Chapter 1: Risk in Modern Society

Howard University Department of Electrical and Computer Engineering

Computer System Safety

Cimoya Collins

1.1 Changing Attitudes toward Risk

- Risk is a combination of the likelihood of an accident and the severity of the potential consequences.
- All human activity involves risk there is no such thing as a risk free life.
- The increase in national and regional concern on safety has made employers responsible for safety importance more than the employees responsibility
- Personal responsibility of one knowing his or her own risk and safety factor is not always wise and can cause tragic result

1.2 Increase Concerned Justified?

- Determining whether technological risk is increasing or not depends the data used.
- Human mortality due to technological hazards were greater in the early stages of industrial development
- Shown in the National Safety Council showing occupational death and injury rates have declined since the early part of the century and not currently rising

1.2 Increase Concern Justified?

- Sixty percent of all the major industrial disasters occurred from 1921 to 1989.

- Past experiences does not allow us to answer the question by using statistical data. When the risk factors in the past differ from the risk factors in the future.

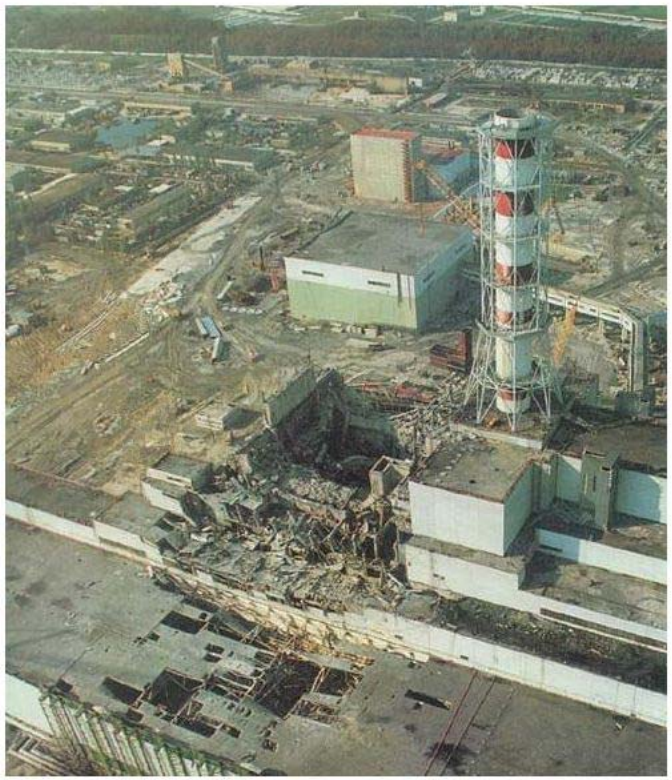
1.3 Unique Risk Factors in Industrialized Society

- Some factors that are particularly relevant today are the appearance of new hazards and the increasing complexity, exposure, energy, etc. in the systems we are trying to build

1.3.1 The Appearance of New Hazards

- Accidents in the early century were the result of natural causes or involved a few relatively well understood technological devices
- Now in the 20th Century scientific and technological advances have reduced or eliminated many risks that were once a commonplace in the early years.
- Science and new technology has also created new hazards. For example children are no longer work in coal mines or as chimney sweepers, but they are now exposed to man-made chemicals and pesticides in their foods

Deep Water Horizon



- The Deep Water Horizon oil platform explosion. This event killed 11 workers and caused an environmentally catastrophic event. The oil that leaked from the platform measured up to hundreds of thousands of barrels of oil, which was discharged into the Gulf of Mexico.

1.3.1 The Appearance of New Hazards

- Some of the new hazards are harder to find and eliminate than the ones in the past.
- What has been learned and practice in past experience to help with new hazards has been passed down through codes and standards of practice.
- The downfall to that is that some lessons learned over centuries are lost when older technologies are replaced with new ones.

1.3.2 Increasing Complexity

- Complexity both in product and process in the systems we are building not only discovers new hazards but also the complexity makes it harder to identify them
- Increased complexity makes it difficult for the designers to consider all the hazards or even the most important ones for the operators to handle all normal and abnormal situations.
- Complexity and scope of projects require numerous people and teams to work together. This gives each individual a specific responsibility

1.3.3 Increasing Exposure

- Not only is our technology becoming more complex but our society has become more complex as well
- Consequences of an accident not only depends on the hazard but also on the exposure of the hazard, i.e: the length of time and the environment which the hazard exist
- Siting of dangerous facilities near large populations is increasing as more people move to cities and larger plants need larger workforce within commuting distance.

1.3.4 Increasing Energy

- Another factor to increased risk is the discovery and use of high energy sources such as exotic fuels, and high pressure systems.
- New systems use more conventional energy sources, but they use technology that requires larger amounts of energy than was required in the past.
- The larger amounts of energy increases both the surrounding area potentially affected by an accident and the amount of damage possible.

