Professional Practices

“Software Safety: Liability and Practice”

Contents

- Introduction
- Regulatory Issues
- Legal liabilities
- Factors affecting system safety

Introduction

- Design and construction of large software systems is an incredibly difficult task.
- It becomes more cumbersome when the failure of such systems are very costly in terms of financial sufferings and human lives.

Introduction

- Computer controlled systems are widely used now a days such as
  - Industry
  - Medicine
  - Transport
  - Military and defense applications
- All these examples are safety related and capable of causing extensive damage….any thing from a single fatality to a major disaster.

Regulatory Issues

- Some form of external regulation is required to develop a success full software.
- Why?
- Objectives of regulation
  - Protection of those who may be harmed.
  - Protection of society as a whole from physical and environmental disaster.
  - Provides a degree of protection to the system designers.

Regulatory Issues

- There are various methods available for regulation, each having its own application to software and system safety.

Regulatory Issues

Standards

- “standard is a document established by consensus and approved by a recognized body, that provides, for common and repeated use, rules, guidelines or characteristics for activities and their results, aimed at the achievement of optimum degree of order in a given context” (IEC)
- The use of appropriate standards is both a familiar and traditional technique for regulating hazardous activities and attempting to ensure the safety of a product.

Regulatory Issues

- One major problem is the rapid rate of change of technology.
- Design standards that mandate a particular method of design are the frequent choice for safety standards, but they can have the effect of crystallizing the technology.
- Other design methods which may arise from improvement in technology may not comply with the standard.
- Problem can be solved by rapidly occurring subsequent revisions.

Regulatory Issues

- **IEC 61508** is an 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 recently adopted by software industry covering general requirements, software requirements, definitions and examples of methods for determination of safety integrity levels.

Regulatory Issues

Certification and Licensing

- Certification and licensing are also the examples of regulation which can be applied to both products and practitioners.
- They can also be used in conjunction with standards as when a product is certified against a particular standard.

Regulatory Issues

- The terms certification and licensing are often used interchangeably but, strictly, certification requires that either the product and the practitioner conforms to some specified standard but there is no bar to the marketing of uncertified products or practicing of uncertified practitioners.
- A licensing requirement, on the other hand, means that the product cannot go on the market at all or practitioner operate, unless the product is licensed or the practitioner in possession of the requisite license.

Regulatory Issues

- Licensing is therefore a more severe form of certification.
- Licensing is bound to have a restrictive effect on the market but this is usually considered to be justified in safety related situations.

Regulatory Issues

Professional codes of practice

- It is common for professional associations to devise codes of practice with which to govern their members.
- The subject matter of such codes may be general or more specific in nature but, in either case, they can perform a valuable regulatory function.

Regulatory Issues

- Although they are a form of self regulation which is not in itself legally binding, they are capable of producing legal effects if incorporated into the terms of a contract.
- Failure to comply with the requirements of a code of practice may itself be evidence of negligence.

Regulatory Issues

Regulation by law

- The law also exerts a regulatory effect either directly of indirectly.
- There are two ways of direct application
  - By requiring compliance with other forms of regulation such as standards and licensing.
  - By incorporating similar requirements into statute.

Regulatory Issues

- Indirect application is by exerting a deterrent effect because of fears of litigation if safety standards are breached.
- Law is frequently reactive rather than preventive, as it is more concerned with providing a remedy after the event.

Legal Liabilities

- Should software manufacturers be held strictly liable for software defects?
- Two school of thoughts.

Legal Liabilities

- Software manufacturers should be held strictly liable because:
  - Strict liability forces manufacturers to take precautions before marketing their product
  - Injured party will be adequately compensated
  - Manufacturer makes a representation of product safety

Legal Liabilities

- Software manufacturers should be held negligent because
  - Strict liability will cause an unnecessary burden upon computer software manufacturers
  - Strict products liability would hinder innovation

Factors affecting System Safety

- Most software engineers are trained to ensure that systems are designed and developed on sound scientific principles.
- Applying these principals to safety related systems means that safety should be made an objective at the first possible opportunity, i.e. at the design stage.

