Independent Safety Assessment of Safety Arguments

Peter Froome
Adelard LLP,
London, United Kingdom

Abstract

The paper describes the role of Independent Safety Auditor (ISA) as carried out at the present in the defence and other sectors in the UK. It outlines the way the ISA role has developed over the past 15–20 years with the changing regulatory environment. The extent to which the role comprises audit, assessment or advice is a source of confusion, and the paper clarifies this by means of some definitions, and by elaborating the tasks involved in scrutinising the safety argument for the system. The customers and interfaces for the safety audit are described, and pragmatic means for assessing the competence of ISAs are presented.

1 Introduction

This paper is based on recent work carried out by Adelard for the UK Ministry of Defence (MoD), to produce guidance for project teams on contracting for Independent Safety Auditor (ISA) services.

It begins by explaining the origins of the Independent Safety Auditor (ISA) in the defence sector, and how the role has developed and expanded into other sectors, most notably the railways, over the last 15–20 years. It then describes the ISA role, by giving definitions of *independent*, *safety audit* and *safety advice*, and illustrates the scope of the role in terms of the way the ISA scrutinises a system's safety argument. The ISA's interfaces with the key customers are outlined, and the paper concludes with a discussion of competency assessment of ISAs.

As well as giving a factual account of the ISA role as captured in the new guidance, the paper provides some illustrations of potential difficulties and practical issues that arise.

2 Origins of Independent Safety Audit

The requirement for an Independent Safety Auditor for MoD projects first appeared in Interim Defence Standard 00-56 (Safety Management Requirements for Defence Systems), published in 1991 (MoD 1991). The aim was to provide an objective, independent opinion of safety that was lacking in defence projects at that time, except in certain special areas such as those covered by the Ordnance Board and the Chief Naval Architect.

Interim Def Stan 00-56 was written by Adelard under contract to the Directorate General Submarines (DGSM), the principal authors being Peter Froome and Robin Bloomfield. The ISA role was based on their experience during the Sizewell B Inquiry in the then CEGB's Health and Safety Department (HSD), which provided scrutiny of safety, independent from operations up to Board level, and was also the interface to the regulator (the Nuclear Installations Inspectorate or NII). Since there was no statutory regulator in the defence sector, the ISA role was intended to cover both independent scrutiny and quasi-regulatory responsibilities.

The role was originally entitled "independent safety assessor", but was changed to "independent safety auditor" at a late stage in the drafting by the Steering Committee that oversaw the development of Interim Def Stans 00-55 and 00-56. This change has led to confusion over the scope of the role ever since.

At the time, MoD was protected by Crown Immunity and safety was seen as largely the Contractor's responsibility, and therefore it was envisaged that the ISA would be appointed by the Contractor. Since the Interim Def Stan was published, the role has developed as a result of the changing legal framework and developing safety policy within MoD. Crown Immunity has been lifted: MoD is now a self-regulating organisation with regard to safety where it has been granted specific exemptions, disapplications or derogations from legislation, international treaties or protocols. The safety offices and safety boards provide this self-regulation within MoD, as defined in their respective safety management publications (e.g. MoD 2002a, MoD 2002b, MoD 2002c, MoD 2003). The ISA role is now founded on MoD safety policy that introduces independence into safety regulation by requiring or recommending that the "Duty Holder" (normally the Integrated Project Team or IPT Leader) seeks an ISA's opinion on the quality of the safety case for new or modified equipment. However, the ISA differs from a statutory regulator in having no executive authority or power of veto. The IPT accepts full responsibility for safety, and may overrule an ISA's recommendations.

The ISA is also important in other sectors. The ISA role (known as "functional safety assessment") is part of IEC 61508 (IEC 1998). The ISA also has an important role in the railway sector, where best practice as detailed in the Yellow Book (Railtrack 2000, RSSB 2003) recommends that Independent Safety Assessment is conducted with a level of rigour and independence that is related to the degree of safety criticality of the change. ISAs are also used in the automotive sector, where the role is mainly assessment with possibly some further analysis. Use of an ISA is not mandatory but automotive manufacturers see it as protection. Experience of the role in these different sectors is being shared through the IEE/BCS ISA Working Group, which is the subject of another presentation at this symposium.

The ISA role is becoming ever more challenging. Functional safety (i.e. the safety of data and commands, as opposed to "physical safety") is an increasing concern, especially with the widespread use of computers running commercial software packages. The MoD's new secure digital voice and data communications system, Bowman, is a "systems of systems" involving over a hundred individual safety cases with complex interdependencies, produced to extremely tight timescales where safety problems can lead to significant financial losses as well as loss of capability.