Safety Critical Systems Analysis

18-849b Dependable Embedded Systems

Robert Slater

February 23, 1999

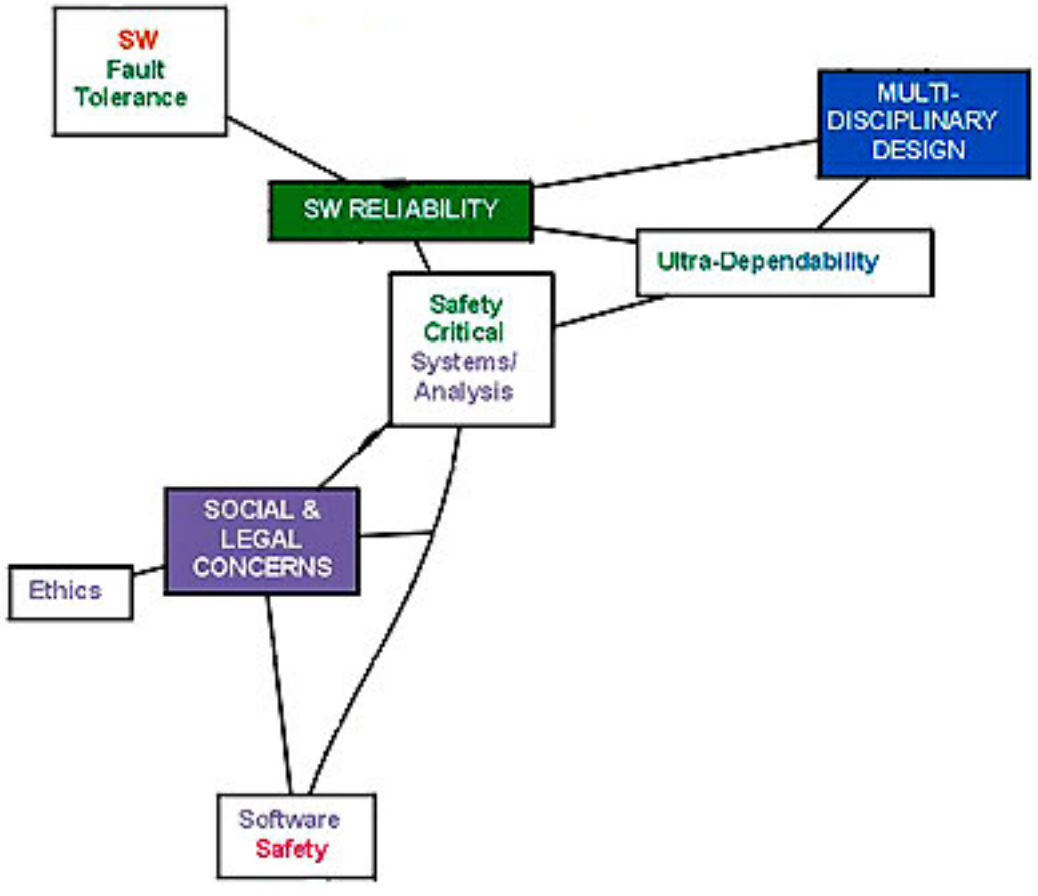
Required Reading:	**Defense Standard 00-58: HAZOP Studies on Systems Containing Programmable Electronics** **http://www.seasys.demon.co.uk/0058h/0058.html**
Best Tutorial:	**Storey, Neil. Safety-Critical Computer Systems. 1996 Ch 3, 4.**
Authoritative Book:	**Blockley, David ed. Safety Engineering. 1992**

Carnegie Mellon

Overview: Safety Critical Systems Analysis

- **Introduction**
  - Connections all over the place
- **Key concepts**
  - Hazard Analysis
  - Risk Analysis
  - Fuzzy human factors
- **Tools / techniques / metrics**
  - Lots of analysis techniques
  - Fuzzy metrics
- **Relationship to other topics**
  - Social & legal, Ethics, SW Reliability, SW Safety, Ultra-reliable, Multi-disciplinary design
- **Conclusions & future work**

