COM4506/6506: Testing and Verification in Safety Critical Systems

Dr Ramsay Taylor

Contents

Terminology

Accident

“An undesired or unplanned (but not necessarily unexpected) event that results in (at least) a specified level of loss.”

Nancy Leveson - Safeware: System Safety and Computers, 1995

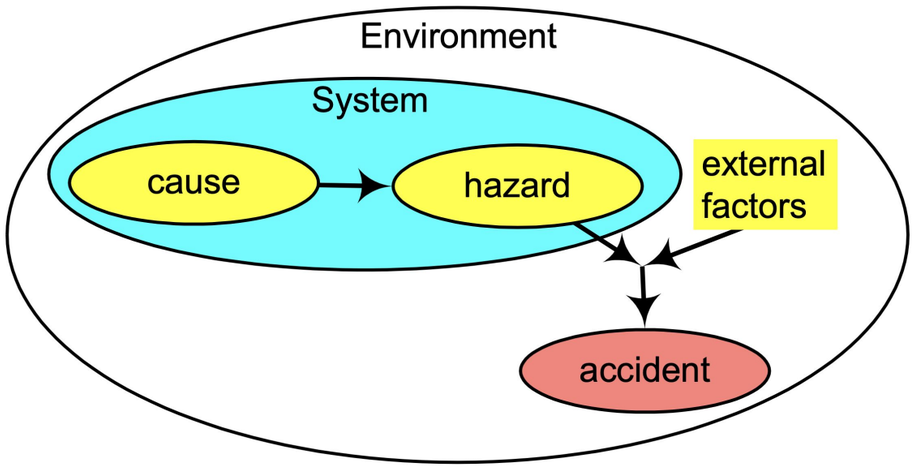
Terminology

Hazard

“A state or set of conditions of a system that, together with other conditions in the environment of the system, will inevitably lead to an accident.”

Nancy Leveson - Safeware: System Safety and Computers, 1995

Terminology



Risk Assessment

```
for h in hazards:
    risk[h] = severity(h) * likelihood(h)
if max(risk) > TOLERABLE_RISK:
    print("Er, I'm not sure this is a good idea!")
```

This does depend on us having a *complete* list of hazards to iterate!

Completeness in Hazard Analysis

Clinton Anderson:

Then what caused the fire?

Frank Borman:

A failure of imagination. We've always known there was the possibility of fire in a spacecraft. But the fear was that it would happen in space, when you're 180 miles from terra firma and the nearest fire station. That was the worry. No one ever imagined it could happen on the ground. If anyone had thought of it, the test would've been classified as hazardous. But it wasn't. We just didn't think of it.

From the Earth to the Moon, *TV mini-series, 1998*
Dramatisation of testimony before US Congress 1967 following the Apollo 1 fire.

HAZOP

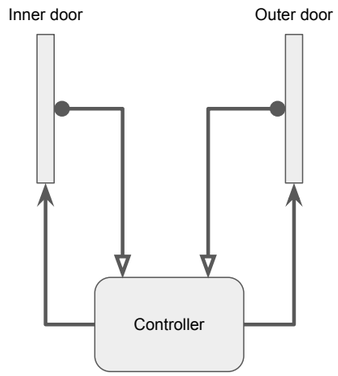
Hazard and Operability Study

- Originally applied to industrial chemical processes (in the 1960s)
- A *structured* approach to identify hazards in a system
- Requires a *structured* definition of the system!

HAZOP

Identify system components and interactions, and apply a series of ***guidewords.***

NO or NOT	**REVERSE**
MORE	**LESS**
BEFORE	**AFTER**
EARLY	**LATE**
AS WELL AS	**PART OF**
OTHER THAN	*[domain specific others]*



HAZOP

Signal	**Word**	**Result**
Inner Door Sensor	EARLY	Outer door could be released before inner is fully sealed
Inner Door Sensor	LATE	Delay in release of interlock. Potential for user frustration, leading to dangerous overrides.
Inner Door Sensor	MORE	Overvoltage in sensor causing damage to sensor transducers.

- HAZOPs are a *human* process, done by engineers and knowledgeable stakeholders
- They should prompt discussion and imagination!
- They are *exhaustive* (and exhausting!)
- The process should have a *facilitator* and a *scribe*

The results should be a large table of signals/interactions, guidewords, and results

Hazard Analysis

Other approaches also exist:

- Human Error Investigation Software Tool (HEIST)
- Systematic Human Error Reduction and Prediction Approach (SHERPA)
- ...

Summary

- *Hazards* are bad things that could happen, *Accidents* are them happening, and *Risks* are the quantification of the problems.
- The *completeness* of the Hazard list is limited by the completeness of the requirement, and by the limits of imagination.
- HAZOPs are one *structured process* that can improve completeness of hazard analysis.