



---

## **Effective Independent Safety Assessment**

Keith Harrison, Joanna Dawson



# Effective Independent Safety Assessment

Keith Harrison, Joanna Dawson

## Abstract

The purpose of an Independent Safety Auditor (ISA) is to audit, assess and review processes used in a project to show compliance to best and appropriate practice and to assess the adequacy of the evidence. The main objective of using an ISA in any project is to provide assurance that a contractor considers and addresses safety issues.

An ISA needs to be convinced that the process captures, understands and mitigates the hazards and identifies safety requirements associated with a system. This is carried out by a review of the safety analysis and support documents that leads to the development of the system Safety Case. In addition, it may be beneficial if the ISA conducts some independent analysis to add to the safety evidence or assist in the understanding of the system and its properties.

This paper describes the role of the ISA as used on a major UK MoD Procurement. It describes the use of independent analysis using creative thinking to develop a hazard model that provides understanding of the system level hazards and their association with the subsystems.

## 1 Introduction

As projects become more and more complex there is a need for additional assurance that a system is safe. Individual safety assessment of components in a complex system does not guarantee that when integrated the system will be of the highest integrity [2]. Although techniques for safety assessment have matured over the years, there is nothing better than bringing a fresh pair of eyes to the system [1]. Most UK systems and software standards including Defence Standard 00-55 [4] and 00-56 [3] mandate the use of an Independent Safety Auditor. The role has never been clearly defined in any of the standards, however, the recently published competency guidelines [5] set out to define core competencies for the role of an ISA. The 'A' in ISA could stand for

---

Further details can go here (this is a footnote attached to Abstract title, with custom mark of [space], and with this mark set as hidden in the footnote so no indent shows).

three different roles, although commonly known, as Auditor could be either an Advisor or Assessor. All these roles can assist in the safety of a system.

It is not the purpose of this paper to describe either the potential hazards associated with systems or to define a best practice approach to safety engineering processes. Instead, this paper identifies the activities performed by an ISA to provide assurance that a project not only considers but addresses safety issues.

## 2 How Safety Can Effect Projects

Systems are becoming more challenging to develop and implement, this is due to increasing complexity of design, integration of COTS / SOUP component. There is a need for more 'adaptable/flexible' products, more autonomous systems and for products to be integrated into super systems with data sharing e.g. C4I , UAV control and cars managed by computer. As these systems are becoming more complex and harder for any one person to understand the interactions between components there is a need for safety to be considered as an integral part of the system development process. Adding safety on at the end of the design process is too late.

Any new or modified system can be very complex such that understanding every component and how it interacts is a difficult task. These functional interactions require a rigorous safety analysis approach to identify, evaluate and mitigate them.

## 3 Typical Project Safety Concerns

There are many books and standards that define how to do safety, however, even if we identify best practice processes from these and implement them rigorously the product may not be safe. However, complete and correct our requirements identification, and safety analysis is, risks cannot be mitigated to an acceptable level if the system is not safe.

Risk cannot be ignored; in the UK we have legal contractual requirements through the Health and Safety act that requires all risks to be As Low As Reasonable Practicable (ALARP). Other standards may allow companies to accept a known level of risk, not iden-



tifying risk or not mitigating it due to contractual or financial reasons is likely to create liability.

Some typical problem areas within safety management are:

- Inaccurate or incomplete identification of hazards and requirements
- Inappropriate depth of analysis
- Incomplete safety argument
- Inadequate evidence supporting the argument
- Insufficient competency or experience of safety engineers

One way of reducing the occurrence of such problems is to have an independent assessment of these elements of the safety process. The ISA can play a major role in ensuring that these areas are not compromised on a project. In order to provide this level of assurance the ISA not only needs access to all the project material as it is produced but also to the design decisions that were made during the early stages of development.

