Peter Froome, "Independent Safety Assessment of Safety Arguments"
First published in Proceedings of Thirteenth Safety-critical Systems Symposium, 8–10th February 2005, Springer-Verlag

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.

Provision of advice is also becoming increasingly important with the emergence of "goal-based" safety standards such as the CAA's SW01 (CAA 1999) and the Issue 3 of Def Stan 00-56 (MoD 2004). These standards require considerably more interpretation than older, prescriptive, standards. The ISA plays a key role in supplying this interpretation, while taking care to preserve their independence.

3 The Independent Safety Audit Role

As mentioned in the introduction, there has been uncertainty over the exact role of the ISA ever since it was invented. The role as currently defined in the MoD's safety management publications, Def Stan 00-56/2 (MoD 1996) and the Yellow Book (Railtrack 2000) is a mixture of assessment and audit. This has been investigated by the IEE/BCS ISA Working Group, which concluded that the role was likely to be a combination of auditing for conformance to planned arrangements, reviewing of project documentation, and performing additional analyses.

Underlying the ISA role is the fact that safety is fundamentally a property of the equipment, not the process used to develop it. Although processes are important for managing projects and ensuring the production of deliverables and other outputs that provide safety evidence, the judgement of whether an adequate level of safety has been achieved has to be made on the basis of the equipment properties and performance. Thus the ISA role has to include assessment and analysis.

This section explores the ISA role as it is carried out at the present time, firstly in terms of key definitions (*independent*, *safety audit* and *safety advice*), and then by considering how the ISA reinforces the safety case by examining the elements of a system's safety argument.

3.1 Definitions

3.1.1Independent

The various safety standards and guidelines devote a considerable amount of space to whether the ISA should be from a separate department, separate organisation, etc., in order to be sufficiently independent. Formal requirements for independence based on Safety Integrity Level (SIL) are provided in IEC 61508 (IEC 1998) and the Yellow Book (Railtrack 2000), and JSP 430 (MoD 2002a) requires that the ISA is from an independent company, or is at least managerially independent up to board level.

However, the key consideration is that the ISA needs to be able to provide an expert, professional opinion without vulnerability to commercial, project or other pressure. Informally, this means that the ISA needs to be sufficiently independent that they are sheltered as far as practicable from pressure to modify their opinion, and that their career prospects are enhanced rather than damaged by carrying out a searching assessment.

The organisation that contracts the ISA must respect this independence. They should give the ISA substantial freedom to conduct the safety audit as the ISA judges to be appropriate. The relationship is similar to contracting an auditor in other areas, such as quality management or accountancy. An authorised ISA has the right and duty to raise significant concerns directly with the procurer or contractor, even when outside their agreed scope of work or terms of reference, and should raise unresolved concerns with the appropriate safety authorities and regulators.

The need for an independent auditor does not mean that the company that is the target of the audit has to accept someone from a competitor. Even if a non-disclosure agreement is signed, it is impossible to remove the information held in the ISA's head and it might be divulged unwittingly or under pressure from peers. The contracting organisation should negotiate a mutually acceptable ISA from an organisation that does not compete with the contractor, even though it may then be more difficult to find an ISA with appropriate domain experience.

3.1.2 Safety audit

Safety audit consists of the activities that enable an expert, professional, independent opinion to be reached on the safety of the system. Worded this way, it is clear that "traditional" auditing against planned arrangements is not sufficient, and expert document review and diverse analysis will generally form the majority of the ISA's work. Note that, in the defence sector, safety audit is targeted at both the contractor and the IPT.

Thus, for example, a contractor should not refuse to co-operate with the ISA over the provision of data to support failure rate claims, on the grounds that analysis of such data is not an audit function. This is not acceptable if the ISA judges the data to be an essential component of the safety argument.

The best way of identifying the safety audit activities on a particular project is to consider how the ISA will scrutinise the safety argument; this is examined in Section 3.2 below.

