Safety Critical Systems

Notes

Efraín Manuel Villanueva Castilla

Febreuary 18, 2020

Contents

1 Introduction

This is my first attempt to make clean notes about what happened in class. In this document you will find notes about Safety Critical System Class 2020

2 Class Introduction

Safety Governance, Market Focused

- People buy things even if the probabilitties 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

Tort and Insurance

- 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

Different Format Regulation

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

Mend Rea → Guilty Mind

2 types of processes

1. Product base Standard
2. Process base Standar

Process Base Standard

- Standards
- Steps
- Specifications

Standard IEC 61508 ← θ and (26262)

- Functional Systems Standard
- ≠ Publishing Audible
- Electronic
- Electrical Electronic Programmable Systems
- Market forces are not enough → Standard
- Standards. 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