Chapter 13
Legal Aspects of Safety Critical Systems

13.1 Introduction

Society is increasingly dependent upon computers and, in particular, computer control systems. Unfortunately, the growth of computer controlled systems in the last three decades has not been matched by any systematic reappraisal by legislative bodies of the legal liability attaching to suppliers of those computer controlled systems.

Instead, legislation passed to improve the safety of employees and consumers has been drafted to encompass computer controlled systems. The result is a haphazard application of the law, rather than any clearly thought through liability for the suppliers of computer controlled systems.

To this must be coupled a fundamental difficulty of the supplier of a computer controlled system: namely the relative ease of supplying a system which inadvertently contains an error even where the system has been tested, validated, verified and assessed.

In many circumstances there is little or no direct consumer pressure to supply error free software. Indeed, in certain industries it is in the manufacturer’s interest to supply an unreliable computer system — so that the manufacturer can fix the system under a maintenance contract. For instance, customers who obtain computerized account systems and other so-called “back office” systems accept that they will pay substantial sums for maintenance of “faulty” software.

In other areas of the computer software industry it is also common to see poor quality software. Examples include games software, operating systems utilities (rather than the operating systems themselves), as well as some types of software supplied on microprocessor controls.

Unfortunately, this industry malaise cannot be carried through to safety-critical areas where the consequences of a poorly programmed software can, all too easily, prove fatal. This is true not only for large scale control systems but also for microprocessor control systems which find themselves in safety-critical applications such as those found embedded in back-up pumps and valves. The economic cost to a pump manufacturer of discovering a safety critical fault in a control unit can be high, particularly if a product recall is required. The manufacturer will wish to pass on that cost to the supplier of the microprocessor control unit.

The number and type of “safety critical” applications is constantly increasing. For instance, the emergency shutdown procedure on an offshore oil installation may depend upon a software based control system. A relatively simple error in that system could result in an incorrect shutdown and a catastrophic accident. If such a mistake was due to an error in the control system, the supplier of the system could be liable.

This chapter examines the range of specific liabilities placed upon manufacturers and suppliers of computer systems with particular reference to safety-critical systems.
Specifically it deals with: the "classical" remedies available; product liability legisla-
tion; and the newer burdens imposed by European Union legislation.

13.2 Classical Remedies

Historically, the two most important aspects of English (and Scottish!) law under
which an injured party can bring a claim are the laws of contract and negligence. Also
considered below is potential liability under the Health & Safety at Work etc Act, 1974.

13.2.1 Contract

In order to bring a claim, there must first be a contract between the parties in dispute. This is by no means a trivial test since typically, there will not be a contract between the injured party and the manufacturer who has introduced the defect into the product. An example of where a contract claim could be brought would be where a computer control manufacturer supplies a component to a motor car manufacturer who is building an anti-lock brake device. If, as a result of a fault in one of the computer units, an accident occurs the car manufacturer could bring a claim for breach of contract. That claim could be very great, since it could include damages for the loss of business suffered by the car manufacturer where it had needed to undertake a product recall exercise. In practice the computer component manufacturer would seek to limit its liability by excluding claims of the same type as consequential loss.

A claim for a breach of contract could be based on an express term of a contract, for example, that goods will comply with a certain British Standard. Additionally, a claim could be based on a term implied into the contract. Among the most important terms implied into most contracts for the supply of goods are that goods will comply with their specification and description; be of satisfactory quality; and be fit for any specific purpose for which they have been supplied.

13.2.2 Law of Negligence

Under the law of negligence, a manufacturer of goods owes a so-called "duty of care" to ensure that the goods it supplies are not likely to cause personal injury. Essentially, the duty is to take "reasonable care".

Historically, claims for defective computer systems have had to be brought under this law — particularly where there has been no contractual relationship between the claimant and the manufacturer. The manufacturer's liability under the law of negligence is more far reaching than under the law of contract. This is at least true in so far as who may bring a claim. A person can bring a claim under the law of negligence if he or she can say that the manufacturer ought reasonably to believe he or she would be adversely affected. This is far wider than under the law of contract where the person bringing the claim must have a direct contractual relationship with the defendant.