The Institution of Engineering and Technology

SaRS Safety and Reliability Society

bcs The Chartered Institute for IT

Institution of Mechanical Engineers

Guidance for Producing an **ISA Plan for Assessing a Safety Case**

www.**theiet.org**/factfiles/isa

Change History

Version	Date	Status
FINAL VERSION	June 2016	WEB

Please send suggestions for improvements, for consideration by the Working Group to:

isawg@theiet.org

Disclaimer

This document is owned and maintained by the IET/BCS/SaRs/IMechE ISA Working group and is not the property of the IET, the BCS, SaRs or the IMechE.

The information contained in this document should not be interpreted as representing the views of the IET, BCS, SaRs or IMechE. Nor should it be assumed that it reflects any current or future IET/BCS/SaRs/IMechE policy. The information cannot supersede any statutory or contractual requirements or liabilities and is offered without prejudice.

While the author, publisher and contributors believe that the information and guidance given in this work are correct, all parties must rely upon their own skill and judgement when making use of them. Neither the author nor the publishers assume any liability to anyone for any loss or damage caused by an error or omission in the work, whether such error or omission is the result of negligence or any other cause.

Where reference is made to legislation it is not considered as legal advice. Any and all such liability is disclaimed.

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)

Contents

1. Introduction

This document provides guidance to ISAs on the production of an ISA plan for the assessment of a safety case or equivalent[1]. Producing an ISA plan contributes to complying with:

- Requirement 10 'Management and Planning' of the Code of Practice for Independent Safety Assessors (ref 1). This states that “The ISA shall ensure that the ISA work programme is planned and managed so that it delivers the required outputs when needed and minimises disruption or delay to the client project or programme”.
- Requirement 11 of 'Guidance on the Procurement of Independent Safety Assessors' (ref 2). This states that “The procurement process and activities shall require that the ISA works in accordance with an agreed ISA plan produced by the ISA that minimises disruption or delay to the target project”.

The guidance:

- Applies whenever an ISA report needs to be produced, whether prior to or after contract award or authorisation to start work.
- May also be used by persons other than ISAs who are required to give a judgement on the adequacy of a safety case.
- May be used where the assessor is not required to be independent, simply by omitting material relating to independence.

An ISA assessment of a safety case involves forming judgements about the safety of a system on the basis of information provided in the safety case. ISAs may be called on to assess safety cases for a wide range of systems with widely varying safety significance. Safety cases range from large and complex to short and simple. Systems range from complex systems of systems to simple devices. The consequences of a safety-significant event may range from minor to catastrophic. This guidance aims to achieve a consistent approach applicable to all safety cases. It is therefore necessarily generic and high level. The guidance may be used as a basis for developing guidance that is sector, system or application specific.

The guidance is considered by the ISA Working Group to reflect good practice. It should be supplemented by regulatory requirements and industry-specific good practice where appropriate.

Footnote

1. For convenience, 'safety case' will be used here for anything which purports to argue that a system (or part thereof) is safe, irrespective of the structure, format or media utilised.

2. Scope

A safety case is intended to be a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment. The means by which this is done is reasoned argument supported by a body of evidence. ISA assessment aims to determine independently whether the safety case achieves its intent, the conclusions of the assessment being justified by argument and evidence. This guidance applies to the production of an ISA plan for:

- Assessing whether the safety case adequately demonstrates that the system which it is intended to address is safe.
- Justifying and documenting the conclusions of the ISA assessment.

The scope of this guidance is shown in Figure 1 in the context of all the ISA activities needed for assessment of a safety case. An ISA plan must necessarily be a plan for the 'Assess' and 'Report' activities. Note that this document does not provide guidance on how to plan either the production of a safety case or the generation of evidence of safety.