#### 4 New Section

Any major procurement involves a number of stakeholders that have specific roles and responsibilities. A simplified view (Figure 1) of the key stakeholders for any UK based safety critical procurement is as follows:

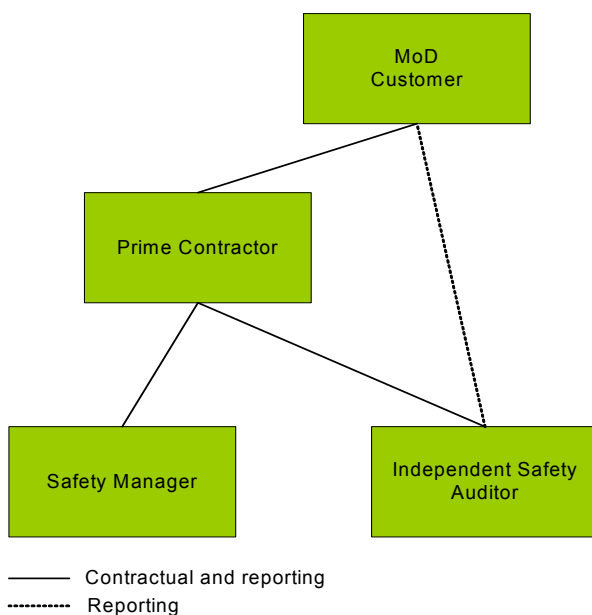


Figure 1 a simplified Project structure

- Customer
- Prime Contractor
- Safety Manager
- Independent Safety Auditor

The Customer is either the UK MoD or some other major company that has a need for the procurement. Their responsibility is simply to define and specify exactly what is required.

The Prime Contractor has the responsibility for designing, developing and producing that which the Customer wants. There is a direct contractual relationship between the Customer and the Prime Contractor. The Prime contractor may employ other contractors as can the Customer. However, the Prime Contractor has ultimate responsibility for the final product.

The Safety Manager has responsibility for the safety management process on the project and to ensure delivery of an acceptably safe product. This person would report to the Prime Contractor and may or may not work for them directly, i.e. as an employee or sub contractor. The Safety Manager needs to convince the Independent Safety Auditor that the product is safe.

The Independent Safety Auditor has the responsibility for ensuring that the safety activities and evidence on the project will enable delivery of a safe product. Whereas most other stakeholders have a responsibility to just one other stakeholder (assuming no complex multi-contractual structures), the ISA is always accountable to both the Customer and the Prime Contractor. Hence, either stakeholder could employ the ISA. In most cases the Prime Contractor would employ the ISA, since the role is part of the overall project. There are two prime conditions that have to be satisfied when using an ISA on a project:

- They are suitably qualified and experienced and acceptable to both stakeholders;
- They have a set of Terms of Reference (ToR) acceptable to both stakeholders.

The following qualifications and experience according to Defence Standard 00-56 [3] are expected of an ISA:



- A degree in an engineering or science subject related to the scope of application of the safety program;
- Chartered Engineer status in an engineering or science discipline related to the scope of application of the safety program;
- Formal training in safety engineering;
- Prior experience as an Independent Safety Auditor or safety engineer for a minimum of 5 years in areas related to the scope of application of the safety program;
- It is also desirable for the ISA to be familiar with the technologies used to implement the system relating to the safety program.

The ISA Terms of Reference, as described under ISA Charter, taken from the paper titled 'Independent Safety Auditing' [2] should contain as a minimum these main points:

- Deal fairly and objectively with all stakeholders;
- Jointly report to the Customer and Prime Contractor;
- Shall conduct the ISA tasks in conjunction with the appropriate quality assurance system;
- Audit objectively against legal and contractual regulations for safety;
- Should record accurately and in a timely manner;
- Plan to conduct ISA tasks to maintain smooth running of the project;
- Only give a judgment of safety issues;
- Only give advice on conformance to best practice.

## 5 Purpose of an ISA

The purpose of an ISA is to audit, assess or advise on processes used in a project to show compliance to best and appropriate practice and to assess the adequacy of the evidence that has been generated during application of those processes. The main objective of using an ISA in any project is to provide assurance that a contractor not only considers but also addresses safety issues. An ISA offers an independent view of the safety processes on a project based on experience and a thorough understanding of the relevant standards.

## 6 Role of an ISA

Part of the role of an ISA could be considered similar to a quality auditor, in the sense that they will be independent of the development process and purely there to review the activities ensuring they meet the project plan and that the standards are adhered to. The additional aspect of an ISA above a quality auditor is that the review of these activities has a safety focus to ensure that there are no compromises on the safety of the final system.