3.1.3 Safety advice

In order to maintain their independence, the ISA cannot give specific advice or contribute directly to the safety argument. However, an ISA may provide general advice on the acceptability of a proposed safety argument, which facilitates the procurer's or contractor's decision-making, helps to develop an effective safety strategy, and reduces project risk from safety matters.

The ISA may also need to give advice where some part of the safety work is unacceptable—it is not particularly helpful if the ISA maintains this without saying why.

A strategic level of advice is reasonable, and is similar to the "assessment guidelines" produced by the statutory regulators. One possible criterion is that advice can be given when it is not specific to the project (e.g. advice on general safety argument structures) and facilitates the project's own decision-making.

A classic problem is that the contractor asks the ISA to revise portions of the safety documentation that they have found unsatisfactory. The ISA should not do this, as they would then take ownership of part of the safety argument. However, they can illustrate how such a revision should be performed, by reference to published standards, guidance or papers, or possibly by analogy with other, similar, projects.

3.2 Scrutiny of the Safety Argument

Many sectors in the UK, including defence and railways, are obliged by law to produce a written safety justification for their operations, which is normally known as a "safety case". The safety case for a system is based on a *safety argument*. Typically the overall, top-level argument is:

The system is safe to use to provide the defined capability because:

- The meaning of "safe" is defined and correctly captured in the safety requirements.
- The system meets the safety requirements.
- Safety will be maintained over the system's lifetime through a culture of safe working and safety management by the contractor and procurer/user organisations.
- The assumptions and prerequisites on which the safety case depends are valid.

Safety cases are beginning to contain an explicit safety argument, in which case the ISA can base the safety audit around that. Many safety cases contain only an implicit safety argument, however, and in that case the ISA has to establish the argument as part of the audit activities.

The ISA's work then consists of examining each of the components of this safety argument and forming an opinion as to whether it is complete and correct. As an example, consider the first bullet point. This is often broken down as illustrated in Figure 1 below.

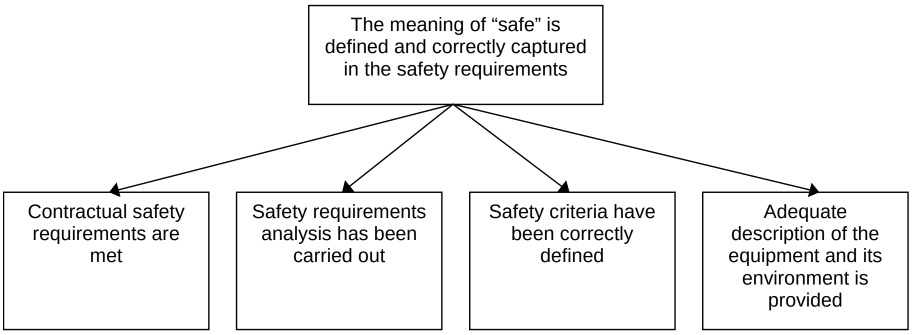
The meaning of "safe" is defined and correctly captured in the safety requirements
Contractual safety requirements are met
Safety requirements analysis has been carried out
Safety criteria have been correctly defined
Adequate description of the equipment and its environment is provided

Figure 1. Safety argument tree for safety requirements definition

The ISA's checks of this part of the safety argument might include the following:

- *Contractual safety requirements*—review for correctness, completeness, consistency, achievability, conformance to standards and legislation; check that evidence likely to be needed for subsequent safety arguments is contracted for.
- *Safety requirements analysis*—check the analysis; review reports for correctness, completeness, consistency, achievability, conformance to standards and legislation; audit the analysis process for conformance to standards and safety management plan; attend analysis meetings to check conducted in accordance with standards and good practice.
- *Safety criteria*—review the report for conformance to standards and safety management plan; check against HSE guidelines such as R2P2 (HSE 2001) and sector-specific standards; check for agreement with criteria from similar projects.

- *System and operating environment description*—check that the description is sufficiently comprehensive for the reader to understand the safety argument.

