SOROTI UNIVERSITY

INNOVATE AND CREATE

SCHOOL OF ENGINEERING AND TECHNOLOGY

CPE4202: PROFESSIONAL ETHICS IN ELECTRONICS AND COMPUTER ENGINEERING

Risks and Liabilities of Safety-Critical Systems (Ethical and Legal Considerations in Computer Engineering)

YEAR 4 SEMESTER 2

By Mr. Matsiko Joshua

Introduction to Safety-Critical Systems

- Safety-critical systems are systems whose failure can lead to catastrophic consequences, including loss of life, significant financial loss, severe environmental damage, or harm to public safety.
- These systems are designed with reliability, robustness, and fail-safes to minimize risks.

Importance in Computer Engineering

- Many modern safety-critical systems are software-driven. Ensuring reliability in these systems is a key ethical responsibility for engineers.
- Failures can result in significant legal, ethical, and financial consequences.
- There is no one criterion that can be used to measure software standards but rather a collection of criteria such as development testing, verification and validation of software, and the programmer's professional and ethical standards.

Introduction to Safety-Critical Systems

Examples of Safety-Critical Systems

- Medical Devices such as Pacemakers, robotic surgical systems, hospital management software.
- Transportation. Autonomous vehicles, air traffic control, railway signaling systems.
- Industrial Control. Power grids, chemical plant automation, nuclear reactor monitoring.
- Defense and Security. Missile defense systems, cybersecurity infrastructure, surveillance systems.

Risk in Safety-Critical Systems

Risk refers to the probability of failure in a system and the potential consequences of that failure. In safety-critical systems, risks involve threats to human life, system integrity, financial assets, and societal stability.

Categories of Risk

1. Operational Risks. Risks due to software/hardware malfunctions or human errors.

2. Cybersecurity Risks. Unauthorized access, data breaches, or system hacking leading to failures.

3. Legal and Ethical Risks. Liability concerns, negligence, and failure to comply with regulatory standards.

4. Environmental Risks. System failures leading to ecological disasters, such as oil spills or radiation leaks.

Risks Associated with Safety-Critical Systems

- **Software Bugs & Failures.** Poor coding, lack of proper testing, and unforeseen conditions can lead to catastrophic failures.
- **Cybersecurity Threats.** Unauthorized hacking or malware attacks may compromise system integrity.
- **Human Error.** Incorrect configuration, misunderstanding of system operations, and maintenance issues.
- **Hardware Malfunctions.** Defective components causing operational breakdowns.
- **AI and Automation Risks.** Unintended consequences due to autonomous decision-making in AI-controlled systems.

Consumer Rights

Consumer rights ensure that individuals are protected from unsafe, defective, or misleading products and services. These rights are particularly crucial in safety-critical systems, where failures can have severe consequences, including financial loss, health risks, or even loss of life. Understanding these rights helps consumers make informed choices and seek redress when necessary.

These include;

- **Right to Safety:** Protection against hazardous products and services.
- **Right to Information:** Full disclosure of product risks, capabilities, and limitations.
- **Right to Choose:** Access to a variety of safe and reliable products.
- **Right to Redress:** The ability to seek compensation for defective or harmful products.
- **Right to Consumer Education:** Awareness and knowledge about consumer rights and responsibilities.
- **Right to a Healthy Environment:** Protection from environmental hazards caused by unsafe industrial or technological practices.

Legal Protections in Safe Critical Systems

- **Contracts**: Legally binding agreements between parties that outline the responsibilities, performance standards, and legal obligations related to product compliance. These agreements also provide consumers with legal recourse in case of product defects or failures. A contract need not be in a physical form like a document; it can be oral or implied.
- **Warranties**: Guarantees regarding product functionality and safety, ensuring that products meet specified standards and perform as advertised within a given period.
- The Ugandan National Bureau of Standards (UNBS) plays a role in regulating warranty policies to protect consumers from defective or substandard products. Warranties may be expressed (explicitly stated in contracts) or implied (automatically assumed under Ugandan consumer protection laws).
- **Third-Party Beneficiary Contracts**: Contracts that extend benefits to individuals or entities who are not direct parties to the agreement but have enforceable rights under it. Additionally, in mobile money services, agreements between telecom providers and financial institutions may grant users protection and access to services even though they are not signatories to the initial contract.