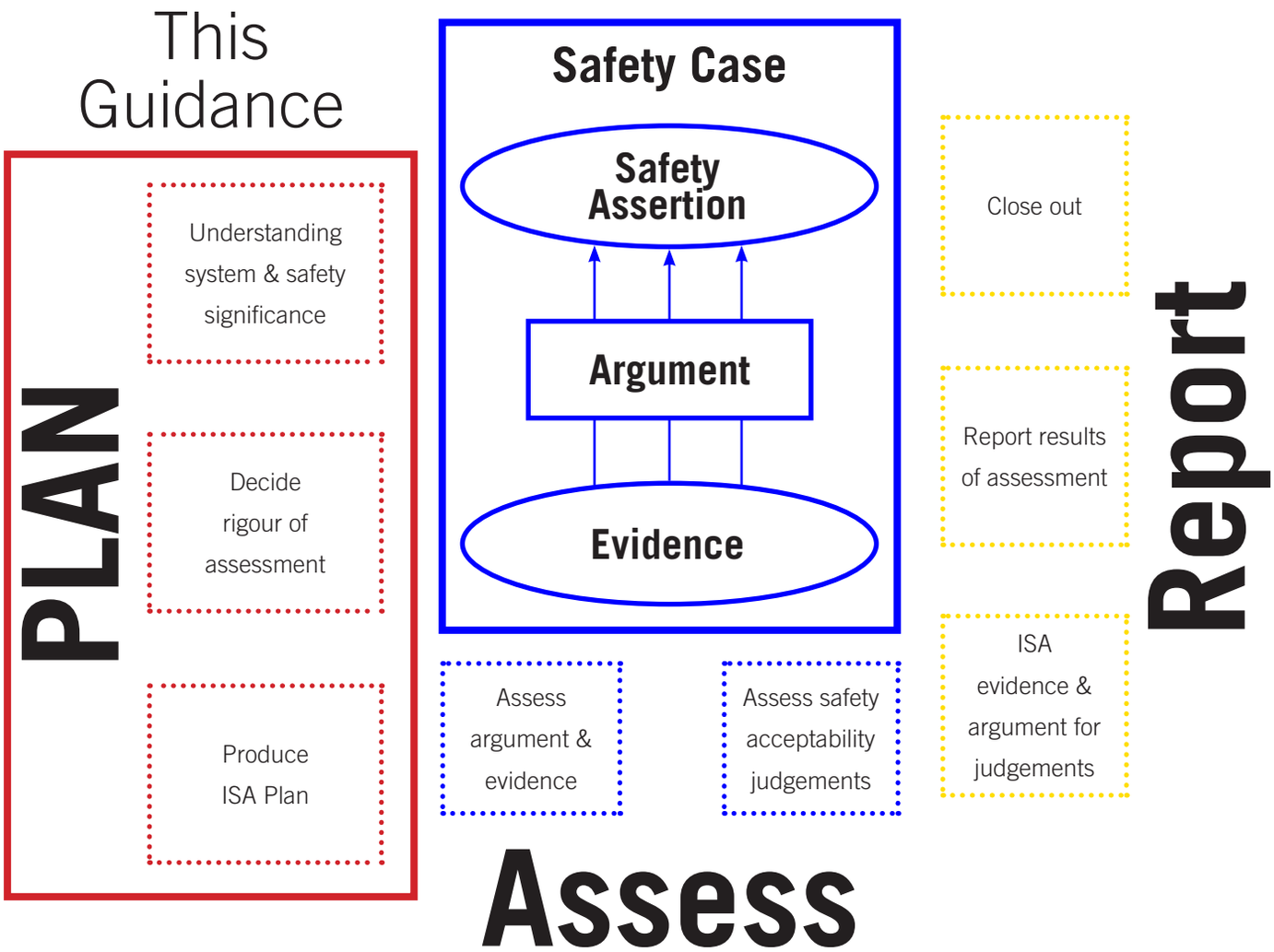

Figure 1: Scope of This Guidance Within ISA Assessment of a Safety Case

The guidance addresses producing an ISA plan only for assessment of a safety case. It does not address other possible ISA activities, for example ISA assessment of safety management, system development, verification and validation. ISA involvement during system design and development is desirable as information gained from such activities may inform the assessment of the safety case (e.g. by supporting or refuting claims made in the safety case). The ISA plan for such activities (which is out of scope here) should therefore take this into account, in particular to ensure that such activities will be of sufficient quality and rigour.

3. Planning an ISA Assessment of a Safety Case

An ISA plan is a specific instance of a project plan. Normal good practice for project planning therefore applies (e.g. defining project scope; resourcing; scheduling; availability of competent persons). This section supplements such good practice by focusing on issues specifically concerned with ISA assessment of a safety case.

The ISA Code of Practice (COP) includes five requirements that must be addressed when planning an ISA assessment of a safety case. They are:

- COP 3 'Competence'
- COP 4 'Communication'
- COP 5 'Proportionality'
- COP 8 'Priority of Safety'
- COP 10 'Management and Planning'

It is a prerequisite for planning that the person drawing up the plan (usually, but not necessarily, the lead assessor for the assessment) has sufficient understanding of the system, its application environment and safety implications that they are able to address the above requirements satisfactorily. If they do not have this understanding (as may be the case before drawing up an ISA plan), they must acquire it.