Broadly speaking, this pattern of work is repeated throughout the lifecycle, but there are some differences. For example, in the design and manufacturing phases, the ISA may carry out diverse analyses to estimate software or hardware reliability by means of appropriate modelling techniques, in order to check the argument tree for the second bullet point in the safety argument above (“The system meets the safety requirements”). Human factors analysis is another diverse analysis often undertaken by the ISA at this phase in the lifecycle, in order to check the safety requirements are met with respect to the entire socio-technical system.

4 Interfaces and Customers

The ISA has a number of customers for their work. The major ones, and the ISA’s interfaces to them, are illustrated generically in Figure 2.

Although the precise customers and interfaces vary with sector, some of the major interactions are as follows.

4.1 The project

Generally, the project contracts the ISA (in the defence sector, the ISA is sometimes contracted by the development contractor). The major deliverable is the ISA Report, which supports the safety case and is part of the submission to the regulator where present.

The ISA has to provide value for money and a project should monitor ISA performance against the contract accordingly. This can obviously lead to tensions in both directions:

- The ISA may feel inhibited about pursuing safety issues if they believe that the project has a negative view of the safety audit activities.

- The project may be reluctant to dismiss an ineffective ISA because of fears of being accused of compromising the ISA’s independence.

These tensions can be avoided by monitoring the ISA’s performance objectively, which is best done by checking their coverage of the safety argument as discussed in Section 3.2.

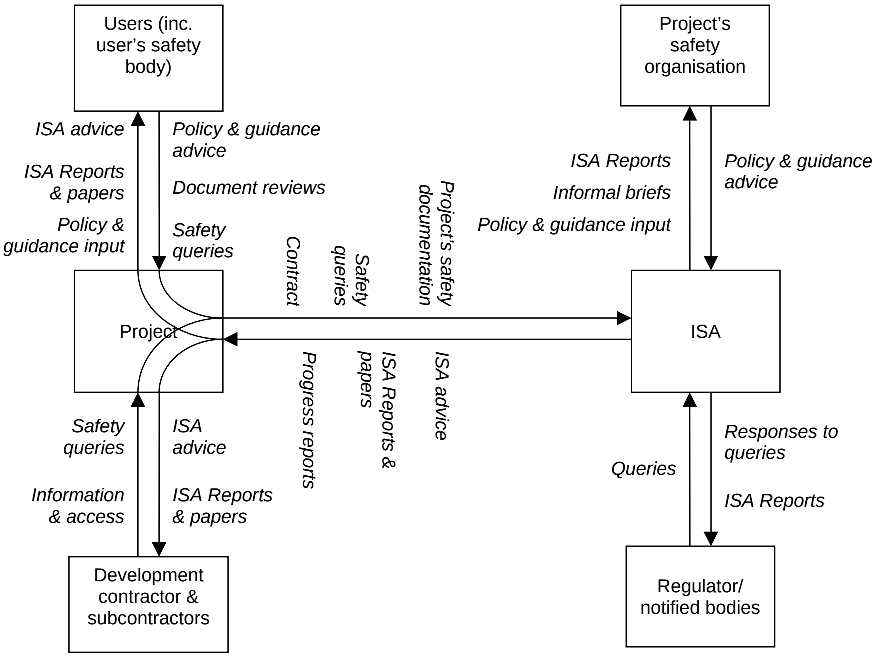

Figure 2. Typical ISA's customers and interfaces

4.2 The development contractor

It is essential that there is a spirit of co-operation between the contractor and the ISA, as otherwise the safety work will get bogged down with the danger to the project that the ISA will be unable to endorse the safety case.

The ISA should be acceptable to the contractor in terms of competence and scopes of work. The contractor can legitimately demand that the ISA safeguards their intellectual property and confidential information, and therefore may reasonably refuse to accept an ISA from a commercial rival. On the other hand, the contractor should provide access to the information that the ISA needs to form an independent opinion.

4.3 The user

Direct contact between the ISA and the user or end customer typically originates in safety committees.

However, it is possible that the user may raise safety concerns directly with the ISA where they are seeking a consensus on some safety issue. For example, user representatives may consider that certain functionality is implemented poorly from a safety perspective, and seek support from the ISA for requesting a change from the project.

