Safety-Critical Computer Systems

PhD Course, Fall 2000

Simin Nadjm-Tehrani
www.ida.liu.se/~snt

Organisation and planning

- Course page
  www.ida.liu.se/~snt/teaching/SCCS
  Course goals, litterature, web resources, schedule, invited lectures, examination details, etc
- Period: October-December´00
- Examination deadline: 01-01-10

Overview

- To get an insight into the broad area of system safety
- To get specific knowlegde about issues in designing safety-critical computer systems, and related standards
- Working in groups, 4 sessions
- 8 Lectures/resource sessions

This lecture

- Short historical perspective
- Basic terminology

Bang goes one billion dollars!

From Time Magazine, Aug 98

Titan 4 rocket

- blasted off on 19 August 1998 from Cape Canaveral
- as large a 20-story building
- carrying a top security satellite
- 40 seconds later it pitched sideways and had to be destructed by air force control command

Early computer-based systems

- 1944: Real-time computer system in the Whirlwind project at MIT, used in a military air traffic control system 1951
- Short life of vaccum tubes gave mean time to failure of 20 minutes

Early space and avionics

- During 1955, 18 air carrier accidents in the USA (when only 20% of the public was willing to fly!)
- 1970: Apollo 13 had less computing power on board than a PC produced ten years later

Still, misshaps/accidents not unusual!

1. **TCAS** is a system designed to avoid mid-air collisions between passenger planes. On 3rd February 1994 two commercial aircrafts came as close as 1.6 km to each other while flying over Oregon in USA.

2. ”Friendly Fire” - duringthe Gulf war 24% of american soldiers (35 av 146) killed by own systems.

3. On 8th February 1986, in Canada, a cargo train collided with a passenger train carrying 120 passengers - 26 people died.

4. During June 85 - January 87 six patients in USA and Canada got very high doses of radiation and severe burns from the cancer-treatment system **Therac 25**. Doses as high as 15,000-20,000 radiation units compared with the normal levels (~ 200 units) had been given. Three of the patients died due to the overdoses and the following complications.

Current trends

- Early (hardware-driven) engineering lessons ”forgotten”
- Significant technological changes (MEM´s, sensors, X-by-wire)
- Mishaps/accidents more likely to be due to complex computer systems in interaction with physical devices

What is safety?

Freedom from exposure to danger, or exemption from hurt, injury or loss.
[Bowen and Stavridou]

- Degrees of safety
- Closely related to **risk**

What is risk?

(1) A combination of the likelihood of an accident and the severity of the potential consequences.

(2) The harm that can result if a threat is actualised.

- The Pinto case
- Acceptable/tolerable risk

Hazards & system safety

- Achieved by anticipitating accidents, and eliminating their causes
- Hazards are potential causes of accidents

Conditions in a system which together with other factors in the environment inevitably cause accidents.

Safety & risk management

- Means anticipating accidents…
- hence anticipating hazards …
- which means quantifying/classifying the potential ...
- Must reduce risks which are not tolerable!

Fail-safe design in aerospace

No single failure or probable combination of failures during any one flight shall jeopardise the continued safe flight and landing of the aircraft. [FAA]

- But what is failure?

Errors, faults & Failures

- **Fault**: a defect within the system or a situation that can lead to failure
- **Error**: manifestation (symptom) of the fault - an unexpected behaviour
- **Failure**: system not perfoming its intended function

Fault ⇒ Error ⇒ Failure

- Goal of system verification and validation is to ”remove” faults
- Goal of reliability analysis is to focus on important faults, those which might lead to failures
- Goal of fault-tolerance methods is to reduce effects of errors if they appear - eliminate or delay failures

What is reliability?

A measure of an item performing its intended function satisfactorily for a prescribed time and under given environment conditions.

The measure is typically expressed as a probability, or time to failure

[Laprie]

Reliability and safety

- Note: reliability defined
  - over time
  - with respect to specified conditions
- Improving software or hardware reliability need not improve safety!

What is dependability?

*Property of a **computing system** which allows reliance to be justifiably placed on the service it delivers.*

[Laprie]

- Wider concept which covers ”safety”, reliability, security, fault-tolerance, availability ...

This course...

- Does not cover security
- Safety, correct behaviour in software, reliability for software and hardware, fault-tolerance, are touched upon
- Also tries to cover some aspects in the larger systems engineering domain