PROGRAMMABLE ELECTRONIC SYSTEMS IN SAFETY RELATED LIFT APPLICATIONS

S. K. MATHUR

Dewhurst plc, UK

SCOPE

With the advent of Programmable Electronic Systems (PESs) in safety related lift systems, need has arisen to clarify those areas covered by the Safety Rules for the Construction of Lifts (1&2) where PESs may or may not, be applied. This paper is based on the guidelines prepared by the National Association of Lift Makers under the chairmanship of the writer.

The guidance applies if one or more of the safety related systems associated with a plant is a PES. It does not apply if an adequate level of safety is assured by one or more conventional systems, separate from the controlling PES, of conventional safety integrity or better. The conventional system will need to adequately cater for, amongst other things, failures of the controlling PES itself.

GENERAL

A PES is a computer-based system which controls, protects or monitors the operation of plant or machinery, it is made up of both hardware and software and is linked to the plant by sensors and actuators.

When evaluating safety it is important to realise that PESs are fundamentally different from conventional control systems. For example, it is not always easy to predict the effect of the failure of a PES, or even to discover where the fault lies. PESs may be used to control or monitor safety circuits but should not be used to fulfil the function of a safety contact such as those listed in Appendix A of references (1&2).

Very often computer controlled lift equipment is installed in place of conventional systems. In these cases, as a general guiding principle, the new systems should be at least as safe as the conventional one. However, as technology develops, there may not be a conventional equivalent and these guidelines combine sound lift engineering practice with the Health and Safety Executive recommendations of references (3&4) to achieve a satisfactory level of safety.

PESs can be used in a variety of ways and the consequences of failure may range from inconvenience to a dangerous situation. The safety measures adopted must be appropriate to the particular application and the degree of the safety strategy needed will depend upon the level of hazard presented.

Where PESs perform a safety function they should be so designed that a combined failure or malfunction of hardware and software cannot reduce the level of safety integrity.

DESIGNING FOR SAFETY

When a new installation is being designed, or the safety of an existing one is being assessed, it is essential to follow the following five logical and systematic steps to make sure that adequate safety precautions have been taken. The correct procedure to follow is shown as a flow chart in Appendix 1.

Step A - Hazard Analysis

The first stage in any safety assessment is to identify the hazards, i.e. dangerous situations in which people are likely to be injured, and then find the chain of events that could lead to these hazards. This analysis has already been carried out for lifts and has resulted in a set of safety rules for electric and hydraulic lifts as covered by references (1&2) respectively.

Step B - Identification of the Safety-Related System

From the hazard analysis it is possible to identify the safety systems and decide whether they fall within the scope of this paper, bearing in mind that a safety related system is one upon which the safety integrity of the lift is to be assured. These systems can broadly be divided into two types - control systems and protection systems.

When attempting to identify a safety related system it is important to note that although the breakdown of a programmable electronic control system might itself be part of a chain of events leading to a hazard, if it is effectively protected by a separate system which prevents the hazard arising, then the control system is not safety related and therefore does not have to comply with these guidelines.

To assist in identifying safety related systems, Appendix 2 covers some of the potential hazards identified and some of the protection systems recommended in (1). Column 3 gives examples of how the use of a PES would make the application of these guidelines relevant.

Step C - Determination of the Required Safety-Related Level

A safety analysis has already been carried out for lifts in references (1&2) and the safety criteria has been established. This falls under three categories, examples of which are indicated in column 4 of Appendix 2.

Category A. All electric safety devices covered in Appendix A of references (1&2) which are defined as safety contacts only and which satisfy 14.1.2.2. PESs are not permitted for this category.

Category B. All electric safety devices covered in Appendix A of references (1&2) which are defined as safety circuits and which satisfy 14.1.2.3. PESs can be used but the guidelines to use are those specified by H&SE for high reliability circuits in their publication 'Programmable Electronic Systems in Safety Related Applications Part 2 - General Technical Guidelines' (4).

Category C. All other safety related conditions not covered by Category A or B above but protected by an electric device. PESs can be used provided they comply with the design guidelines which involve improving three fundamental aspects of an installation, the configuration, reliability and quality. These are described in detail below in Step D.

Step D - Design of the Safety-Related System

Configuration. Three principles must be satisfied to provide an acceptable design and assessment strategy. These are:

(a) The combined number of PES and non-PES safety related systems which are capable, independently, of maintaining the lift in a safe state or of bringing the lift to a safe state when required should not be less than the number of conventional systems which have provided conventional safety integrity; and
(b) No failure, random or systematic of a single channel of programmable electronics hardware should cause a dangerous mode of failure of the total configuration of safety related systems. It should be recognised that systematic hardware failures may affect all identical designs of programmable electronics; and
(c) Faults within the software associated with a single channel of programmable electronics should not cause a dangerous mode of failure of the total configuration of safety related systems. It should be assumed that a software fault will affect all identical software.

These guidelines assume that the configuration of the relevant circuitry is covered by one of the following:

(1) Non PES control systems protected by a PES circuit.
(2) PES control system monitored by one or more PESs each totally independent of the other.