It is assumed that the person drawing up the plan is competent to draw up an ISA plan. This includes the ability to identify when they need to call on specialist assistance to cover areas where their domain knowledge and experience is weak. If they are not sufficiently competent, they should not produce the plan.

COP 3 'Competence'

An ISA is required to be “demonstrably competent to undertake the assessment activities, to make judgements regarding safety and to communicate effectively the results of their work” (ref 1, clause 3). The ISA plan must therefore:

- Establish that the ISA is fully and demonstrably competent to undertake the assessment activities, make judgements regarding safety and communicate effectively the result of their work for:
  - the system addressed in the safety case.
  - the application environment addressed in the safety case.
  - the safety arguments and evidence that would typically be used in a safety case for the system and application environment.
- Explain how any gaps in competence will be filled (e.g. by using specialist technical assessors).
  - Reasonably foreseeable gaps that might arise during the work (e.g. due to retirement or maternity leave) should be addressed.

Aspects of the system that need to be addressed when considering competence include:

- Technologies used for the system.
- Safety criticality or integrity (sometimes expressed in terms of safety integrity level (SIL), development application level (DAL) or equivalent).
- Complexity.

Aspects of the application environment that need to be addressed when considering competence include:

- Operational environment.
- Regulatory environment.
- Safety expectations and risk tolerability.

Aspects of the safety arguments and evidence that need to be addressed when considering competence include:

- Safety techniques and methods.
- Size and complexity.
- Potential hazards and accidents.
- Type and extent of interactions with the client that are needed for the assessment.

Further guidance on ISA competencies can be found in ref 3.

COP 4 'Communication'

Formal communication from the ISA regarding safety is required to be timely and documented. The ISA Plan must therefore address:

- The timing of key ISA outputs, particularly those which might affect the project work programme or timescales.
- How formal communication regarding safety is to be documented (e.g. use of e-mail to confirm points made in a telephone conversation).

In exceptional circumstance, it may be necessary for the ISA to escalate a safety concern to a level above that which they would normally deal with in the project. The ISA Plan should provide for such communication.

COP 5 'Proportionality'

Proportionality requires an ISA to apply a degree of rigour in their assessment that is in proportion to the safety risk addressed. This is to ensure that ISA effort, resources and methods used for assessment are sufficient for the ISA safety judgements that must be made while not being excessive. The greater the degree of rigour, the greater the chance that an error or deficiency in the safety case will be detected by the ISA, although the effort and expense needed for the assessment will also be greater.

The 'safety risk addressed' is a judgement that must be made before producing the ISA Plan. There are two components to the judgement:

1. The likelihood that the safety case will have errors or deficiencies that are significant for safety.
2. The maximum potential safety risk that the system may pose.

The safety risk to be addressed by the ISA's assessment becomes greater with increases in each of the components[2]. Factors that may influence each component are given in Appendix A. The greater the safety risk to be addressed by the ISA assessment, the more important it is for safety that any errors or deficiencies in the safety case are detected by the ISA assessment.

Degree of rigour is characterised by what will be examined during the ISA assessment and by what technique or method will be used (see Appendix B for more detail). The same degree of rigour need not be applied throughout a safety case. For example, suppose a system consists of two parts, one of which has the potential to cause many deaths while the other could at worst cause a few minor injuries. It would be appropriate to use a greater degree of rigour for assessing the first part and a lesser degree of rigour for the second part.

The ISA plan should plan for the use of methods and techniques that are appropriate for the required degree of rigour and should allocate sufficient time and resources. Note that at the planning stage, it will usually only be possible to establish degree of rigour of assessment in broad term unless the safety case already exists and has been examined by the ISA. That is because what is found in the safety case is likely to affect the degree of rigour that is appropriate for individual parts of the safety case. The ISA Plan should therefore make provision for reassessment and refinement of degree of rigour in the light of what is found when examining the safety case.

Footnote

[2] Note that the 'safety risk addressed' is not the risk from the system as claimed in the safety case. This distinction can be seen by considering a possible safety case for system X which concludes that the risk from X is very small. Suppose, however, the safety case contains major errors and the risk from X is actually very large. Using a low degree of rigour when assessing the safety case might easily result in missing the major errors that cause the risk from X to be grossly underestimated. This would be unacceptable. Thus, the 'safety risk addressed' cannot be simply the risk from the system as claimed in the safety case.