Legal Protections in Safe Critical Systems

Disclaimers

- Legal statements that limit manufacturer liability by informing users of potential risks and setting boundaries on the extent of legal responsibility.
- Disclaimers are often included in product manuals, software agreements, and medical device warnings.
- For example, telecom companies may include disclaimers stating that they are not responsible for service interruptions due to network issues beyond their control. However, disclaimers cannot override statutory consumer protection laws, which ensure that companies remain accountable for gross negligence or failure to meet mandatory safety standards.

Legal Concepts in Safety-Critical Systems

Negligence. Failure to exercise reasonable care, leading to harm. If there is provable evidence that the product lacked a certain degree of care, skill, and competence in the workmanship. E.g. Poorly maintained ferries in Uganda leading to capsizing and loss of life

Malpractice. Professional misconduct or failure to meet industry standards for example Faulty medical equipment in Ugandan hospitals leading to misdiagnosis or an Engineer falsifying tests on Mechanical condition of a vehicle.

Strict Liability. Companies are held accountable for product defects regardless of intent. Strict liability ensures that businesses take responsibility for defective products even if negligence or intent cannot be proven.

For example, in Uganda, telecom companies have faced fines and legal action for distributing faulty SIM cards that have led to identity theft and financial fraud.

The rationale behind strict liability is that manufacturers, suppliers, and service providers are in the best position to prevent defects before products reach consumers.

Legal Concepts in Safety-Critical Systems

Misrepresentation

Providing false or misleading information about system safety or capabilities. Misrepresentation occurs when a company, seller, or service provider provides inaccurate or deceptive information that influences a consumer's decision.

For example car dealerships in Uganda selling vehicles with tampered mileage readings, misleading customers about the actual wear and tear of the vehicle.

Similarly, some electronic retailers misrepresent the battery life of devices such as smartphones or solar panels, leading to consumer dissatisfaction and potential hazards.

In the telecommunications sector, internet providers may advertise broadband speeds that do not reflect actual service performance, misleading consumers into purchasing plans that fail to meet their needs.

Case Study - Therac-25 Medical Radiation Disaster

Therac-25 was a computer-controlled radiation therapy machine developed by Atomic Energy of Canada Limited (AECL) in the 1980s. It was designed to deliver high-energy radiation to cancer patients.

However, a series of software errors led to severe overdoses of radiation, causing at least six confirmed cases of serious injuries and deaths. The problem arose from a race condition in the machine's software, where rapid user input could bypass safety checks, leading to unintended radiation doses.

Additionally, the lack of proper interlocks and fail-safes exacerbated the issue, as the system failed to detect and prevent excessive radiation exposure. Investigations revealed that AECL had ignored prior reports of issues with earlier versions of the machine and did not conduct thorough software validation.

The disaster underscored the critical need for rigorous software testing, redundancy in safety-critical systems, and transparency in reporting failures.

Case Study - Therac-25 Medical Radiation Disaster

Key Issues

- **Software Errors.** Failure to detect and correct race conditions in software.
- **Lack of Redundancy.** No backup safety mechanisms to prevent radiation overdoses.
- **Poor Testing & Quality Assurance.** Inadequate software verification before deployment.

Moral Responsibility in the Therac-25 Case

Should the developers and managers at AECL be held morally responsible for the deaths resulting from the use of the Therac-25 they produced?

Two conditions must be met for moral responsibility in a harmful event

- **Causal Condition:** The agent's actions (or inactions) must have caused the harm.
- **Mental Condition:** The actions (or inactions) must have been intended or willed by the agent.

In this case;

- The **causal condition** is clear. AECL employees' actions (creating the faulty therapy machine) and inactions (failing to withdraw the machine from service or inform users about overdoses) led to the deaths.
- The **mental condition** applies through negligence and recklessness. While AECL engineers did not intentionally design a lethal system, they neglected safety measures, failed to implement interlocks, ignored prior warnings, and did not properly test the software.
- In conclusion; The Therac-25 team at AECL is morally responsible for the deaths caused by their failure to implement proper safety measures and thorough testing.