The main role of an ISA is to review, assess or inspect the safety evidence generated on a project, in particular the safety argument. Hence, the ISA needs to be convinced that the process captures, understands and mitigates the hazards and identifies safety requirements associated with a system. This is carried out by a review of the safety analysis and supporting documents that leads to the development of the system Safety Case.

Evidence can be in two forms:

- Direct evidence, such as, results of inspections, tests, demonstrations or analysis.
- Indirect or supporting evidence, such as, processes that created the direct evidence, competence of organization and staff.

The role of an ISA has three possible interpretations, two are most definitely related (Audit and Assessment) and the third (Advisor) is independent of the other two. For the purpose of this paper the role of Auditor will also include Assessor.

Therefore, the role of the Safety Auditor comprises of two main two main activities:

- Process review and auditing for compliance to standards and safety plan.
- Independent analysis in order to assess the implementation and results of project safety tasks.

In many cases a team as opposed to a single person performs the role of ISA. This allows the two activities to be split such that technical data and processes can be considered separately.

The Advisor role is very different to an Auditor in that rather than reviewing results of safety tasks and assessing processes, advice will be given on the methods for generating results and processes to be



used on a project. Once advice has been given to a project the Advisor cannot then take on the role of Auditor since the level of independence would be compromised.

Throughout the life of a project the Safety Auditor should be involved in all the safety related meetings and reviews to assess all the revisions of the safety documentation. The Safety Auditor must be a member of the project safety committee and report any findings to both client and contractor concurrently. Above all, the ISA must remain independent.

An ISA should be able to assess the safety activities free from conflicts of interest. Even if a client is paying for the ISA's services there should be a level of professional independence such that the ISA is not influenced by project time scale and funding. This is more easily achieved by using independent companies that have a reputation for giving sound and professional audits.

## 7 Benefits of an ISA

The ISA provides a level of independence and a different view as to what should be done on a safety program. This view or expectation can in the long term save the project valuable time and effort, i.e. if the safety program is running to the satisfaction of the ISA then the project completion will not be delayed.

As mentioned previously, companies are now starting to bring in external ISA's when there are no contractual or standard compliance requirements, this it to allow a fresh set of eyes to look at the problem and to establish if the project has not only considered but also addressed safety issues. This relies on the ISA being independent of the development. This provides a level of assurance / confidence and therefore can reduce the commercial risk if a hazard materializes.

In addition, it may be beneficial if the ISA conducts some independent analysis to add to the safety evidence or assist in the understanding of the system and its properties. The value of the independent analysis is not always appreciated in terms of its effect on the risk reduction process and may not be apparent to the project. However, it can be very effective in guiding the project safety activities.

If the ISA is involved from an early stage in the project and accepts the safety plan and the safety argument/strategy then any risk to the project is greatly reduced. This approach can also reduce the

cost and timescales of a project, as until the initial safety argument is defined and agreed, the project needs to assume that the entire system can cause the worst-case hazard associated with its use.

Therefore, getting an acceptable (to project, customer, ISA) safety argument and accident/hazard model defined and agreed by the relevant parties at a early stage of a project can significantly reduce the risk of either over or under engineering for safety.

## 8 Case Study of an ISA Involvement on a Project

The ISA role on a major UK procurement has led to some interesting activities that will assist in the safety assessment of the project. Praxis Critical System is contracted to a Prime Contractor to provide the role of Independent Safety Auditor.

The ISA role was split into two parts: The first of these was to perform audits, and the second was the undertaking of independent assessment.

### Audit

The audit role consisted of reviewing safety documentation, performing audits and being present at project safety meetings.

### Assess

The assessment role included the development of an Accident Model, Independent Safety Argument, Hazard Scenario list and the production of a Hazard Database all of which provide support in assessing the completeness and correctness of the project Safety Case.

Figure 2, 'ISA interface to project' shows how the activities performed during the assessment and audit relate to the project development of a Safety Case. As can be seen the main aim of assessment was to check for completeness and correctness at different levels of the Safety Case development.