COP 8 'Priority of Safety'

An ISA is required to seek to ensure that safety is given due priority. Of particular importance for an ISA plan is that the ISA should encourage openness and a balanced view with respect to safety matters. Measures and activities that support this objective need to be included in the ISA plan.

Appropriate measures and activities may include:

- Discussion with the client before starting the assessment to ensure that the ISA understands the key points of the safety case from the client's viewpoint.
- Early, informal communication (e.g. verbal or e-mail) and discussion of potentially important safety concerns.
- Client to be given the opportunity to comment on (but not to veto or require changes to) ISA reports and other ISA documents before they are finalised.

COP 10 'Management and Planning'

A safety case may be made available for ISA assessment either as a single version or as one or more drafts plus a final version. The version to which the ISA assessment applies is the final (or, if appropriate, the only) version. This should be made clear in the ISA plan. If drafts prior to the final version are to be made available to the ISA, assessments of drafts may be carried out and should therefore be included in the ISA plan for the safety case assessment. However, they are to be regarded as informing the assessment of the final version rather than being part of that assessment. The ISA plan should make clear the relationship between assessments of drafts and assessment of the final version of the safety case.

The ISA work programme must be planned and managed so that it delivers the required outputs when needed and minimises disruption or delay to the client project or programme. This poses particular challenges for planning the ISA work programme because:

- There may be little time available for the assessment to be carried out.
- Negative findings from an ISA assessment may necessitate changes to the system or safety case when there is very little time to do it.
- Findings during an ISA assessment might necessitate changes to subsequent ISA work and thus revisions to the ISA Plan (e.g. because some evidence given in the safety case is found to be unexpectedly weak so other, complementary evidence must be assessed in much greater detail than originally envisaged).

In spite of this, the ISA must ensure that their assessment is always adequate, with safety as the top priority. The ISA work programme must therefore be planned so as to address, as far as is practicable, these two challenges. Addressing the challenges is likely to be straightforward if the safety case has already been produced and is not novel or complex. However, it may not be straightforward if either (a) the ISA is to be engaged before the production of the safety case and may have to assess drafts or incomplete versions of the safety case; and/or (b) the safety case is novel or complex so the assessment is subject to considerable initial uncertainty.

Measures that can be included in the ISA plan to address the above challenges include:

1. Noting critical dates for the client (e.g. submission of documents to their customer or regulator) in the ISA plan and planning the ISA work programme so that it does not compromise those dates.
   - Also encourage the client to include key dates from the ISA work programme in their project plan.
2. Interaction with the safety case developers to identify and warn of potential safety concerns as soon as possible.
   - Also encourage openness with respect to safety matters.
3. Firm dates for receipt of documents for ISA review, allowing adequate time for ISA review before the ISA output is needed by the client.
   - Need to ensure that the dates correspond to dates in the client's project plan.
4. Contingency for delays in the client's programme.
   - If possible, establish and be consistent with any contingencies the client has built into their work programme.
5. Allow for holidays and other foreseeable absences (both for client and ISA).

The optimum mix of measures for a particular ISA assessment necessarily depends on the nature and details of the what is to be assessed.

Irrespective of the measures included in the ISA plan, the ISA plan should:

1. Explain how the ISA work programme will be planned and managed so that it delivers the required outputs when needed and minimises disruption or delay to the client project or programme
2. Make it clear that timely and efficient conduct of the ISA assessment depends on timely access to documents that are to be provided by the client.
3. Identify specific dependencies on the client.
4. Identify ISA project risks due to these dependencies.
5. Identify mitigations for the assessment risks that are identified in the ISA plan.