In addition, the user may have its own in-service safety body, which may liaise with the ISA during the review of specific safety documentation and if safety issues arise.

4.4 Project's safety organisation

In some sectors, the project's organisation may include a safety department. In the defence sectors, these are the *functional safety management offices*. The safety department's role is to monitor effective safety management by contractors and projects, and to provide advice and guidance on safety management.

The ISA interfaces with the project's safety department in several ways, ranging from the formal ISA Reports to informal communication. Some safety departments also offer a useful arbitration service in case the ISA becomes deadlocked with the project and/or the contractor.

4.5 Regulator/Notified Bodies

In a sector where there is a formal regulation or certification regime, the ISA may interface with the regulator or certification body by means of the ISA Report and response to questions. In the railway sector, the ISA will need to interface to the Notified Body, if appointed.

5 Competence of ISAs

The ISA has to provide an authoritative, expert opinion on safety, and therefore has to be properly qualified. The qualifications required are not only technical, because the ISA also needs managerial and social skills in terms of safety audit planning, control of meetings, negotiating ability, and ability to defend their position in a firm but non-confrontational manner.

The author's approach is to prefer ISA teams for most projects, and this is also the position of the Yellow Book (Railtrack 2000). As well as enabling effective peer review of the assessment's outputs, teams and can provide specialist expertise in areas such as in human factors and software reliability modelling. Where a team is employed, it is the balance of skills that is important, and the team leader should demonstrate the ability to properly manage and co-ordinate the team. Individual team members should provide the in-depth knowledge that is required.

Competency requirements for ISAs are contained in sector-specific safety publications, and usually include Chartered Engineering status and several years' relevant experience. Formal competency assessment for ISAs has been discussed at length at the IEE/BCS ISA Working Group but there are difficulties with all schemes where competence is assessed by independent, third parties. In the absence of a completely satisfactory third-party scheme, this section discusses how ISA competence may be pragmatically assessed.

5.1 Competence criteria

There are three types of competence required for an ISA:

- *Technical competence*—safety and technical knowledge (of the application area and technology) required to support the activities of a safety audit.

- *Auditing competence*—skills necessary to perform the safety audit, i.e. to perform the activities that enable an expert, professional opinion to be reached on the safety of the system.

- *Behavioural competence*—qualities and attributes of behaviour and character needed to successfully perform the ISA role.

These are described in more detail in the following subsections.

5.1.1 Technical competence

Technical competence has two aspects:

- Technical competence in safety audit independent of the specific application and technology used. This includes knowledge and experience of the legal and safety regulatory framework, understanding the principles and concepts of safety management (e.g. ALARP, risk and safety requirements), and knowledge and experience of the standard safety analysis techniques such as Hazops and Fault Tree Analysis. It also includes the ability to estimate the necessary resources to perform such analyses and to judge the scope and depth of analyses carried out.

- Technical competence in the application domain, covering an understanding of the specific technologies used and their context in the particular domain. This includes safety engineering knowledge and experience appropriate to the application area and technology, including safety practices appropriate to the organisation and application area. It also includes engineering knowledge and experience appropriate to the application area (e.g. air traffic control) and technology (e.g. digital network communication). Experience of other systems engineering disciplines such as human factors may also be relevant.

5.1.2 Auditing competence

By contrast to technical competence, auditing competence considers the specific activities performed as part of a safety audit. This includes the ability to:

- Determine the scope and objectives of the safety audit and manage the auditing activities.

- Collect and analyse objective evidence to support the professional, expert opinion. As well as reviewing documents, this may include interviewing personnel at all levels and observing activities.

- Investigate evidence of possible problems.

- Carry out formal process audits against relevant standards, plans, etc.

- Make a judgement on the safety of a system.

- Document findings.