Case Study - Boeing 737 MAX Crashes

Two Boeing 737 MAX aircraft crashed in 2018 and 2019 due to software-related failures in the MCAS (Maneuvering Characteristics Augmentation System), leading to the deaths of 346 people. The first crash, Lion Air Flight 610, occurred on October 29, 2018, shortly after takeoff from Jakarta, Indonesia. The second crash, Ethiopian Airlines Flight 302, happened on March 10, 2019, minutes after departing from Addis Ababa, Ethiopia.

The MCAS was designed to automatically adjust the aircraft's pitch to prevent stalls, but it relied on a single angle-of-attack (AOA) sensor. In both crashes, faulty sensor data triggered MCAS to repeatedly push the aircraft’s nose down, making it difficult for pilots to regain control.

Boeing had failed to disclose MCAS’s full functionality to airlines and pilots, and the system was not mentioned in initial training programs. Additionally, regulatory bodies such as the FAA were criticized for lax oversight and reliance on Boeing's internal safety assessments.

Case Study - Boeing 737 MAX Crashes

Financial Impact of Boeing 737 MAX Crashes

- Over $20 billion in direct costs, including legal settlements, compensation to victims' families, and fines.
- Suspension of 737 MAX production for months, leading to significant revenue losses.
- A decline in Boeing's stock value, erasing billions in market capitalization.
- Loss of customer trust, with airlines canceling or delaying aircraft orders.

Moral Responsibility in the Boeing 737 MAX Case

- Boeing engineers and management ignored critical safety concerns to expedite aircraft certification.
- The company failed to ensure proper pilot training and transparency about MCAS.
- Negligence in risk assessment led to preventable loss of lives.

Conclusion: Boeing holds moral responsibility for the crashes due to their failure to prioritize safety and fully disclose MCAS functionality.

Key Standards for Safety-Critical Systems in Uganda

- **UNBS Standards for Electronic Devices**. UNBS establishes safety regulations and quality benchmarks for electronic devices to protect consumers from faulty and hazardous products.
- These standards cover areas such as electrical safety, electromagnetic compatibility, and energy efficiency. Manufacturers and importers must obtain certification before distributing electronic goods to ensure consumer protection and adherence to industry best practices.
- **Uganda Civil Aviation Authority (UCAA) Regulations**. Enforcing air safety standards, including aircraft certification, operational safety, air traffic management, and adherence to international aviation protocols.
- **NITA-U Guidelines**. The National Information Technology Authority-Uganda provides regulatory frameworks to enhance cybersecurity and software reliability in IT systems.
- **Ministry of Health Regulations**. Governing medical device safety, including licensing, quality control, and compliance with international best practices to ensure patient safety and system reliability in Uganda. These regulations also mandate periodic inspections, certification of medical equipment, and adherence to operational guidelines.

Key Standards for Safety-Critical Systems in Uganda

- **ERA Standards**. The Electricity Regulatory Authority (ERA) in Uganda establishes safety and operational standards for power generation, transmission, and distribution. Compliance with ERA standards is mandatory for all energy providers, and non-compliance can lead to penalties or license revocation.
- **UCC Regulations**. The Uganda Communications Commission (UCC) is responsible for ensuring network stability in telecommunications by enforcing compliance with quality standards, regulating spectrum allocation, and monitoring service providers to maintain reliable and secure communication infrastructure.

Risk Mitigation Strategies in Safe Critical Systems

- **Rigorous Testing** through extensive software and hardware testing before deployment.
- **Redundancy.** Backup safety mechanisms to prevent failures.
- **Clear Documentation**. Detailed user manuals and error reporting mechanisms.
- **Regular Audits.** Compliance checks and periodic system reviews.
- **Training and Awareness.** Continuous training for engineers, operators, and end-users to ensure proper handling of safety-critical systems.
- **Regulatory Compliance.** Adherence to industry standards and national regulations to minimize risk exposure.
- **Ethical Design Principles.** Incorporating safety-first approaches in the development phase to anticipate potential risks.
- **Incident Reporting and Response Systems.** Establishing protocols for prompt reporting and mitigation of failures.
- **Transferring Risk Through Insurance.** Obtaining liability insurance to cover damages resulting from system failures, ensuring financial protection for companies and affected users.

Discussion Questions

1. Who should bear the responsibility for failures in safety-critical systems—engineers, management, or regulatory bodies?
2. How can companies balance cost efficiency with rigorous safety testing?
3. Should there be stricter penalties for negligence in safety-critical system development?

Thank You