Software Engineering 4

Safety-Critical Systems

Andrew Ireland

School of Mathematical and Computer Science
Heriot-Watt University
Edinburgh

What Are Safety-Critical Systems?

- Any system where failure may, directly or indirectly, threaten human life or the environment can be classified as safety-critical, *e.g.*
  - ▷ Fly-by-wire control systems;
  - ▷ Military command and control systems;
  - ▷ Secondary air traffic control radar systems;
  - ▷ Automatic railway signaling systems;
  - ▷ Nuclear reactor control systems.
- Increasingly control mechanisms rely upon software rather than hardware which makes software of crucial importance within many safety-critical applications.

Definitions & Terminology

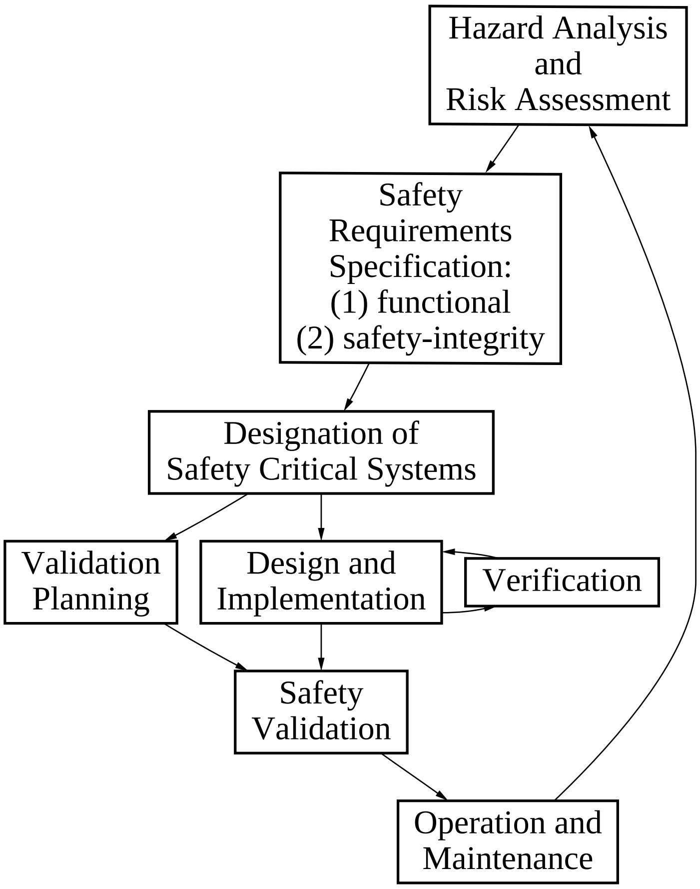
Leveson (Leveson, N.G. "Safeware: System Safety and Computers", Addison-Wesley, 1995):

- **Safety** is freedom from accidents or losses.
- An **accident** is an undesired and unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss (loss of life, damage to property or the environment).
- A **hazard** is a state or set of conditions of a system (or an object) that, together with other conditions in the environment of the system (or object), will lead potentially to an accident (loss event).

Definitions & Terminology (more)

- **Hazard severity** is the worst possible accident that could result from the hazard given the environment in its most unfavorable state.
- **Hazard likelihood** is the probability of occurrence.
- **Hazard level** is the combination of severity and likelihood.
- **Risk** is the hazard level combined with (1) the likelihood of the hazard leading to an accident and (2) hazard exposure or duration.

The Safety Life-cycle



Hazard Analysis

Hazard analysis represents the heart of an effective safety programme. The objective is to discover potential hazards and causes which may arise given a systems operational environment.

1. Hazard identification: determining what hazards might exist during operation of the system.
2. Hazard classification: order hazards with respect to hazard level (severity & likelihood of arising).
3. Hazard decomposition or causal analysis: an analysis of the individual hazards is carried out in order to determine root cause(s).

Example Hazard Severity Categories

US Department of Defense (MIL-STD-882B: System Safety Program Requirements):

Category I: Catastrophic; may cause death or system loss.

Category II: Critical; may cause severe injury, severe occupational illness, or system damage.

Category III: Marginal; may cause minor injury, minor occupational illness, or minor system damage.

Category IV: Negligible; will not result in injury, occupational illness, or system damage.

Hazard Likelihood Categories

Leveson (Leveson, N.G. 1995):

Frequent: Likely to occur frequently to an individual item, continuously experienced throughout the fleet or inventory.

Probable: Will occur several times during the life of an individual item, frequently throughout the fleet or inventory.

Occasional: Likely to occur sometimes during the life of an individual item, several times throughout the fleet or inventory.

Hazard Likelihood Categories

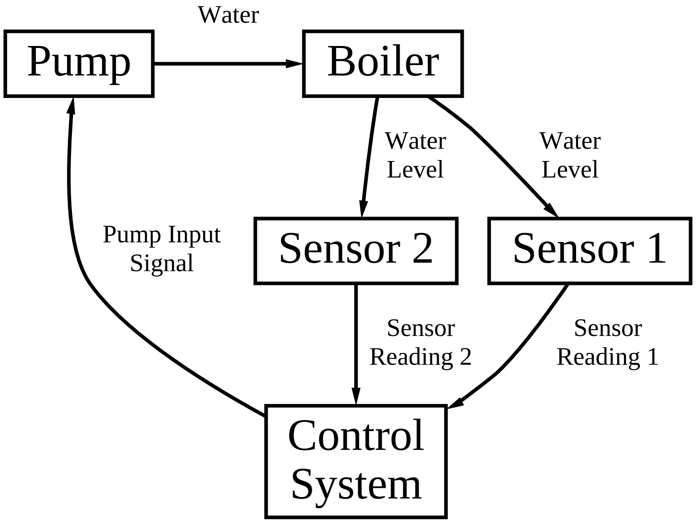
Leveson (Leveson, N.G. 1995):

Remote: Unlikely to occur but possible during the life of an individual item but reasonably expected to occur in an fleet or inventory.

