Safety-Critical Computer Systems

Standards and processes

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

Recall from earlier...

- 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.

This lecture

- What is the role of standards in achieving higher safety levels?
- Relating safety and system development life cycles
- Examples of standards applicable in various cases and some comparative analysis

Comparative analysis

- Excellent survey by Wabenhorst and Atchison

A Survey of International Safety Standards
November 1999

Defining responsibility

- Who is in charge? Who ensures that all major potential sources of accidents are investigated?
- Should standards be prescriptive or simply give guidance?

Overall responsibility

- Assuring safety is the responsibility of the purchaser not the producer of a system!
- The producer is responsible to deliver the product according to the specified requirements of the purchaser, and to ensure adherence by sub-contractors

Independent reviews

- Most standards mandate some independent review of safety-related processes or technical content (c.f. Hercules case)
- Who appoints the reviewer?
  - UK stan 00-56: the contractor & customer
  - Australian Def stan: independent of the developer

Safety process: relation to Development

- **Before:** Produce a plan to assure customer safety requirements
- **During:** Monitor the plan, deal with anomalies and residual risks, construct safety case
- **After:** Provide evidence, and maintain logs to monitor and continuously justify the decisions

Control procedures

- Progress in design affects the safety case
- All changes to the safety case must be reviewed and approved
- All post-development modifications to design or changes to operating conditions lead to new safety case

How to capture requirements?

- Standards require agreement between the customer and the developer
- Mandate use of structured design, assignment of safety integrity levels (SILs), and sometimes detailed guidance on languages, tools and methods

Hazard identification

- All standards require a preliminary hazard analysis as well as a later *system hazard analysis*
- Typically mandate FTA, FMEA, and similar techniques

Guidance on risk

- Standards typically leave measures of risk open: qualitative or quantitative
- But they force you to document which measures you allocate and to justify that!
- The levels of residual risk are used to allocate resources later

Design assurance

- How to ensure that every component´s design is in agreement with the safety requirements for that component to the extent required by the allocated SIL?
- Design specifications ”sufficiently formal”

Tools and techniques (1)

- Australian Def stan: model of component design verified against component safety specification
- MIL-STD-882: Safety tests
- UK Def stan 00-55: software requirements traceability, formal specs for design and requirements, analysis and prototyping

Tools and techniques (2)

- UK Def stan 00-54: use of formal specification language for design, use of analytic means, representative simulations
- DO-178B: requirements and SW architecture should be traceable, verifiable and consistent, SW-HW integration emphasised

Software specific

- safe subsets
- control flow, data flow analyses
- suitable test coverage criteria
- input failure modes, data rates, boundry tests
- formal proofs
- formally verified compilers!

Hardware specific

Hardware assurance outside the scope of:

- NATO STANAG guidelines for munition-related safety-critical *computing systems!*
- ARP 4754 guidelines for highly integrated complex aircraft systems, specially *electronic systems!*

Electronic hardware?

- UK Def stan 00-54: FTA and FMEA to cover random failures, physical test coverage, simulations, use of methods and CAD tools justified in relation to the safety programme plan

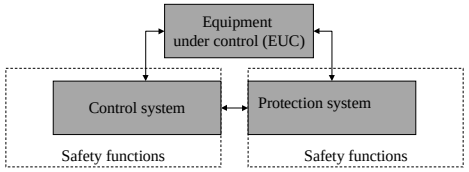
Human aspects?

- Surprisingly little attention in ARP, and outside scope of DO-178B!
- MIL-STD-882: Humans treated as components, and their errors covered by hazard analysis
- STANAG: Need for feed back mechanisms, concise and unambiguous operator displays

Closing discussion

- Do standards help?
- In what ways?
- To what extent?

Structure of safety-critical systems



Overall safety lifecycle (IEC 61508)