On the project side of Figure 2, the low-level subsystem hazard analysis for all subsystems was being supplied to the prime contractor. This was reviewed and compared to the independent hazard analysis developed by the ISA. The system hazard log was compared with the ISA hazard scenario list and the System Safety Case was compared to the ISA generated safety argument. In comparing the system outputs with the ISA expectation a simple check was made for completeness and correctness. It was very



easy to see the holes in the safety analysis for the system.

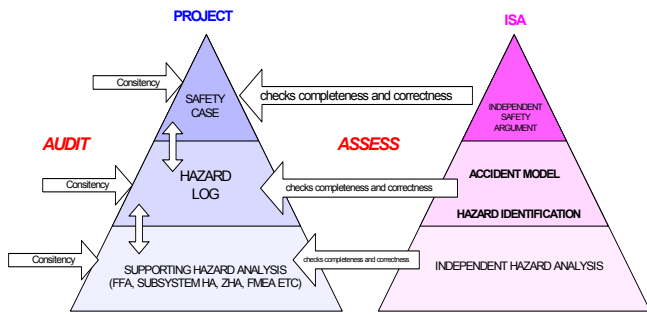


Figure 2 ISA interface to project

The first stage of the independent analysis was to construct an accident model for the entire system. This helped in understanding the system and to discover the possible hazards associated with the system.

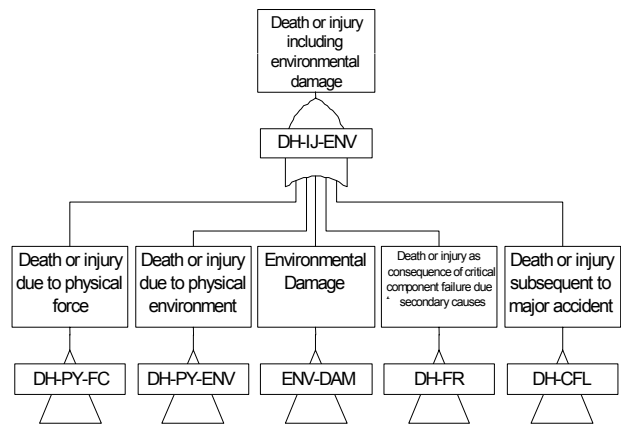
### Accident Model

The top level structure of the accident model Figure 3, is driven by the application of the immediate cause principle, i.e. each event needs to determine the immediate, necessary and sufficient causes for the occurrence of the event. These are not the basic causes of the event but the immediate causes or mechanisms for the event. [7] Throughout the development of the model, Praxis Critical Systems identified the next immediate, necessary and sufficient cause for the occurrence of the gate above.

The accident model (not completely published) identifies twenty accident scenarios; these are developed into hazard scenarios in the hazard scenario list in Table 1. The accident and hazard scenarios are not specific to the design of the System and therefore, are at an abstract level.

The top gate within the model is “Death or Injury including environmental damage” this has been broken down into five main causes as shown in Figure 3. The five causes of the top event, ‘Death or injury due to physical force’, ‘Death or injury due to physical environment’, ‘Environmental damage’, ‘Death or injury as a consequence of critical component failure due to secondary causes’ and ‘Death or injury subsequent to major accident’ captured all the other causes for the top level system failure. These are described in further detail after Figure 3.

Figure 3 Hazard accident model



- Death or injury due to physical force (DH-PY-FC). This branch of the tree considers hazards that could result from contact with system or non-system components, which can cause death or injury to operators, maintainers and third party individuals.
- Death or injury due to physical environment (DH-PY-ENV). This branch of the tree considers failures which can result in hazards to operators, maintainers and third party individuals, such as, hypoxia, disease and poisoning caused by the system.
- Environmental Damage (ENV-DAM). This branch of the tree analyses the potential causes of environmental damage throughout the system life-cycle.
- Death or injury as a consequence of critical component failure due to secondary causes (DH-FR). This identifies potential zonal hazards that could affect critical systems. As an example it includes uncontrolled fire and loss of all electrical power.
- Death or injury subsequent to major accident (DH-CFL). This branch of the tree scenarios such as, difficulty in exiting the air platform or ground platform following a major accident, loss of air platform emergency locator beacon etc.

