Safety Critical Systems

Notes

Efraín Manuel Villanueva Castilla
February 18, 2020

Contents

1 | Objectives of the class

1. Understand the professional and social issues involved in the design and testing of fafety-critical systems.
2. Recognise the importance of standards and show a clear understanding of recent initiatives in this area.
3. Be able to apply a number of **risk analysis techniques** such as **Failure Modes, Effects and Criticality Analysis and Fault Tree Analysis**
4. Be able to apply a unmber of safety critical design techniques such as literate specification
5. Be able to apply a number of safety critical evaluation techniques such as Black Box testing and the observational evaluation of operator performance.
6. Be able to identify the main characteristics of an appropriate **safety culture** within large organisations

2 | Class Introduction

- What is a none-functional requirement?
  - Requirements that can't be tested in certain way
- What is ALARP and what is the relation with Safety Critical Systems?
- As Low As Reasonable Practicable (ALARP) vs As Low As Reasonable Achievable (ALARA)
- Testing can prove the presence of errors, but not their absence
- Is Safety "relative" or "absolute"?
  - Relative.You can only improve safety, not make it perfect

2.1 The Bathtub Curve

The bathtub curve is widely used in reliability engineering. It describes a particular form of the hazard function which comprises three parts:

1. The first part is a decreasing failure rate, known as early failures.
2. The second part is a constant failure rate, known as random failures.
3. The third part is an increasing failure rate, known as wear-out failures.

This is very used in hardware testing, because as the time pass the hardware ages and is has the following behaviour:

1. In the first part, the probability of failure is high because the hardware is new
2. In the second part, the probability of failure is low (constant), since known failures have been fixed
3. In the third part, the hardware is old and does not have more support or improvement, so the probability of failure goes up again

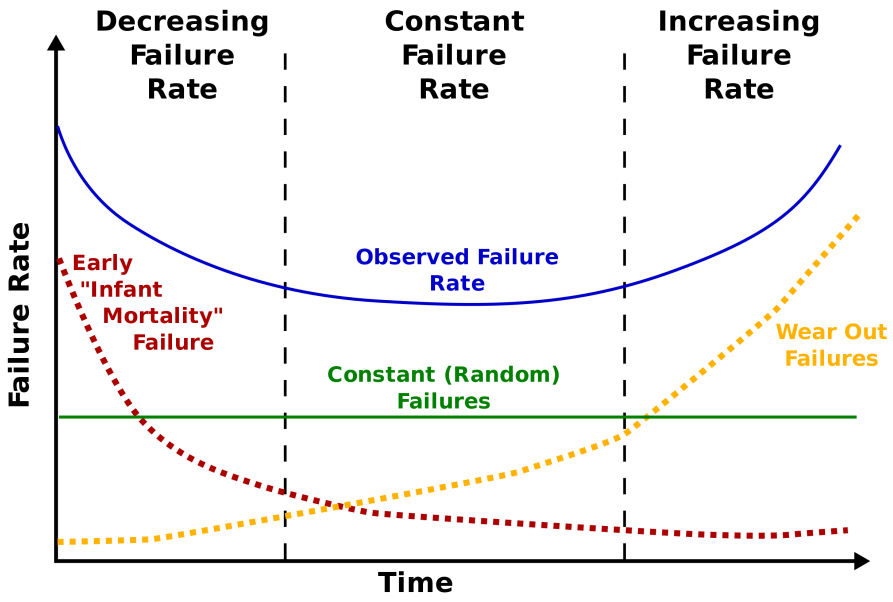

Figure 2.1: Bathtub Model representation

2.2 Safety Governance

Safety Governance. Provides the structure through which the vision and commitment to safety is set, the means of attaining safety objectives are agreed, the framework for monitoring performance is established and compliance with the legislation is ensured.

Three flawed forms of safety governance:

1. Market forces: 3rd party effects;
2. Tort and insurance: inefficent and retrospective;
3. State regulation: risk based, can be bureaucratic;

2.2.1 Market Focus

- People buy things even if the probabilities of death are high.
- Imperfect information. Companies not telling the truth about safety of their products
- θ Third party effect. Does apply for market forces, because it does not affect the buyer
- Some of the companies who causes detah to third parties, sometimes needs to pay for what their product caused

2.2.2 Tort and Insurance: inefficient and retrospective

- Legal fees do not improve safety
- Some companies are just fine for what their product did, but that does not improve safety
- Companies often get insurance
- Moral hazard. When companies feels very protected when they are sorrounded
- Government put limits (tops) to fines

2.2.3 State Regulation: risk based, can be bureaucratic

Different Format Regulation

- Government Organizations who prevents the sales of hazardous products
  - Standards and Organizations

Mens Rea → Guilty Mind

2 types of processes

1. Product base Standard
2. Process base Standar

2.3 Process Base Standard

- Standards
- Steps
- Specifications

2.4 Standard IEC 61508 and (26262)

International standard published by the International Electrotechnical Commission consisting of methods on how to apply, design, deploy and maintain automatic protection systems called safety-related systems. It is titled Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES).

- This is a Functional Systems Standard
- ≠ Publishing Audible
- The market forces are not enough so an Standard was build to ensure that companies follow the appropriate steps to have safety in their products

- A standards is a set of rules of conduct
- * Minor Changes. How much I have to change for the system is safe

IEC 61508

- Programmable Systems
- Across the process industries
- Zero risk is impossible
- Reduce Risks
- Reduce unnacceptable RIsks
- Demonstrate Reductions
- Implics High Level od Documentation
- Equipment Under Control **(EUC)**
  - Software is not hazard but hardware is