Hardware Reliability. All PESs used in either the control system or protection circuitry must satisfy a qualitative appraisal using engineering judgement. Aspects of the programmable electronics which should be considered are:

(a) The extent to which the programmable electronics are used to monitor the correct operation of critical items such as sensors and actuators using, for example, signal validity checks designed into the applications software.
(b) The extent and effectiveness of measures to ensure that critical failures of the programmable electronics do not remain unrevealed. Such measures include:
  - sum checks or other means of detecting corruption of program or data stored in Read Only Memory (ROM).
  - bit pattern tests or other means of testing the correct functioning of Read/Write Memory (RAM).
  - watchdog timer to detect program halt or loop conditions.
  - power supply monitor to detect incipient failure.
(c) The effectiveness of the means by which safety is maintained on detection of a failure, either automatically or by alarms and operator response.
(d) the testing provisions of critical elements not necessarily covered by (a) and (b) above including in particular the proof check intervals for the item in question.
(e) the predominant failure modes.
(f) the complexity and relative reliability of the hardware.
(g) the adherence to applicable systems which may specify hardware failure criteria such as, for example, that no single failure should result in an unsafe condition.
(h) the degree of redundancy of all parts of the programmable electronics.

Software Reliability. The necessary phases of a software development will vary according to the system but, typically, the following phases should be carried out to reflect high quality and good reliability of the software.

(a) Requirements specification
(b) Software specification
(c) Software design
(d) Software coding
(e) Software test
(f) System test

All aspects of software production and change should only be carried out by authorised and competent personnel. Each phase of the software development program should be documented sufficiently in order to:

(a) Allow adequate communication between all participants in the design program.
(b) Allow the design to be reviewed with agreed milestones as it proceeds.
(c) Allow each stage in the design to be checked and approved on completion.
(d) Allow the operation of the software to be fully understood in the future.
(e) Allow changes to be incorporated in a controlled manner.
(f) Allow the full implications of changes to be evaluated.
(g) Clearly define the software being used on site.

Quality. The minimum level of overall quality for safety related systems is specified in (a) and (b) as follows:

(a) Quality of manufacture. The programmable electronics should be manufactured using an established quality assurance system, such as BS 5750. Other parts of the PES should be to a level of quality not inferior to conventional safety integrity; and
(b) Quality of implementation. The safety related systems, particularly those that are PES based, should be engineered by competent and experienced people who understand PES safety engineered principles related to lift systems.

Step E - Safety Analysis

Once the design has been completed an analysis should be carried out to ensure that the required level of safety integrity for the safety related systems has been achieved. The analysis must extend to all those components, of safety related systems, whose failure could cause the safety related systems themselves to fail and affect the safety of the lift installation.

The analysis must cover all three system elements of configuration, reliability and overall quality and therefore confirm that the requirements listed under safety categories B and C.

ENVIRONMENTAL ASPECTS

Temperature. The design of the equipment, and the components used, must be suitable for the ambient temperature in which they are to work, there must be due regard for the temperature rise of the equipment itself and the temperature under which the equipment may be stored and transported.

Humidity. The equipment must be protected from the effects of humidity during storage and operation, and particularly where there is a possibility of installation being undertaken in initially unheated buildings.

Dust, Corrosive and Explosive Atmosphere. Due consideration must be given, including during storage and transport, where the environment is such there might be dust, corrosive or explosive atmospheres, and the design needs to take these into account.

Interface - Electrical and Electro-Magnetic. Electrical and electro-magnetic interference has four possible sources, it may be:

(a) Mains borne
(b) Generated by the lift control system
(c) Generated by the PES itself
(d) Radiated from external sources

Interference such as spikes, surges and dips, flicker, harmonics and transients from these sources must not affect the PES in any way that reduces the level of safety.

The equipment should be designed using sound engineering practice. Due consideration should be given to the quality of power supplies, logic and mains, along with earth bonding, screening, de-coupling, avoidance of earth loops and segregation of power/signal cables.

Any suppression and filtering necessary to ensure correct operation of the PES, in order to achieve the required safety criteria, should be documented. This is to guard against the possibility of the suppression devices being removed or changed during the life of the equipment.

Electro-Static Discharge (ESD) Damage. Many devices used in electronic systems are susceptible to ESD damage. This damage is not necessarily destructive or immediately apparent, but can lead to intermittent faults or degraded performance.

Steps should be taken during manufacture, storage, transport and installation of the equipment to minimise risk and provide guidance on correct handling procedures.

Programmable Memory Devices. Adequate precautions should be taken to safeguard against the effects of X-rays and ultra-violet light radiation.

SOFTWARE CONSIDERATIONS

Software for safety related applications should be of a high quality to ensure reliable operation throughout its life. Quality must be considered from the outset to make certain that software is correctly specified, designed, documented, tested and controlled.

Adjustments to equipment operation parameters (e.g. door dwell times) on site using hardware jumpers, pinboard, switches etc. must be fully documented if they affect software functions. Records should be kept on site and at the offices of manufacturers and/or service organisations.