Factors affecting System Safety

- Nothing can be made inherently safe and so any assessment of the safety of an object or process will depend on balancing a number of factors.
- This section provides an overview of all the factors which need to be taken into account while developing a secure system.

Factors affecting System Safety

Hazards Analysis

- Before finalizing and proceeding further with the design of a safety related application, it is necessary to arrange a full hazard analysis.
- Reason is the identification of all potentially dangerous situations.
- Such an analysis needs to include not only the obvious hazards, but also the more elusive dependent hazards which may arise due to unusual combinations of circumstances.
- Examples of some formal techniques of hazard analysis are fault mode analysis (FMA) and fault tree analysis (FTA).

Factors affecting System Safety

Requirements and specification

- Detailing the requirements is the first step towards ensuring that the correct end product is produced.
- For this to be achieved, it is necessary for the analyst, designer and implementer to fully understand the nature of the product.

Factors affecting System Safety

- In many cases, the user, despite possessing detailed knowledge of the application, will not have sufficient understanding of the precise workings of the computer system to appreciate whether it is trustworthy or not.
- This is also true in reverse, the software engineer cannot be expected to be immediately aware of all the subtle shades pertaining to the particular application.

Factors affecting System Safety

- One pre-requisite therefore for the safe design is “full and frank discussions” between the customer and designer with a view to creating total understanding regarding **both** the nature of the product and the required safety performance.

Factors affecting System Safety

Reliability and Safety

- Reliability is defined as “the probability of performing the intended purpose adequately for the period of time intended under the operating conditions encountered”.
- Safety on the other hand can be defined as “the probability that no accidents will occur in a given length of time due to a system failure or malfunction”

Factors affecting System Safety

- Although the reliability of a system is an important parameter, one must be careful not to confuse system reliability with system safety.
- Reliability is concerned with making the system failure-free. i.e. performing its specified functions correctly.

Factors affecting System Safety

- It is perfectly possible for a system to be functioning correctly that is as specified and yet for a mishap to occur.
- Safety is therefore concerned with making system hazard-free.
- From a safety point of view, system failures can be tolerated, provided they fail to safety.

Factors affecting System Safety

Design

- There are a number of standards and other publications which provide general reference material for designers of programmable systems for safety related applications.
- The design approach chosen for the safety system will depend on the intended application but there are a few principles which can be considered.
- These are based on the premise that hazards can either be prevented or they can be detected and treated.

Factors affecting System Safety

- This leads to three possible design strategies
  - Prevention or minimization of hazards
  - Use of automatic safety devices to control the hazard if it occurs.
  - Provision of warning devices, safe systems of work and suitable training to instruct personnel how to react in the event of a mishap.

Factors affecting System Safety

Testing and debugging

- All large software systems will contain bugs.
- These may have been generated by coding and design errors or by faulty interpretation, ambiguity or incompleteness of the functional specification.
- Software testing is the controlled exercise of programs using sample input data.

Factors affecting System Safety

- One of the aims of testing is to locate bugs and to remove them by debugging techniques followed by retesting to ensure that no further bugs have been introduced in the process.
- Testing and debugging will thus be undertaken many times in the software lifecycle.
- Different aspects of the developing system will need to be tested for the safety requirements.
- Testing and debugging also contribute to increase the reliability of the system.

Factors affecting System Safety

Documentation

- Well developed software should be described by comprehensive and intelligible documentation throughout the development process.
- It should include references to design methods, software tools employed and details of test plans together with results.

Factors affecting System Safety

- There may be a number of individuals who could be classified as users, e.g. operators, maintenance personnel, managers etc. and the user documentation needs to be relevant and understandable to them all.
- Documentation of the safety requirements should include a description of the safety systems.

Factors affecting System Safety

- It will need to explain
  - When and how the system should be maintained.
  - The safety precautions necessary before maintenance.
  - The testing procedures after maintenance.
  - Explanation of any extra training necessary for operators and maintenance staff.
  - It should include a complete and easy to use index.