The Institution of Engineering and Technology

SaRS Safety and Reliability Society

bcs The Chartered Institute for IT

Institution of Mechanical Engineers

What is **Independent Safety Assessment (ISA)?**

Change History

Version	Date	Status
1.0	28 June 2010	First Issue
2.0	22 February 2011	Second Issue

Please send suggestions for improvements, for example of other open access sources of data, for consideration by the Working Group to:

- isawg@theiet.org

Disclaimer

Cover Images (clockwise from top left)

- Nuclear power plant
- Euro fighter
- Oil and natural gas offshore platform
- London Underground

About the supporting organisations

- The IET is registered as a Charity in England & Wales (No. 211014) and Scotland (No. SC038698)
- The BCS is a registered charity (No. 292786)
- IMechE is a registered charity in England and Wales (No. 206882)
- SaRS is a registered charity in England and Wales (No. 801207)

1. Definition of ISA

Independent safety assessment is the formation of a judgement, separate and independent from any system design, development or operational personnel, that the safety requirements for the system are appropriate and adequate for the planned application and that the system satisfies those safety requirements. A person who carries out independent safety assessment is known as an independent safety assessor or ISA.

Note: In some industry sectors the term 'Functional Safety Assessor' is used for 'Safety Assessor'.

In carrying out independent safety assessment, the key tasks are:
- Acquiring an appreciation of the scope and context of the assessment
- Selecting and planning a cost-effective assessment strategy
- Gathering relevant evidence
- Forming a judgement
- Managing any outcomes.

Gathering the evidence is likely to be a combination of auditing for conformance to planned arrangements, reviewing project documentation and performing additional analyses.

The individual, department or organisation carrying out the assessment should be demonstrably competent for the safety tasks undertaken.

A supplier, company or project can call in external safety advisors. However, this is not considered by the ISA Group to be within the ISA role as defined in current international and UK standards. Independent safety assessors may be asked to give advice to a supplier, company or project but this may compromise the independence of the ISA role and function.

2. Who uses Independent Safety Assessors?

Anyone who needs or wants an independent assessment of safety.

Reasons include:
- To comply with a standard that requires an ISA
- To be assured that a contractor's product is safe
- To assure your customer that what your product is safe
- To assure yourself that your product is safe
- To demonstrate to a regulator that your product is safe

Because the safety assessment provided by the ISA is independent of existing safety analysis and assessment, it can provide confidence that safety claims are justified and that any weaknesses that are identified have been dealt with appropriately.

In some situations an ISA is mandatory. For instance, when carrying out work on safety critical systems for the UK railway industry.

In some other cases, use of an ISA is good practice. For instance, IEC 61508 represents best practice for safety-related electrical/electronic/programmable electronic systems (E/E/PES). It requires the use of independent safety assessment (called functional safety assessment in the standard) where the degree of independence depends on the Safety Integrity Level of the system.

Independent safety assessment is retained in the industry-specific standards based on IEC 61508. Within the motor industry, the MISRA (Motor Industry Software Reliability Association) Development Guidelines for Vehicle Based Software recommend the use of an independent assessor and/or auditor in order to act as an advocate for the level of confidence in the safety delivered to the end customer. In Defence, Def Stan 00-56 recommends an Independent Safety Audit role that encompasses safety assessment.

As well as providing assurance of safety, using an ISA can help to focus safety planning and analyses. This can come about naturally by answering questions and providing safety information for the ISA. However, in addition, an ISA is often able to offer generic guidance that does not compromise independence, particularly in the early stages of a project.

3. Independent safety assurance FAQ's

The ISA Working Group have generated an initial set of answers to frequently asked questions.

Q - What are ISAs used for?

ISAs objectively assess the safety aspects of a process, system or organisation. From the evidence gathered in the assessment the ISA forms a judgement on whether the safety requirements have been met. The ISA may use techniques such as auditing, analysis, interview, review or witness testing to gather the required evidence. See also the definition of the ISA function.

Q - Can an ISA be involved directly with a project for example to help write the safety case?

It is not recommended and should be avoided. Any direct involvement with a safety product could compromises the independence of the ISA. The pitfalls of advice are summarised in the ISA Guidelines for MOD Projects, which states:

> "Suppliers and IPTs (the supplier's customer) often need in-depth independent safety advice, particularly if the ISA identifies an evidence shortfall, in what safety processes can provide the necessary additional evidence. Such advice can compromise the ISA as they then have an interest in the success of the advice. Therefore it is best to provide independent safety consultants for advice rather than the appointed ISA. Clearly, it would be the ISA's responsibility to identify areas of weakness and evidence shortfall in the safety argument."

Furthermore, any advice an ISA gives should be documented so that the context of the advice is understood.

Q - What is the scope of the ISA's task and how deep is their involvement, for example does he/she have to do witness testing?

The precise scope of an ISA's task will depend on the standard they are working to or the detail of their contract. Guidance on what might be included can be found on the ISA Working Group's web site. In general however, the ISA should assess the safety product evidence so that he/she is sufficiently confident to make a clear statement that the safety requirements have or will be met. This clear statement may be an endorsement of the safety case or some other clear stamp of approval.

The severity of the hazard or the safety risk of the project determines the depth of the ISA role. For example the ISA may judge that witnessing the testing of a particular safety property with high risk or severe consequence is essential to establishing his/her confidence in the evidence. However, witnessing the testing would be only one part of the evidence that the ISA may examine in order to come to a judgement on the veracity of a particular test.

The ISA may expend analysis and assessment effort reviewing the test objectives, specification and test environment. The international standard IEC 61508 gives little guidance on the extent of ISA involvement but does make strong recommendations on the degree of independence and defining the scope of the assessment. The depth of assessment should be agreed with the customer and the ISA.

Q - What does Independence mean?

The definitions from IEC 61508 and other standards should be used. An ISA should be sufficiently independent that there is nothing that might affect or call into question their ability to carry out an impartial assessment or to make impartial judgements regarding safety.

Q- How do I contact an ISA?

Currently there is no central list of ISAs. A web search for the term 'ISA' will **not** be helpful! A web search for 'functional safety' provides a list of some potential companies **but** has some notable omissions. The professional institutions may also have lists of their members active in the field. The Safety Critical Systems Club has some relevant links. The BSI may be able to provide contact details of individuals/organisations active in standards work.

A further route is to contact procuring organisations for their recommendations. Further details will be added later.

Q - How do I become an ISA?

There is no single route to becoming an ISA. In general an ISA will be expected to have acquired expertise in at least one technology domain before building up competence in safety assessment. The IET/BCS competency guidelines provide a useful checklist of the experiences/training required.

Q - What competencies are required?

The ISA Working Group has published a Competence Framework for ISAs which can help an ISA or their customer determine what competencies are required for a specific ISA role.

This builds on the IET/BCS competence guidelines "Competence Criteria for Safety-related System Practitioners".

Also look at the 'Code of Practice for ISAs' produced by the working group.