Hazard Analysis: Determining Context for the Use of Formal Methods

Peter Lindsay
Software Verification Research Centre,
The University of Queensland, Australia 4072
pal@it.uq.edu.au

Formal methods are frequently recommended for critical software components of safety-related systems. How does one determine what are the critical components and what are their critical requirements?

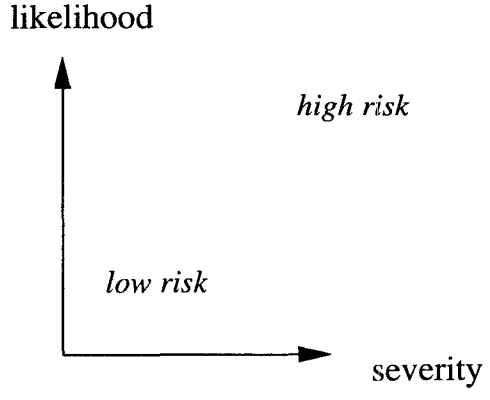

Figure 1. Risk = severity × likelihood.

This tutorial presents an introduction to Hazard Analysis and some of the techniques that have been successfully adapted to software, including:

- Failure Modes and Effects Analysis (FMEA)
- Fault Tree Analysis
- Event Tree Analysis
- Hazard and Operability Studies (HAZOP).

The tutorial will demonstrate how hazard analysis can be applied to derive safety requirements against which designs should be verified.

It will outline a number of important standards for safety-related software, their approaches to defining integrity levels, and their recommendations for use of formal methods.

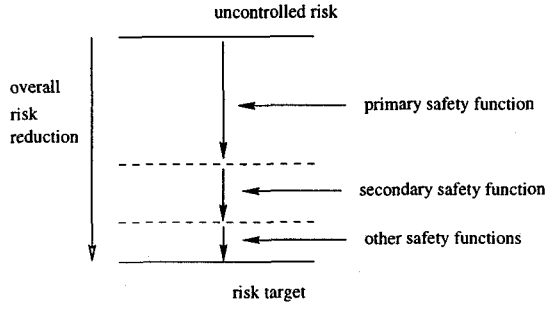

Figure 2. Principles of risk reduction.

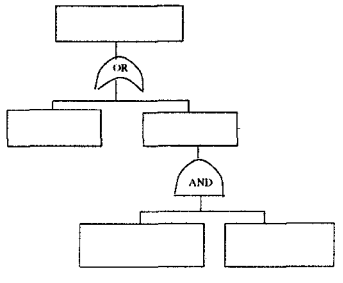

Figure 3. Example fault tree.

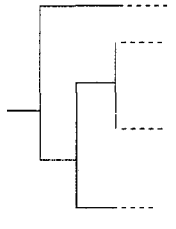

Figure 4. Example event tree.