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 safety-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 number 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 is a term often used in the regulation and management of safety-critical systems. States that the residual risk shall be reduced as far as reasonably practicable.
  - A risk is ALARP when PROVED that the cost of any further risk reduction is grossly disproportionate to the benefit obtained from that risk reduction
  - 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
- What is safety?
  - Freedom from accidents/losses
- Accidents are complex multi-causal events, almost impossible to predict

Risk = frequency X cost

2.1 Terminology

2.1.1 Dependability

- Attributes
  - Availability - Security
  - Reliability - Security
  - Safety - Security
  - Confidentiality - Security
  - integrity - Security
  - Maintainability
- Means
  - Fault Prevention
  - Fault Tolerance
  - Fault Removal
  - Fault Forecasting
- Threats
  - Faults
  - Errors
  - Failures

2.2 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

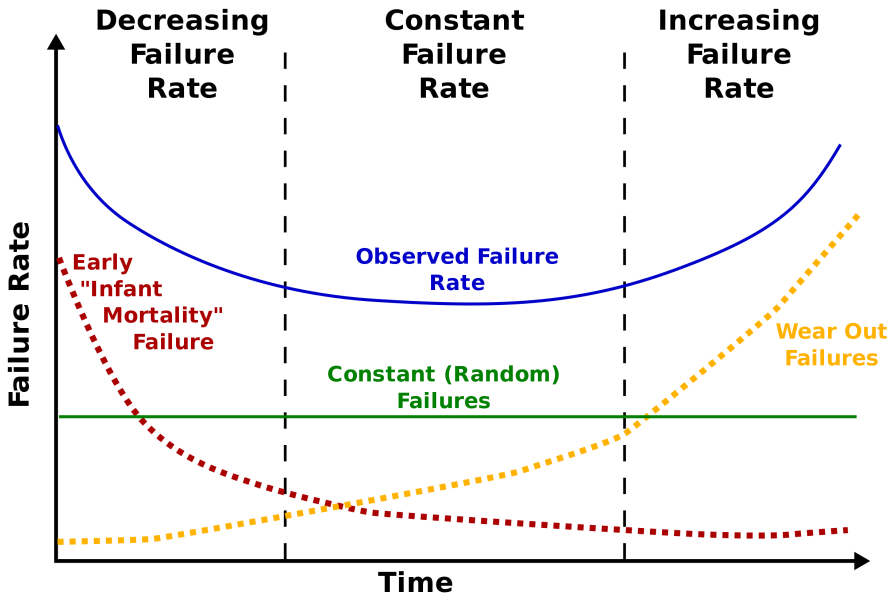

Figure 2.1: Bathtub Model representation

2.3 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;

2.3.1 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

2.3.2 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

2.3.3 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

2.4 Process Base Standard

- Standards
- Steps
- Specifications

2.5 Standard IEC 61508

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
- 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

Standard 26262
The standard ISO 26262 is an adaptation of the Functional Safety standard IEC 61508 for Automotive Electric/Electronic Systems. ISO 26262 defines functional safety for automotive equipment applicable throughout the lifecycle of all automotive electronic and electrical safety-related systems.

ISO 26262 defines a **h**azard as "a potential source of harm caused by malfunctioning behaviour of the item where harm is physical injury or damage to the health of persons"
This standard make use of analyses such as **F**ault Mode Effect Analysis (FMEA) to identify how faults lead to failures that may cause harm.
In an article titled "An Analysis of ISO 26262: Using Machine Learning Safely in Automotive Software" mention two tools of fault detection and techniques for Machine Learning. Chakarov et al and Nushi et al

EUC - Equipment Under Control

SIL - Software Integrity Level

There are four different levels of SIL being SIL level 4 the most dangerous and level 1 the less.

2.5.1 Fault Trees Analysis (FTA)

It is a **t**op-down, deductive failure analysis in which an undesired state of a system is analyzed using Boolean logic to combine a series of lower-level events. This analysis method is mainly used in safety engineering and reliability engineering to understand how systems can fail, to identify the best ways to reduce risk and to determine failure. FTA is used in the aerospace, nuclear power, chemical and process, pharmaceutical, petrochemical, and other high-hazard industries; but is also used in fields as diverse as risk factor identification relating to social service system failure. FTA is also used in software engineering for debugging purposes and is closely related to the cause-elimination technique used to detect bugs.

Fault tree analysis can be used to:

- Understand the logic leading to the top event / undesired state.
- Show compliance with the (input) system safety / reliability requirements.
- Prioritize the contributors leading to the top event- creating the critical equipment/parts/events lists for different importance measures
- Monitor and control the safety performance of the complex system (e.g., is a particular aircraft safe to fly when fuel valve x malfunctions? For how long is it allowed to fly with the valve malfunction?).
- Minimize and optimize resources.
- Assist in designing a system. **T**he FTA can be used as a design tool that helps to create (output / lower level) requirements.
- Function as a diagnostic tool to identify and correct causes of the top event. It can help with the creation of diagnostic manuals / processes.

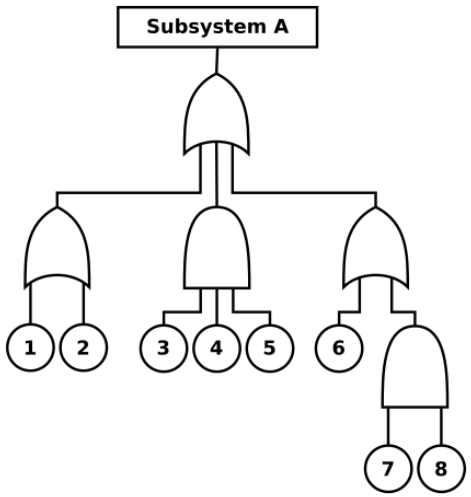

Figure 2.2: *Fault Tree Diagram*

2.5.2 Faulire Modes and Effects Analysis (FMEA/FMECA)

Is the process of reviewwing as many componentes, assemblies, and subsystems as possible to identify potential failure modes in a system and their causes and effect. For each component, the failure modes an their resulting effects on the rest of the system are recorded in a specific FMEA worksheet. There are numerous variations of such worksheets. An FMEA can be a qualitative analysis, but may be put on a quantitative bases when mathematical failure rate models are combined with a statistical failure mode ratio database. An FMEA is often the first step of a system reliability study.

A few different types of FMEA analyses exist, such as: Funcitonal, Design and Process

How to apply the Failure Modes Effect Analysis:

1. Construct functional block diagram.
    - Establish scope of the analysis
    - Break system into subcomponents
    - Different levels of detail?

    - Some unkowns early in design?
2. Use diagram to identify any associated failure modes.
    - many different failure modes: complete failure, partial failure, intermittant failure, gradual failure, etc.
    - Not all wil apply?
    - compare with HAZOPS guidewords
3. Identify effects of failure and assess criticality.
4. Repeat 2 and 3 for ptential consequences.
5. Identify causes and ocurrence rates.
6. Determine detection factors.
7. Calculate Risk Priority Numbers.
8. Finalise hazard assessment.

2.5.3 Hazard and operability study (HAZOPS)

Structured and systematic examination of a complex planned or existing process or operation to identify and evaluate problems that may represent risks to personnel or equipment. Often used as a technique for identifying potential hazards in a system and identifying operability problems likely to lead to nonconforming products.