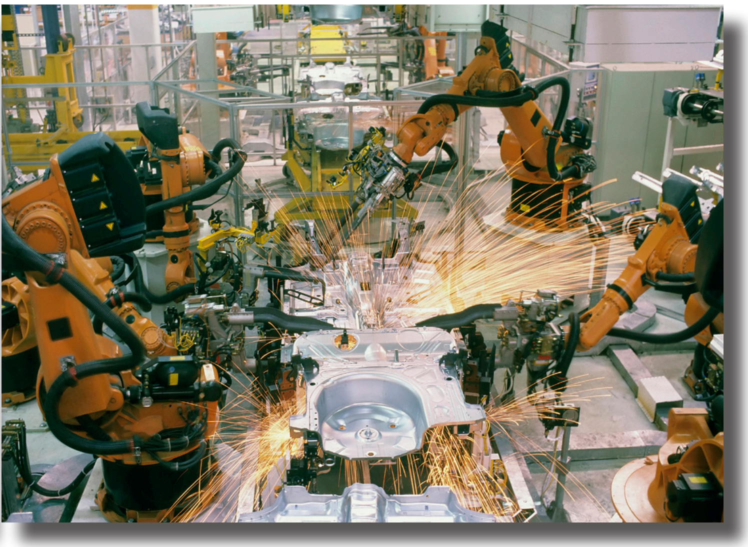
The Institution of
Engineering and Technology

CPD™
http://www.theiet.org/cpd

Computer Based
Safety-Critical Systems

A Factfile provided by the Institution of **Engineering and Technology**



www.theiet.org/factfiles

About This Factfile

The Institution of Engineering and Technology acts as a voice for the engineering and technology professions by providing independent, reliable and factual information to the public and policy makers. This Factfile aims to provide an accessible guide to current technologies and scientific facts of interest to the public.

For more Factfiles and Position Statements on engineering and technology topics please visit http://www.theiet.org/factfiles.

This document has been written by the ISA Working Group in association with the IT Policy Panel.

The Institution of Engineering and Technology

The Institution of Engineering and Technology (IET) is a global organisation, with over 150,000 members representing a vast range of engineering and technology fields. Our primary aims are to provide a global knowledge network promoting the exchange of ideas and enhance the positive role of science, engineering and technology between business, academia, governments and professional bodies; and to address challenges that face society in the future.

As engineering and technology become increasingly interdisciplinary, global and inclusive, the Institution of Engineering and Technology reflects that progression and welcomes involvement from, and communication between, all sectors of science, engineering and technology.

The Institution of Engineering and Technology is a not for profit organisation, registered as a charity in the UK.

For more information please visit http://www.theiet.org

Enquiries

policy@theiet.org

Contents

Introduction

Computer based systems are widely used in transport, medicine, process control, energy generation and elsewhere. Systems are commonly called computer based safety-critical systems when computers[1] have a strong, perhaps dominating, influence on safety.

The use of computers can provide safety benefits as well as performance and financial benefits. Examples of safety benefits include (**i**) operators able to manage plant safety more effectively due to operator-friendly presentation of information in plant control rooms; and (**ii**) timely and effective automatic management of rapidly developing unsafe situations due to the ability to monitor, process and respond to large amounts sensor data quickly and accurately. However, faults in computers (including their software) can result in accidents. This position statement specifically addresses systems where safety depends critically on computers. However, it is also relevant to situations where, for example, financial loss, economic disruption, environmental damage or compromise of personal privacy or national security depends strongly on computers.

Computer based systems

A computer based system is any system in which functionality depends partly or wholly on computers. Physical or other harm cannot result directly from a computer (except for harm that may be caused by use of electricity and by the physical attributes of the computer). However, a computer that is part of a wider, computer based system may cause the wider system to behave in an unsafe way. Indeed, for a computer based safety-critical system, the safety of the system depends strongly on its computers.

Safety can depend on computers in two ways:

- The computer helps to control a wider system. If it does not do that correctly then the wider system may behave in an unsafe way and cause harm. Examples include (**i**) a control system uses computers to directly control a process plant; (**ii**) an air traffic control system uses computers to process and present information to air traffic controllers; (**iii**) the control system for a driver-less train uses computers to control speed, braking, doors and other functions important to safety.
- The computer helps to protect against harm if the wider system behaves in an unsafe way. Examples include (**i**) a fire control system for a building; (**ii**) a computerised automatic shutdown system for a nuclear power plant; (**iii**) an automatic braking system for a car.

