INTRODUCTION

Systems comprised of electrical and/or electronic ~~components~~ elements (1) have been used for many years to perform safety functions in most application sectors. Computer-based systems (generically referred to as programmable electronic systems ~~(PESs)~~) are being used in all application sectors to perform non-safety functions and, increasingly, to perform safety functions. If computer system technology is to be effectively and safely exploited, it is essential that those responsible for making decisions have sufficient guidance on the safety aspects on which to make these decisions.

This International Standard sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic ~~components (electrical/electronic/programmable electronic systems (E/E/PESs))~~ (E/E/PE) (2) elements (1) that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems. A major objective is to facilitate the development of product and application sector international standards based on the IEC 61508 series.

NOTE 1 Examples of product and application sector international standards based on the IEC 61508 series are given in the Bibliography (see references [1], [2] and [3]).

In most situations, safety is achieved by a number of ~~protective~~ systems which rely on many technologies (for example mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic). Any safety strategy must therefore consider not only all the elements (1) within an individual system (for example sensors, controlling devices and actuators) but also all the safety-related systems making up the total combination of safety-related systems. Therefore, while this International Standard is concerned with ~~electrical/electronic/programmable electronic (~~E/E/PE~~)~~ safety-related systems, it may also provide a framework within which safety-related systems based on other technologies may be considered.

It is recognized that there is a great variety of ~~E/E/PES~~ applications using E/E/PE safety-related systems in a variety of application sectors and covering a wide range of complexity, hazard and risk potentials. In any particular application, the required safety measures will be dependent on many factors specific to the application. This International Standard, by being generic, will enable such measures to be formulated in future product and (10) application sector international standards and in revisions of those that already exist.

This International Standard

– considers all relevant overall, E/E/PE~~S~~ system (2) and software safety lifecycle phases (for example, from initial concept, through design, implementation, operation and maintenance to decommissioning) when E/E/PE~~Ss~~ systems (2) are used to perform safety functions;

– has been conceived with a rapidly developing technology in mind; the framework is sufficiently robust and comprehensive to cater for future developments;

– enables product and application sector international standards, dealing with E/E/PE safety-related ~~E/E/PESs~~ systems (2), to be developed; the development of product and (10) application sector international standards, within the framework of this standard, should lead to a high level of consistency (for example, of underlying principles, terminology etc.) both within application sectors and across application sectors; this will have both safety and economic benefits;

– provides a method for the development of the safety requirements specification necessary to achieve the required functional safety for E/E/PE safety-related systems;

– adopts a risk-based approach ~~for the determination of~~ by which the safety integrity ~~level~~ requirements can be determined;

– ~~uses~~ introduces safety integrity levels for specifying the target level of safety integrity for the safety functions to be implemented by the E/E/PE safety-related systems;

NOTE 2 The standard does not specify the safety integrity level requirements for any safety function, nor does it mandate how the safety integrity level is determined. Instead it provides a risk-based conceptual framework and example techniques.

– sets ~~numerical~~ (3) target failure measures for safety functions carried out by E/E/PE safety-related systems, which are linked to the safety integrity levels;

– sets a lower limit on the target failure measures~~, in a dangerous mode of failure, that can be claimed~~ for a safety function carried out by a single E/E/PE safety-related system (4). For E/E/PE safety-related systems operating in

  – a low demand mode of operation, the lower limit is set at an average probability of ~~failure~~ a dangerous failure on demand of 10^{-5} ~~to perform its design function on demand~~;(4)

  – a high demand or a continuous mode of operation, the lower limit is set at ~~a probability~~ an average frequency of a dangerous failure of 10^{-9} ~~per hour~~ [h^{-1}];(4)

NOTE 3 A single E/E/PE safety-related system does not necessarily mean a single-channel architecture.

NOTE 4 It may be possible to achieve designs of safety-related systems with lower values for the target safety integrity for non-complex systems, but these limits are considered to represent what can be achieved for relatively complex systems (for example programmable electronic safety-related systems) at the present time.(6)

– sets requirements for the avoidance and control of systematic faults, which are based on experience and judgement from practical experience gained in industry. Even though the probability of occurrence of systematic failures cannot in general be quantified the standard does, however, allow a claim to be made, for a specified safety function, that the target failure measure associated with the safety function can be considered to be achieved if all the requirements in the standard have been met;(7)

– introduces systematic capability which applies to an element (1) with respect to its confidence that the systematic safety integrity meets the requirements of the specified safety integrity level;(8)

– adopts a broad range of principles, techniques and measures to achieve functional safety for E/E/PE safety-related systems, but does not explicitly use the concept of fail safe ~~which may be of value when the failure modes are well defined and the level of complexity is relatively low. The concept of fail safe was considered inappropriate because of the full range of complexity of E/E/PE safety-related systems that are within the scope of the standard.~~(5) However, the concepts of “fail safe” and “inherently safe” principles may be applicable and adoption of such concepts is acceptable providing the requirements of the relevant clauses in the standard are met.(9)