5.1.3 Behavioural competence

The ISA role can be stressful and demanding, particularly when the project under review is in trouble and time and money are in short supply. The ISA needs to have certain attributes of conduct and character in order to perform the role of ISA with efficacy. These include:

- Interpersonal skills.
- Competence in communicating at all levels of the organisation.
- Interviewing skills.
- Reporting and presentation skills.
- Integrity and trustworthiness.

5.2 Assessment of competence

The previous subsection lists the competence attributes that are expected of an ISA. Potential ISAs should be able to supply evidence of competence covering these attributes, supported by verifiable examples, as part of their proposal when bidding for an ISA role.

In principle, this evidence of competence could be of three types, according to who does the assessment:

- Self-assessment, i.e. the ISA presents evidence to demonstrate the competencies as part of their proposal. This will have to be assessed by the project on a case-by-case basis.
- Organisational assessment, i.e. the ISA is assessed by their organisation according to a scheme such as the IEE/BCS Competency Guidelines for Safety-Related System Practitioners (IEE 1999) or the Network Rail ISA Accreditation Scheme (NR 2003). The project should ask for any third-party audit of the scheme, which might be an ISO 9001 audit in the case of the IEE/BCS scheme, or Network Rail's audit in the case of their scheme.
- Assessment by a third-party independent organisation that designs a scheme and independently assesses the ISA. Currently the only third-party scheme in the UK is the CASS (Conformity Assessment of Safety-related Systems, see www.cass.uk.net) scheme, and there are very few registrants.

Given the limited extent of formal competency assessment of ISAs at the present time, projects will probably have to assess potential ISAs on the basis of organisational assessment where it has been carried out, supplemented by self-assessment to establish competence related to the specific programme.

6 Conclusions

The paper has described the ISA role as carried out at the present in the defence and other sectors in the UK. It has explained how the role arose in the defence and railway sectors in order to provide an expert, professional, independent opinion as part of the regulatory regime in those sectors. The balance of ISA activities between "traditional" audit and assessment is a source of confusion, but the paper has shown how the role can be defined in terms of the safety argument for the system that is the focus of the activities. The paper has also outlined the principal customers and interfaces for the ISA.

Clearly the ISA (whether an individual or a team) must be competent, but at present there is no established competency assessment scheme for ISAs. The paper has described the three types of competence required by ISAs (technical, auditing and behavioural), and discussed how ISA competence may be pragmatically assessed.

References

CAA (1999). CAP 670, Part B, SW01 (Requirements for Software in Safety Related ATS Systems), Civil Aviation Authority 1999

HSE (2001) Reducing Risks, Protecting People—the HSE's Decision-making process, HSMO, 2001

IEC (1998). IEC Functional safety of electrical/electronic/programmable electronic safety-related systems, IEC 61508 Parts 1–7

IEE (1999). *Safety, Competency and Commitment: Competency Guidelines for Safety-Related System Practitioners*, IEE, 1999. ISBN 0 85296 787 X

MoD (1991). Interim Def Stan 00-56, Safety Management of Defence Systems, 1991

MoD (1996). Def Stan 00-56 Issue 2, Safety Management Requirements for Defence Systems (Parts 1 and 2), 1996

MoD (2002a). JSP 430, MoD Ship Safety Management, Issue 2, May 2002

MoD (2002b). JSP 454, Procedures for Land Systems Equipment Safety Assurance, Issue 3, July 2002

MoD (2002c). JSP 520, Ordnance, Munitions and Explosives Safety Management System, February 2002

MoD (2003). JSP 553 (formerly JSP 318B), Military Airworthiness Regulations, 1st Edition, July 2003

MoD (2004). Def Stan 00-56 Issue 3, Safety Management Requirements for Defence Systems (Parts 1 and 2), to be published

NR (2003). Rail Corporate Independent Safety Assessor Accreditation, Crystal Blake, +44 (0) 20 7557 8513

Railtrack (2000). Engineering Safety Management, Issue 3 (Yellow Book 3), Railtrack, January 2000

RSSB (2003). Engineering Safety Management Yellow Book 3 Application Note 4, Independent Safety Assessment. Issue 1.0, Rail Safety and Standards Board