Understanding and Applying Total System Risk Summing
(As Outlined in the Risk Summing Guidebook)

William T. Edmonds, CSP, Headquarters Army Materiel Command, Redstone Arsenal, Alabama, USA

P. L. Clemens, PE, CSP, A-P-T Research, Inc., Huntsville, Alabama, USA

Tom Pfitzer, President, A-P-T Research, Inc., Huntsville, Alabama, USA

R. G. Baker, Chief Analyst, A-P-T Research, Inc., Huntsville, Alabama, USA

M. A. Emery, Senior System Safety Engineer, A-P-T Research, Inc., Huntsville, Alabama, USA

Abstract

System safety, in majority practice, does not assess whole system risk. Instead, as most often applied, system safety subjectively assesses the separate partial risks of individual hazards identified as posing risk to valued assets. Risk acceptance authorities then judge the acceptability of whole system risk based exclusively on their consideration of these numerous partial risks. As a result, systems are committed to operation with acceptance of whole system risk but without knowledge of its overall value. This shortcoming has long been recognized, but has gone without remedial attention in the standards guiding practice of the discipline. Risk Summing ideas and techniques applied in routine system safety practice date back to 1972. This paper incorporates some of the early concepts and strategies as well as more recent research and case studies. In 2005, an international risk summing workshop arrived at consensus on criteria for a risk summing method. Such a method, now developed and described herein, satisfies requirements for simplicity, universal applicability, and interpretability of results. In addition to summing, it recognizes a family of aids for characterizing and interpreting total system risk. Opportunities for conservation of resources while lowering overall system risk are also made apparent.

Introduction

The mission of the Defense Safety Oversight Council (DSOC) Acquisition and Technology Programs (ATP) Task Force is to investigate and recommend or implement changes to policies, procedures, initiatives, education and training, and investments to ensure that acquisition programs address safety throughout program life cycle. DSOC funded development of the Risk Summing Guidebook (ref. 1) to provide the system safety community with a means to generate and communicate whole system risk. This paper provides a summary of the Risk Summing Guidebook and details for using the methodology and process defined by the guidebook. In addition, the guidebook contains background information, supplementental information, and practical worked examples and should be used to obtain more detail and explanations.

The Need

In today's most prevalent mode of system safety practice, the assessment of system risk begins by identifying system hazards, i.e., the sources of potential harm to identified assets. These individual hazards are then analyzed singly as line item entries in an inventory. The process can be modeled by a multiple path flow representation, as in Figure 1. Here, the system safety analyst first examines the individual hazards (H_1 through H_n) as to the severity of the harm that each would be expected to inflict (S_1 through S_n), and these data are recorded. Similarly, the probability that harm at that level of severity might occur is examined and recorded (P_1 through P_n).The analysis product is a line-item inventory of individual system hazards and their risk, as arrived at subjectively.

Thank you for your interest in our papers!

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