IEC 61508 – A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems??

Derek Fowler and Phil Bennett

CSE International Ltd
Glanford House, Bellwin Drive, Flixborough, N Lincs, DN15 8SN, UK
Tel. +44 1724 862169, Fax: +44 1724 846256
df@cse-euro.demon.co.uk
pab@cse-ltd.demon.co.uk

Abstract. IEC 61508 is widely viewed as the best available international generic standard for the management of functional safety in the development, operation and support of electrical, electronic and programmable electronic systems (EEPES). There is a danger, of course, that the existence of IEC 61508 will be seen as the solution to a wider range of problems in the development of safety-critical systems than such a standard could be capable of addressing. The suitability of IEC 61508 for the specification of relatively simple protection systems is not in doubt. However, in considering how effectively IEC 61508 could be used in the more complex environment of transport-infrastructure systems, the paper discusses the fundamental nature of, and means of deriving, safety requirements and considers how effectively compliance to the Standard may be used to provide assurance that a system is safe. From these discussions, the paper concludes on the feasibility and value of system certification against IEC 61508.

1 Introduction

CSE International Ltd has provided consultancy services in the field of software-intensive, safety-critical systems since the Company was founded in 1983. The techniques developed by CSE have been applied by the Company very successfully on software-intensive systems for a wide range of applications from safety-critical vehicle management systems to large infrastructure projects, including, the Channel Tunnel, Hong Kong’s International Airport at Chek Lap Kok, Railtrack’s West Coast Route Modernisation programme, a number of new European Air Traffic Management programmes, and Heathrow Airport’s Terminal 5 project. The Company has also been heavily involved in the development of safety standards, especially IEC 61508, and in the design and delivery of safety training courses.

IEC 61508 [Ref 1] sets out a generic approach for all safety lifecycle activities for developments that involve the use of electrical, electronic and/or programmable
electronic systems (EEPES) to perform safety functions. A key objective of the Standard is to facilitate the development of specific application-sector standards based on a rational and consistent technical policy.

The suitability of the Standard for use in relatively simple protection systems - typical of, say, the process and automotive industries – is fairly evident; indeed it is in such applications that the Standard has its origins.

Based on analysis first described in [Ref 2], this paper considers how IEC 61508 could be adapted to more complex, safety-related environments such as the development of transport-infrastructure systems. It examines two key areas: the derivation of safety requirements (including safety integrity levels (SILs), on which the application of most of IEC 61508 depends) and the relevance of the Standard to the safety assurance process (on which safety approval is usually based). It then outlines the evidence-based approach, adopted by the UK Civil Aviation Authority Safety Regulation Group, and proposes this as an improved way of applying the IEC 61508 to safety assurance. It concludes by considering whether system conformance and/or certification are meaningful concepts in the context of complex transport-infrastructure systems.

2 IEC 61508 Fundamentals

It is a fundamental requirement of IEC 61508 that, in the specification of any potential safety-related system, three key elements be identified:

• equipment under control (EUC) – “equipment, machinery, apparatus used for manufacturing, process, transportation, medical or other activities”;

• EUC control system - “…responds to input signals from the process … and generates output signals causing the EUC to operate in the desired manner”;

• safety-related system - “system that … implements the … safety functions necessary to achieve or maintain a safe state for the EUC and is intended to achieve … the necessary integrity for the … safety functions”.

The third point, that safety-related systems (SRS) are those systems whose primary purpose is to reduce risk from the EUC / control system, is fundamental to understanding the nature of system safety requirements, as explained below.

3 System Safety Requirements

According to IEC 61508, safety requirements (ie the requirements of an SRS) need to be specified in two, complementary forms:

• a description of the functions to be performed by the SRS; and

• the integrity required of each of those functions;

as necessary to reduce to an acceptable level the risks originating in the EUC.