Improbable: Extremely unlikely to occur to an individual item; possible for a fleet or inventory.

Physically Impossible: Cannot occur to an individual item or in a fleet or inventory.

Example: A Simple Boiler System

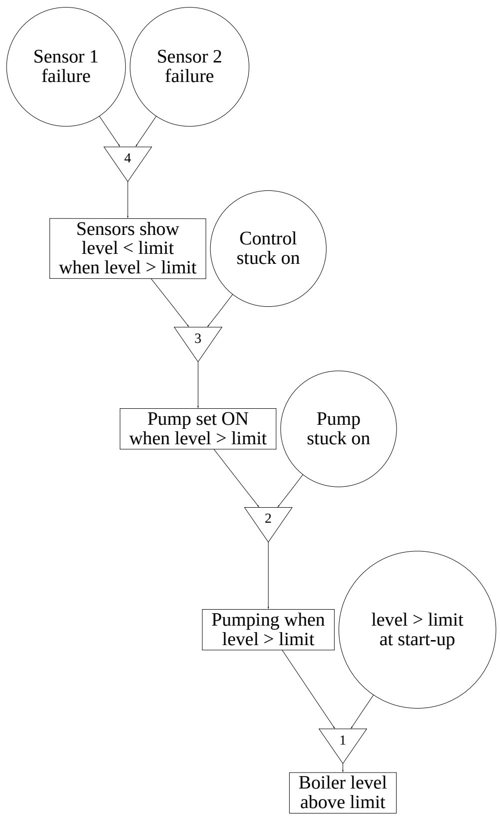


Hazard Analysis: Fault Trees

- There are many techniques for analysing hazards in order to identify the root causes. **Fault trees** are one such technique.
- Fault trees are used to show the causal links between systems events and particular system faults.
- Building blocks:
  - ▷ Basic events denoted by circles;
  - ▷ Intermediate events denoted by rectangles;
  - ▷ System fault denoted by the tree root;
  - ▷ Events are connected by AND- and OR-gates.
- As an example consider the following fault:

  "Boiler water level higher than safe limit."

A Fault Tree for the Boiler System



Note: • denotes AND while + denotes OR.

Risk Assessment

- Risk assessment follows on from hazard analysis and is involved in classifying the acceptability or **safety integrity** level of each hazard.
- This classification is based upon the:
  - ▷ hazard level for each of the identified hazards and
  - ▷ likelihood of an accident resulting from the hazard.
- During hazard analysis worst-case effects are usually only considered and simple qualitative methods are employed. In contrast risk analysis involves more quantitative analyses, *e.g.* statistical analysis based upon historical data.

Safety Integrity Level

Sommerville (Sommerville, I. 1995):

1. **Intolerable:** The system must be designed in such a way so that either the hazard cannot arise or, if it does arise, it will not result in an accident.
2. **As low as reasonably practical (ALARP):** The system must be designed so that the probability of an accident arising because of the hazard is minimized subject to other considerations such as cost, delivery and so on.
3. **Acceptable:** While the system designers should take all possible steps to reduce the probability of this hazard arising, these should not increase costs, delivery time or other non-functional system attributes.

Safety Requirements Specification

Hazard analysis & risk assessment identify safety-critical functions and associated safety integrity levels which provide the basis for a safety criteria used by the system designers, *i.e.* a statement of **what** has to be achieved with respect to each of the hazards (but not **how**):

1. Hazard avoidance: design so that the hazard cannot arise, *e.g. The "dead-man's handle" eliminates the hazard of a run-away train.*
2. Hazard probability reduction: design to ensure that hazards cannot arise as a result of any single failure, *e.g. install both software and hardware interlocks.*
3. Accident prevention: design to detect hazards and remove them before an accident arises, *e.g. automatic detection of aircraft engine fire linked with an automatic engine shut-down mechanism.*

Safety Case

- Safety critical systems require certification by a regulating authority, *e.g.* FAA, HSE, ...
- A **safety case** documents the safety justification for a system and provides basis for the certification process – *came to prominence through Lord Cullen's recommendations following the Piper Alpha disaster (1988).*
- A safety case records all the safety activities and should therefore be created early on during the development of a system.
- A safety case must also be maintained throughout the operational life of a system.

Safety Case: Key Components

- A high-level rigorous safety argument, *e.g.*

  if X fails then Y will prevent Z from occurring ...

- Supporting evidence, *e.g.* test data, mathematical proofs showing that

  Y follows from the failure of X and that Y will prevent Z.

- All assumptions need to be made explicit, an unjustified assumption represents a flaw in the safety argument.
- Safety cases are typically multidisciplinary, as a consequence hard to manage.

Summary

- The nature of safety critical systems
- The safety life-cycle
- Hazard analysis and risk assessment
- Safety requirements
- Safety case

  Further reading:

  "Safeware" Leveson, N.G. Addison-Wesley, 1995.

  "Safety-Critical Computer Systems" Storey, N. Addison-Wesley, 1996.