4. References

1. Code of Practice for Independent Safety Assessors (ISAs), http://www.theiet.org/factfiles/isa/isa-code-page.cfm
2. Guidance on the Procurement of Independent Safety Assessors, http://www.theiet.org/factfiles/isa/guide-procure-isa-page.cfm
3. Competency Framework for Independent Safety Assessors (ISAs), http://www.theiet.org/factfiles/isa/comp-frame-page.cfm

Appendix A

Factors That May Influence Planned Degree Of Rigour Of Assessment

Factors that can affect the perceived (to the ISA) likelihood that the safety case will have errors or deficiencies that are significant for safety, include:

- What experience the system and safety case developers have with similar systems and safety contexts.
  - Little previous experience raises the possibility of errors due to unfamiliarity.
  - Much previous experience raises the possibility of errors due to complacency.
- System complexity.
  - Increasing complexity increases the possibility of errors of omission and incorrect understanding of system behaviour.
- Use of novel technology.
  - Novelty raises the possibility of errors due to poor or incomplete understanding of the technology.
- Safety case complexity.
  - Increasing complexity increases the possibilities of errors of omission and of incorrect safety argument.
- Safety Management System.
  - Weak safety management raises the possibility of errors and omissions being committed and not discovered and rectified.
- Legal and regulatory environment.
  - A strong and mature legal and regulatory regime decreases the possibility of inadequate attention being paid to safety with consequential errors and weaknesses.
- Size and complexity of the system development project.
  - The greater the size and complexity, the greater the possibility of errors due to misunderstanding and incorrect use of information.
- Use of previously developed items.
  - The greater the use of previously developed items, the greater the possibility that safety-related properties and behaviour of such items will not be adequately understood.
- Quality of previous safety cases from the same safety case developers.
  - A known history of weak safety cases suggests that a new safety case is also likely to be weak.

If the safety case has not yet been produced, client safety management organisation and practices and time and resource pressures on the development of the safety case may also exert influence.

Factors that can affect the perceived (to the ISA) maximum potential safety risk that the system may pose, include:

- Prior failures, incidents and accidents involving similar systems.
- Severity of possible accidents.
- Reliance on active (rather than passive) mitigations for hazards.
- Potential rates or probabilities of hazard causes.
- Outline safety argument or strategy.

Appendix B

Techniques, Methods and Degree of Rigour

Degree of rigour of assessment is characterised by what will be examined during the ISA assessment and the technique or method used for the assessment.

What will be examined

This has two dimensions: coverage and depth. 'Coverage' refers to how comprehensively all the strands of the safety argument will be addressed in the ISA assessment. 'Depth' refers to how far down an argument/evidence chain the assessment goes. In general, the greater the coverage and depth, the greater the degree of rigour of assessment. However, rigour must be focussed on where the perceived likelihood and consequence of error is greatest, otherwise the intended rigour of assessment will not be achieved.

Coverage can vary from full coverage to selective assessment of the most risk significant strands of the safety argument. For example, an assessment of hazard mitigations might be based on assessment of each mitigation or on a sample of hazards and/or mitigations. Full coverage will typically be appropriate for complex, novel or high risk systems and safety cases. Selective coverage (which might be random or focussed on, for example, highest consequence hazards) will typically be appropriate for systems that are low risk or are modest variants of established systems.

Depth can vary from assessment of top level argument and evidence through to comprehensive assessment down to a low and detailed level. For example, an assessment of an argument for the use of COTS hardware might regard reliance on reliability data from industry usage as adequate if the hardware is to be used in a benign environment. However, additional evidence of satisfactory performance of critical components in the specific application environment might be sought if the application environment is unusual or extreme (e.g. temperature, vibration or radiation). Note that planning should be based on the depth of argument and evidence likely to be needed to satisfy the ISA. If the safety case does actually not provide argument and evidence to this depth, then that is a weakness in the safety case and not, on its own, a reason for reducing the degree of rigour of assessment.

What technique or method

Different techniques and methods are appropriate for different areas of application. However, for each area of application, there is typically a range of techniques and methods with varying degrees of rigour (usually effectiveness and cost increases with rigour of method or technique). For example:

Area of Application	Less rigour		More rigour
Documentation	Credibility check		Structured read-through, multiple reviewers
Calculations	Plausibility assessment		Repeat calculations, diverse method, sensitivity assessment
Arguments	Credibility check		Completeness and correctness analysis
Validity of evidence	Plausibility check		Comparison with independent data for specific environments
Tests	Plausibility assessment of results		Assess applicability, coverage, method, conduct and results
Hazards completeness and correctness	Informal assessment		Structured completeness and correctness analysis
Hazard mitigations	Check presence and plausibility of mitigations for selected hazards		Analysis and critical assessment of argument and evidence for adequacy and correctness of mitigations for each hazard
Safety Management System	Informal walk-through		Process analysis including failure analysis
Derived requirements	Process check		Structured assessment of completeness, correctness and traceability