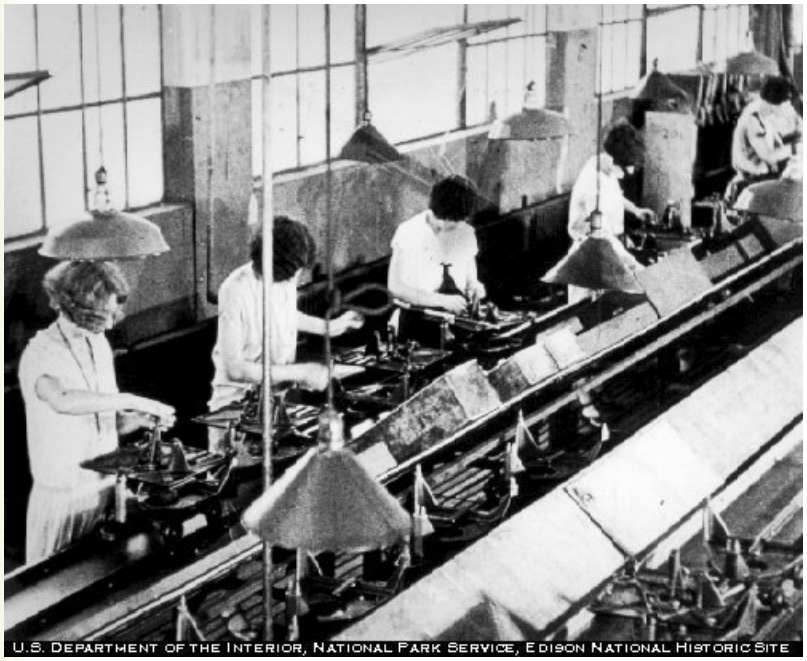
1.3.5 Increasing Automation of Manual Operations

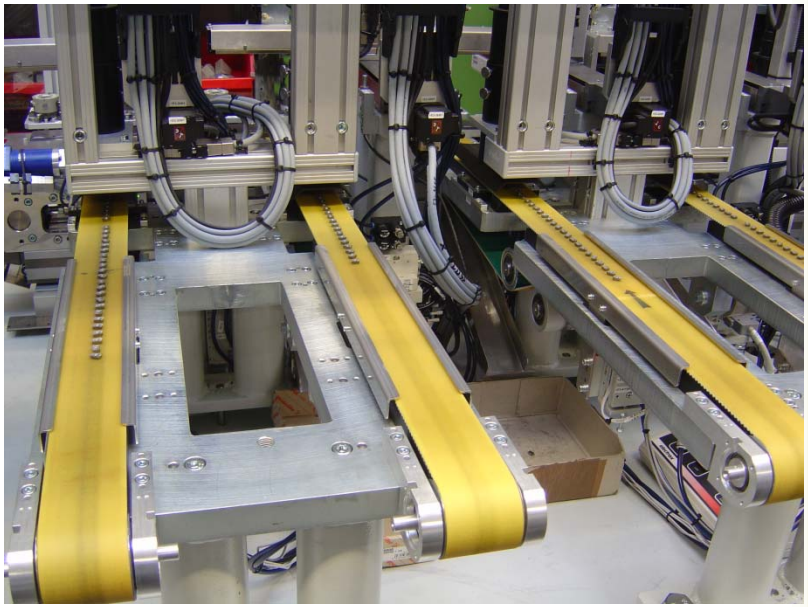
- It seems that automation would decrease the risk of operator, but automation does not remove people from systems it just moves them to maintenance and repair functions and to higher-level supervisory control and decision making process more difficult

- Operators in automated systems are often relegated to central control rooms where they must rely on indirect information about the system state which can be misleading

- When accidents happen the blame is primarily put on the human when in reality it was an error in the automated system

Then and Now


U.S. Department of the Interior, National Park Service, Edison National Historic Site



1.4 How Safe is Safe Enough?

- The goal is to understand and manage risk in order to eliminate accidents or to reduce their consequences
- Unfortunately hazards will never be eliminated completely from all systems. In addition to the technical difficulty of anticipating and reducing risk
- Designing a system to protect against a variety of hazards is possible but designing a system to protect again all hazards is possible but causes so many compromises on functionality that makes the system useless