Sometimes, safety may depend on computers in both of the above ways. For example, computers may be used not just to control a plant but also to protect against harm if the computerised control system were to fail to keep plant parameters within safe bounds.

Computer systems have characteristics that distinguish them from typical physical systems. The most important characteristics for safety are in respect of software (computer code, which may have been burnt into a chip) and associated data. The following are particularly significant for safety:

- Software is invisible, it is not possible to see errors or changes except by examination and analysis of coding and data.
- Software does not wear out as physical systems do. Software failures result from errors that are always present in the software or from incorrect data.
- Relationships between inputs and outputs can be complicated, discontinuous and not predictable except by detailed analysis of coding.
- A computer, particularly its software, is usually sufficiently complex that it is not practical to test all possible inputs and outputs exhaustively.

Basic Principles for Safety

Safe use of computer based systems in safety-related applications requires that the special characteristics of computers (and software in particular) are addressed. Application of the following basic engineering principles provides a sound basis for safety.

- A computer must be regarded and treated as an integrated part of the wider system to which it contributes. This includes consideration of functionality, reliability, integrity and potential faults and failures.
- What is required of a computer (typically what it must do, how well it must do it and under what conditions) must be no greater than what it can be shown to achieve. The extent to which requirements are satisfied is typically limited by human error in design and production and by interdependencies both within the system and with respect to external factors.
- Design of the wider, computer based system as well as of the embedded computer(s) (including software) must take into account the ways in which the computer(s) (including software) may fail. The design must include measures to avoid multiple failures arising from a single cause, including propagation of failures.
- The design, production and assurance of computers and software must adopt and incorporate principles and practices appropriate for what is required of the computers and software. This includes the degree of rigour of the design, production and assurance processes, attributes of the design and the extent and rigour of checking and testing.
- Appropriate means must be used to confirm that computers and software meet their requirements. Such means include analysis, testing and assessment. Rigour and independence should be in proportion to the safety significance of the computer and software. For the highest degree of rigour, formal methods may be used. (http://www.theiet.org/factfiles/it/formal-methods-page.cfm) Confirming to an adequate level of confidence that computers and software achieve what is required of them becomes more difficult (and more expensive) as the safety significance of a system increases. A high level of confidence is typically both difficult and expensive to achieve.

- When pre-existing software is to be used, both its functionality and confidence in its ability to perform satisfactorily in the situation in which it is to be used must be established. Satisfactory performance in one situation does not necessarily imply satisfactory performance in another.
- A user interface, where provided, must be appropriate for both the intended use of the system and the persons who will use it. For example, what is suitable for a trained operator may not be suitable for members of the public.
- Maintenance and upgrade must be strictly controlled so as to maintain the safety attributes of the system (for example, its safety functions and the degree of confidence that they will be carried out correctly). Safety of the wider system needs to be considered before any change is made to a computer (including software) as there may be unintentional safety impacts. For example changed software may fail in a new or unexpected way.
- Computer systems must be protected from unauthorised change or interference of any kind. This includes both human interference (malicious, inadvertent or otherwise) and physical or electronic interference (for example, electromagnetic or via a network).
- Good practice must be used at all times, from concept through to use and maintenance. Sources of good practice include national and international safety-related engineering standards.
- Everyone involved with the computer system must be competent for their role. Technological change means that competency of system developers needs to be kept current.

Many of these principles are also relevant to other systems where, for example, computer failure may result in financial loss, economic disruption, environmental damage or compromise of personal privacy or national security.

IET Position

The IET supports the appropriate use of computer based safety-critical systems when underpinned by the use of 'good practice' engineering principles and practices.

The IET recommends

1. The use of appropriate 'good practice' engineering principles, practices and processes for the development and assessment of all computer based safety critical systems.
2. Further development of 'good practice' engineering principles, practices and processes and of cost-effective tools and approaches for implementing and applying them.
3. Increased education and training in the use of 'good practice' engineering principles, practices and processes for development, assessment and use of computer based safety critical systems.

End Notes

[1] For simplicity, 'computer' is used in this position statement for any programmable electronics that is embedded in a system. The programmable electronics can range from an embedded chip to a complex network of computers.

The Institution of
Engineering and Technology

The Institution of Engineering & Technology
Michael Faraday House
Six Hills Way
Stevenage
SG1 2AY

01438 765690 - Policy Department
email: policy@theiet.org
http://www.theiet.org/policy
http://www.theiet.org/factfiles

CPD™

This content can
contribute towards your
Continuing Professional
Development (CPD) as
part of the IET's CPD
Monitoring Scheme.
http://www.**theiet.org**/cpd