YOU ARE HERE MAP



Description of Topic

- **Well, Safety Analysis**
  - More specifically, it's a way of determining the ways in which a system is unsafe, and what has been done to prevent unsafe events from occurring
  - Also development of what is an acceptable level of safety
- **Comes from nuclear, avionics, civil engineering, chemical processing industries**
  - Often for certification
  - Original definition of safety comes from these field; "avoiding uncontrolled releases of energy"
- **Key Concepts and Definitions**
  - Hazard - a situation in which there is actual or potential danger to people or the environment
  - Risk - a combination of the frequency or probability of a specified hazardous event and its consequence
  - Risk Management - the reduction of risk to acceptable levels

Hazard Analysis

- **Analytical method to specify hazards**
  - Use guidelines to identify hazards, their root causes, and possible countermeasures
  - Generally follows a rigorous procedure/discipline, often based in committees
- **Probabilistic Hazard Analysis**
  - Add frequency or probability of occurrence to hazards identified
- **The Big Problem**
  - How do you know you got them all?

Risk Analysis

- **Carries the work of Hazard Analysis two steps further**
  - Identifies the possible consequences of identified hazards, and their probability of occurring
  - Combines these to acquire some sort of a 'risk level'
  - Identifies untenable hazards, prioritizes list for future work, and may identify safeguards to be used
- **Probabilistic Risk Analysis - heavy on the statistics**
  - Extensive modeling and number-crunching on determining peak loads and safety margins
  - Traditional probability distributions, First-Order Second Moment (FOSM) analysis, Monte Carlo simulation
- **The Big Problem**
  - How accurate is your estimation/calculation?

Fuzzy Human Factors

- **How much safety is enough?**
  - Obviously, safety costs
  - Human perception of risk an issue, as well as responsibility
  - How to account for human error
  - In some cases, it mean putting a monetary value on a human life
- **Some guidelines**
  - Regulations and codes spell it out
  - Sometimes in requirements
  - Other times, comes to a judgement call
- **Accuracy of results**
  - Highly dependant upon the people and knowledge involved
  - Can depend on ‘safety culture’

Tools / Techniques

- **Lots of analysis techniques**
  - Checklists, Fault Tree Analysis, Event Tree Analysis, Failure Modes and Effects (and Criticality) Analysis, HAZard and OPerability studies
  - All basically methodologies to make sure analysis is thorough
- **Metrics sometimes fuzzy**
  - Failures per year, fatalities per year, accidents per year, $ lost to lawsuits, etc…
  - Deliniating acceptability can be tough
- **Codes and regulations**
  - Lots of codes and regulations out there
  - IEC Standard 812, 1025, & 1508, Defense Standard 00-58, FAA, FCC, CAA, DoD, NRC, FDA, everybody's got them

Relationship To Other Topic Areas

- **Ultra-reliability**
  - 'Safety cases' can be made for untestable systems
- **SW Reliability, Fault Tolerance, & Safety**
  - Analysis techniques being adapted to the software domain
- **Multi-disciplinary design**
  - Often design overlaps with other areas because damage occurs in the physical world
- **Social & Legal concerns, Ethics**
  - Social values determine what is safe enough, and who is liable for injuries caused
- **Validation, Verification, & Certification**
  - Often used in 'safety cases' for certification

Conclusions & Future Work

- **Hazard and Risk analysis are both necessary for a true evaluation of safety**
  - Good analysis will come up with suggestions for dealing with identified hazards
- **Highly dependant upon the people involved**
  - Still an art, not a science; highly domain dependant
  - It's an emergent property, so while people grasp these poorly, they're our best shot
- **Ultimately management issues involved**
  - Perfect safety is impossible, so must determine: "How important is safety?"
- **Future Work**
  - Proving applicability in the computerized domain
  - Improving ease of use
  - Guidelines for ethical judgement calls

HAZOPS for programmable electronics

- **Tell you how to do safety analysis on electronic devices**
  - Isn't this exciting?
- **Key points**
  - HAZOPS - key words, analysis models, committee process
  - Adapts to new areas of concern in computerized systems
  - Guidelines in addition to requirements
- **What's the purpose for the standard?**
  - Trying to adapt old methods to new areas.