Introduction to Software safety and Liability and practice

WALEED RAZA

Introduction to Software safety Liability and practice

- We will explore areas of legal liability and mechanisms for regulating potentially hazardous activities as well as the factors which should be taken into account for safety related applications
- Nowadays, computer-controlled systems are to be found in a wide range of diverse applications such as:-
  - Industry: Manufacturing systems, robots etc.
  - Medicine: Intensive care monitoring, radiotherapy etc.
  - Transport: Railway signaling systems, aircraft, space shuttle etc.
  - Military and defense applications

Regulatory Issues

- **Standards:**

Use of appropriate standards is both a familiar and traditional technique for regulating hazardous activities and attempting to ensure the safety of a product

- **Certification and licensing:**

Certification requires that either the product or the practitioner conforms to some specified standard whereas licensing means that the product cannot go on the market at all, or the practitioner operate, unless the product is licensed or the practitioner in possession of the requisite license

Regulatory Issues

- **Professional codes of practice:**

Professional and trade associations should devise codes of practice to govern their members

- **Regulation by law:**

The law may exert a regulatory effect either directly or by requiring compliance with other forms of regulation such as standards and licensing because of fears of litigation if safety standards are breached

Legal Liability

- **Introduction**

System designers and software engineers may have legal responsibilities under laws such as the Health and Safety

- **Product Liability and the Consumer Protection Act 1987**

Product liability is the area of law in which **manufacturers, distributors, suppliers, and retailers** are held responsible for any injuries products cause. Regardless of any contractual limitations of liability, if a product or any of its component parts are defective its manufacturer may be liable for damage under the Consumer Protection Act (CPA) or the common law of negligence

Legal Liability

- **Negligence**

The manufacturer or system designer has failed to take due care in the construction or design of the system, and this lack of care has resulted in failure leading to injury

Competence, training and experience

- Competence means "knowledge and the ability to apply that knowledge"
- There is an understood assumption that all those engaged in the design and development of safety system software are competent to perform the necessary tasks
- Factors such as training and relevant experience are also considered important traits for a competent software engineer

Factors affecting system safety

- Hazard analysis
- Requirements and specification
- System Reliability and safety
- Design
- Testing and debugging
- Safety integrity analysis and risk assessment
- Documentation