as tolerable for each line-item in the PHA hazard inventory. As a result, the tie-down system was judged to be “safe.” But, *is it, really?*

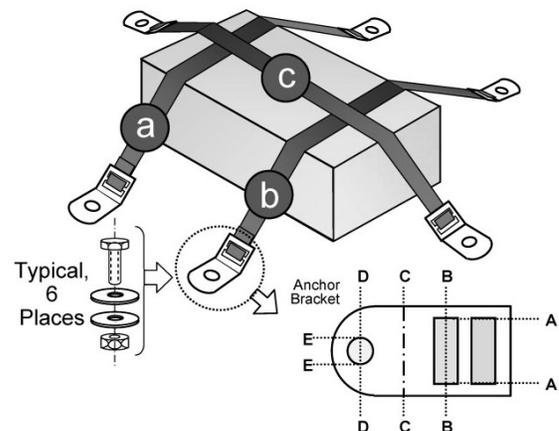


Figure 1 — Tie-Down System



***Thank you for your
interest in our papers!***

*For the rest of the paper, please email
aptinfo@apt-research.com*