### Independent Safety Argument

The independent safety argument was developed to determine the type of evidence that is required to



produce a Safety Case. This was done using Goal Structuring Notation (GSN) [6]. GSN is a diagrammatical way of presenting an argument by using a specific notation that describes goals and how to satisfy them. The purpose of this was to produce some sort of framework as a guide for the safety auditing. The Safety Argument identifies all the safety evidence that is required to produce a Safety Case.

### Hazard Scenario list

A hazard scenario list was compiled for the whole system showing high-level hazards and their contributing factors. This will be used to compare the system level hazard analysis with the independent ISA view to check for completeness. Table 1 shows the hazard scenarios that were identified through brainstorming and review.

<b><i>Death or injury due to striking system component</i></b>	
	Persons trapped by system component
	Persons striking system caused by excessive movement
	Persons injured by tripping/slipping due to system
<b><i>Death or injury due to contact with system component</i></b>	
	Exposure to toxic materials
	Exposure to excessive cold temperatures
	Incisions/Abrasions due to sharp/rough edges
	Component incorrectly configured for manual handling
	Exposure to excessive hot temperatures
<b><i>Death or injury due to poisoning</i></b>	
	Exposure to toxic materials
	Food contamination
	Excessive oxygen partial pressure
<b><i>Death or injury due to shock (psychogenic)</i></b>	
	Psychogenic shock caused by system environment
<b><i>Environmental damage due to system manufacturing</i></b>	
	Not developed at present
<b><i>Environmental damage due to system operation</i></b>	
	Not developed at present
<b><i>Environmental damage due to system decommissioning</i></b>	
	Not developed at present
<b><i>Unable to locate system in time to mitigate injuries</i></b>	
	Loss of emergency communications
<b><i>Unable to survive environment following accident</i></b>	
	Survival aids insufficient or fail to operate
<b><i>Unable to escape system following accident</i></b>	
	Unable to escape system
<b><i>Death or injury as a consequence of critical system</i></b>	

<b><i>damage due to excessive physical force</i></b>	
	Component becomes detached from system
	System experiences excessive physical force
<b><i>Death or injury as a consequence of insufficient energy to sustain system critical function</i></b>	
	Insufficient energy to sustain system critical function
<b><i>Death or injury due to being struck by a system component</i></b>	
	Loss of system structural integrity
	Component becomes detached from the system
	System experiences excessive physical force
	Extraneous operation of system component
	Hazardous operation of system releasable component
<b><i>Death or injury due to hypoxia</i></b>	
	Insufficient supply of oxygen
	Insufficient oxygen partial pressure
<b><i>Death or injury due to being hit by a projectile as a consequence of system action or inaction</i></b>	
	Transmitting incorrect or intercepted offensive info
	Transmitting incorrect or intercepted defensive info
	Incorrect deployment of defensive aids
	System incorrectly identified as hostile
<b><i>Death or injury due to hypothermia</i></b>	
	Exposure to environment below -X degrees
<b><i>Death or injury due to disease</i></b>	
	Exposure to excessive system radiation
	Exposure to excessive non-system radiation
	Physiological stressing
	Deep vein thrombosis
	Exposure to water borne pathogen
	Exposure to air borne pathogen
	Exposure to food borne pathogen
<b><i>Death or injury due to energy overdose</i></b>	
	Exposure to excessive electrical power
	Exposure to excessive noise
	Exposure to excessive microwave radiation
	Exposure to excessive laser radiation
	Exposure to excessive X-radiation
	Exposure to environment above +X degrees
<b><i>Death or injury due to unpredictable external conditions affecting system</i></b>	
	Not developed further
<b><i>Death or injury as a consequence of critical system damage due to excessive energy</i></b>	
	Critical system damage due to mechanical overload
	Critical system damage due to overheating
	Critical system damage due to fire
	Critical system damage due to EM interference
	Critical system damage due to excessive electrical power

Table 1, hazard scenario list



The final stage of the independent analysis phase was to develop an ISA hazard database to capture all the low-level subsystem hazards in their raw form, the system level hazards again in their raw form as generated from the low-level hazard and the ISA hazards from the hazard scenario lists. The database structure is shown in Figure 4.