It is essential that throughout the software development or modification phase all changes should be implemented in a controlled fashion to ensure that:

(a) All possible implications of a change are considered and the proposed change authorised before implementation.
(b) The specification changes are communicated to all the relevant people involved in the design, application and maintenance work of the lift equipment.
(c) The documentation relating to each type and version of software should be clearly numbered and dated. The same program number should be marked clearly on the device housing the software in the lift equipment for easy recognition.
(d) The software has maintained the original level of safety integrity and errors have not been introduced inadvertently.

REFERENCES

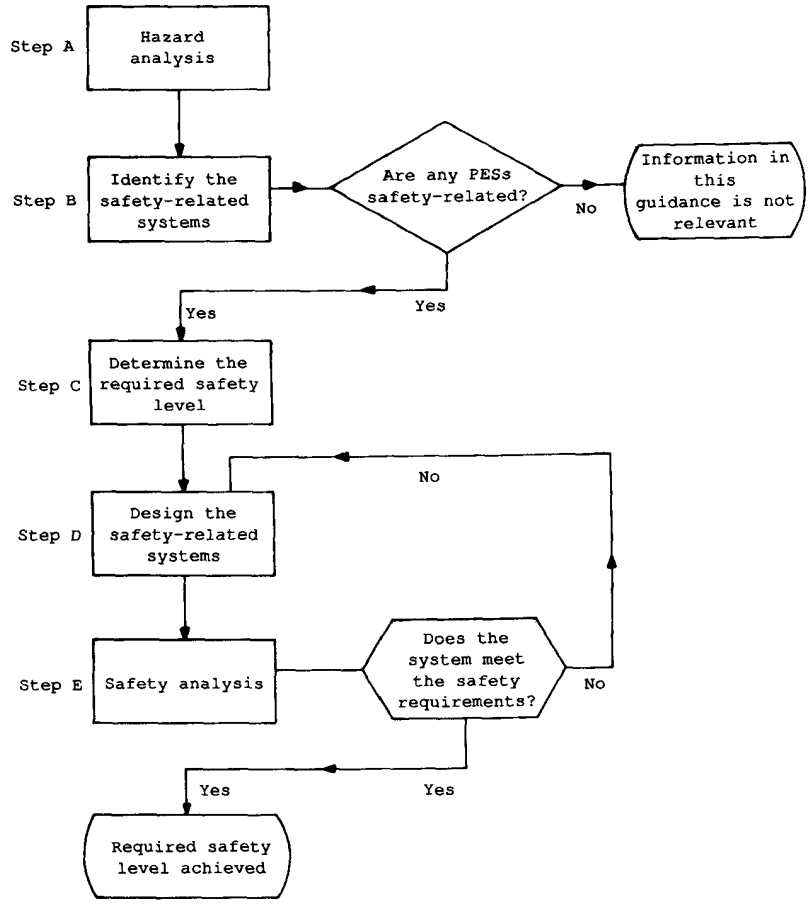
1. Safety Rules for the Construction and Installation of Electric Lifts, 1986, BS 5655:Part 1.

2. Safety Rules for the Construction and Installation of Hydraulic Lifts, 1988, BS 5655:Part 2.

3. Programmable Electronic Systems in Safety Related Applications - Part 1: An Introductory Guide, 1987, Health and Safety Executive.

4. Programmable Electronic Systems in Safety Related Applications - Part 2: General Technical Guidelines, 1987, Health and Safety Executive.

APPENDIX 1



Design and Assessment Flow Chart

APPENDIX 2

Potential Hazard	Examples of Protection	PES Application	Category
Lift travelling beyond terminal floor	Final limit switch	Safety contact	A
Unexpected car movement on inspection control	Mechanical switch on car roof to neutralise normal operation	Safety contact	A
	Movement of car dependent upon constant pressure buttons	Constant pressure buttons feeding directly a PES control system with no separate protection circuitry monitoring button operation	C
	Check car speed does not exceed predetermined value	PES used to monitor speed check	C
Lift exceeding contract speed	Overspeed governor/other device by means of safety device initiates stopping of lift machine	PES used as a safety circuit to initiate stopping of lift	B
Lift hitting reduced stroke buffer at a speed in excess of design value	Auxiliary slowdown system	PES as part of slowdown system	B
Lift moving with doors open	Limit all movement to within unlocking zone	PES used in a safety circuit limiting movement to within unlocking zone	B
	Check speed does not exceed predetermined value	PES used to monitor speed check	C
Unexpected car movement during docking operation	Movement limited to pre-determined zone	PES used in a safety circuit limiting movement in unlocking zone	B
	Check car speed does not exceed predetermined value	PES used to monitor speed check	C
Person being struck by a door	Sensitive protective device	Protective device feeds directly into a PES	C
	Door speed reduced to limit kinetic energy	PES controls speed of door motor	C
Machine not stopping when initiated by a safety device	At least two independent means	PES used to monitor and verify blocking flow of energy by either of two independent means	C
Oscillating lift operation due to control system failure	Not defined	Power control system using a PES, no additional circuit protection	C

Some Examples of Potential Hazards, Protective Systems and PES Applications