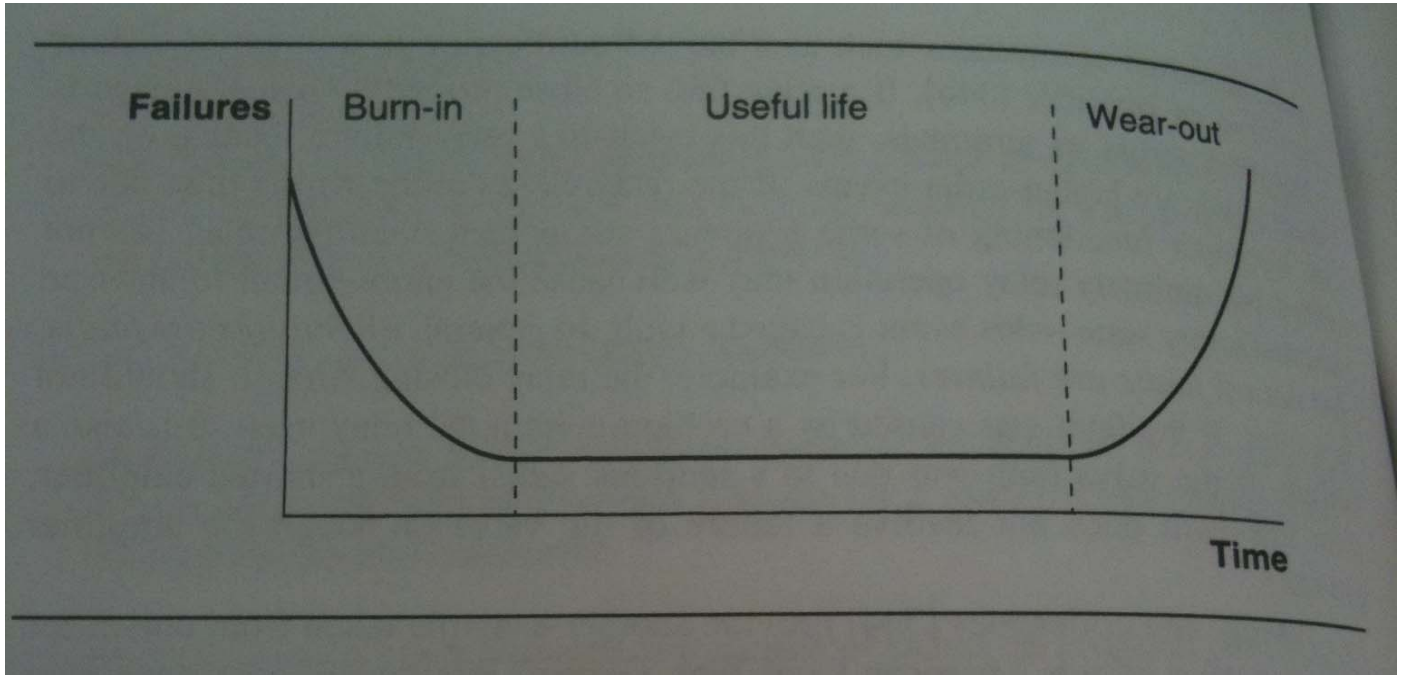
1.4.1 Risk-Benefit Analysis and the Alternatives

- To approach a risk benefit analysis you must first measure risk and then choose an appropriate level for decision making. A system must be built with the knowledge of their risk.
- Risk assessment tries to solve this dilemma and quantify risk which can stop the severity of loss.
- Even if risk could be measured, there is still the problem of choosing the level of risk to use in decision making.
- The most common criterion is that of the acceptable risk. Which is a threshold level is selected below which risk is tolerated

Chapter 9 Terminology

- 9.1 Failure and Error
  - Reliability: the probability that a piece of equipment or component will perform its intended function correctly for a prescribed time
  - Failure: the nonperformance of inability of the system or component to perform its intended function for a specified time

Failure Bath Tub Model



9.1 Failure and Error

- A failure may be caused by design flaws which is called systemic failure. Another failure may result from an operation that doesn't follow the original design due to environmental disturbances
- A failure occurs at a particular instant in time
- Error: is a design flaw or deviation from a desired or intended state.
- An error remains until removed by some sort of human intervention. Diagrams, programs, and models can have errors but can be fixed

9.1 Failure and Error

- In todays world engineers distinguish between a fault and a failure. In engineering failures are abnormal occurrences such as burned out bearings in a pump or a short circuit in an amplifier
- In a primary fault (and failure) a component fails within the design or environment
- Secondary faults (and failures) occurs when components fail because of excessive environmental stresses that exceeds the requirement of the design
- Command faults involve the operation of the component because of a failure to control the element or the component operates correctly just at the wrong time and place

9.2 Accident and Incident

- An accident is an undesired and unplanned event that results in at least a specified level of loss
- A near miss or incident is an event that involves no loss or only minor loss but with the potential for loss under different circumstances

Accident and Incident

9.3 Hazard

- 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 will lead to an accident or loss event

- A hazard is defined with respect to the environment of the system or components

9.4 Risk

- Risk is the hazard level combined with the likelihood of the hazard leading to an accident sometimes called danger and hazard exposure or duration

- Exposure or duration of a hazard is a component of risk

9.5 Safety

- Safety is freedom from accidents or losses
- By accepting a relative definition of safety it is possible to ignore design alternatives that eliminate or greatly reduce particular hazards but require compromises with respect to other goals

9.6 Safety and Security

- Security and safety both deal with threats or risk one with threats to life or property and the other with threats to privacy or national security

Questions or Comments