### ISA Hazard Database

The hazard scenarios have been entered into the ISA Hazard Database, the database also contains the current applicability of each hazard scenario to each segment based in the system. The project documentation having been reviewed is then cross-referenced to all functional failures, subsystem and system level hazards to identify to which hazard scenarios they contribute. This provides the facility to identify the completeness and correctness of the system hazards and the traceability for subsystems.

This analysis will allow us to track the coverage of the system Safety Case, and to identify if there are any 'gaps' in the hazard analysis that have no corresponding hazard scenarios.

As previously explained, the ISA Hazard log can be used to compare various attributes of the project safety analysis and the ISA independent hazard analysis.

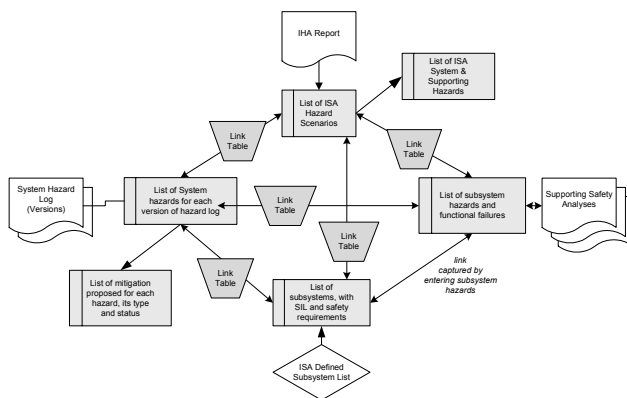


Figure 4 ISA Database Structure

- System hazards for each version of the hazard log (including mitigations);
- Functional failures for each Subsystem;
- An ISA defined subsystem list;
- The ISA Hazard scenarios (including the ISA low-level analysis).

The link tables are added to connect the ISA analysis with the actual analysis being performed at the subsystems and system level. The comparison of these links will show any gaps in the analysis at the system level. Although the ISA analysis is not complete it does give a second independent view of what the system and its components should look like. The database itself has the ability to generate various reports to compare the tables.

## 9 Summary and Conclusions

In the UK although there is a mandate for the use of an ISA, there are advantages that can be gained from effective use of the ISA roles. The two main roles, audit and assessment of an ISA can be used to significantly de-risk a project.

Early ISA involvement in the project through auditing can identify potential risk especially with complex systems. The ISA audit focuses on the safety aspects of a project rather than a generic quality audit. This ensures that there are no compromises in the safety requirements of the final system. However, the audit role is just one aspect of an ISA.

The use of independent assessment has proven very useful and assists in the audit role. Therefore an ISA should audit but also perform some independent assessment to add to the safety program and give a far better judgment on the safety activities. The independent assessment activity offers a greater opportunity to explore the program in far more detail than the audit. This can include the development of an independent safety argument, fault tree analyses and hazard assessment.

A project may also use an ISA (Advisor) to provide advice on the safety engineering process. This would be a separate role to Auditor/Assessor and may be of use to organisations not familiar with UK safety processes.

An ISA is essential to a project for a number of reasons:

- Provide an independent view of the safety activities;
- Ensure safety is considered properly;
- Makes recommendations on acceptance of the project system to the customer.



## Acknowledgements

The authors would like to thank Derek Fowler for his constructive comments on the paper and assistance in its completion.

## References

- 1 T. Cockram Where Inspections and Audits Fit Into the Safety Process and How Can We Have Confidence in their Effectiveness. 8th Safety Critical Systems Symposium: Southampton, UK, 2000.
- 2 C. Rees, V. Hamilton Independent Safety Auditing. 6th Safety Critical Systems Symposium: Birmingham, UK, 1998.
- 3 MOD, Def Stan 00-56/2, Safety Management Requirements for Defence Systems, 13th December 1996
- 4 MOD, Def Stan 00-55/2, Requirements for Safety Related Software in Defence Equipment, 1st August 1997
- 5 EE, Competency Guidelines for Safety-Related Systems Practitioners, 1999
- 6 T.P.Kelly, A Six-Step Method for the Development of Goal Structures, York Software Engineering, Flixborough, UK 1997
- 7 NUREG0492, Fault Tree Handbook, Jan 81