Document reference STG/181/1/9/1 Version 1.0 dated 1 June, 2004

Guidance for Integrated Project Teams for Use in Contracting for Independent Safety Auditor (ISA) Services

This guidance has been issued by the Safety Management Offices Group having been developed with assistance from Adelard

Contents

Figure

Table

1 Introduction

1) This document provides guidance for IPTs on contracting for Independent Safety Audit (ISA) services. It has been issued by the Safety Management Offices Group.

2) The document contains guidance on the ISA role, how to select ISAs, and the scopes of work for ISAs at different lifecycle phases.

3) The document is guidance for an IPT that can be used in part or additional work items can be added. Some or all of the activities may be appropriate depending on the system complexity and the information that the IPT may require in order to assure themselves of the validity of a safety argument.

2 Glossary

1) See Def Stan 00-56/3 for a complete set of relevant definitions.

ADRP	Airworthiness, Design Requirements and Procedures
ALARP	As Low As Reasonably Practicable. HSE's interpretation of the requirement in the Health and Safety at Work Act that risks are to be reduced "so far as is reasonably practicable".
BCS	British Computer Society
CASS	Conformity Assessment of Safety-related Systems
CLS	Contractor Logistic Support
COTS	Commercial off-the-shelf
DOSG	Defence Ordnance Safety Group
DRACAS	Data Recording and Corrective Action System
Duty Holder	The person responsible for safe operation of a system. Normally the IPT Leader.
EMS	Environmental Management System
FRACAS	Fault Recording and Corrective Action System
Hazops	Hazard and Operability Study
HCI	Human Computer Interface
IEE	Institute of Electrical Engineers
ISA	Independent Safety Auditor
LSSO	Land Systems Safety Office
Occupational safety	Safety associated with physical or inherent hazards, such as weight, sharp corners or electric shock.
OHHA	Occupational Health Hazard Analysis
OME	Ordnance, Munitions and Explosives

OSHA	Operating and Support Hazard Analysis
PFI	Private Finance Initiative
PHA	Preliminary Hazard Analysis
PHL	Preliminary Hazard Listing
Physical safety	Safety associated with inherent hazards of a system such as electric shock, radiation, weight, sharp corners, etc. Sometimes known as occupational safety.
PPP	Public Private Partnership
QMS	Quality Management System
Safe	Risk has been reduced to a level that is broadly acceptable, or tolerable and ALARP, and relevant prescriptive safety requirements have been met, for a system in a given application in a given operating environment.
Safety argument	A logically stated and rigorously demonstrated reason why the system is safe.
Safety Audit	A systematic and independent examination to determine whether safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose. See also Section 5.2.
Safety case	A structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment.
SEMS	Combined Safety and Environmental Management System
SMO	Safety Management Office
SMP	Safety Management Plan
SMS	Safety Management System
SOW	Statement of Work
SRD	System Requirements Document
SSMO	Ship Safety Management Office
URD	User Requirements Document

3 Bibliography

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

4 Basis for the ISA role

1) Any equipment contracts that will require ISA input on behalf of the MoD will include appropriate contract clauses and conditions. To enable the ISA role to be undertaken it is essential that the following clause is included: "The Contractor shall provide access to records, including sub-contractor records, for contract purposes, to enable the MoD appointed Independent Safety Auditor to carry out safety audits and other assessment activities to meet MoD safety requirements." It is strongly recommended that the advice of Commercial Officers is sought as appropriate.

2) Where an IPT contracts for the provision of ISA services any contract will require appropriate contract clauses and conditions to be included to take account of reporting requirements and dispute resolution procedures between the ISA, Duty Holder and the Contractor. The requirement for the ISA to sign documents produced by the contractor to indicate that they have been reviewed or endorsed by the ISA should also be considered.

4.1 MoD policy and practice

1) This section describes the basis for the ISA role in MoD policy and practice.

2) The MoD is a self-regulating organisation with regard to safety where it has been granted specific exemptions, disapplications or derogations from legislation, international treaties or protocols. This leads to a potential conflict of interest between the need to deliver new and enhanced capability to time and budget, and the obligation under the Health and Safety at Work Act and the Secretary of State's safety policy to reduce safety risks so far as is reasonably practicable.

3) The ISA role is founded on MoD safety policy that introduces independence into safety regulation by requiring or recommending the IPT (formally the "Duty Holder", normally the IPT Leader) to seek an ISA's opinion on the quality of the safety case for new or modified equipment. This independence is of benefit to both the IPT and the contractor and helps to achieve safety certification and compliance with legal requirements.

- In the maritime sector, JSP 430 requires an IPTL to authorise the safety case on the basis of an endorsement from an independent safety audit of the Safety Case. Before authorisation, the IPT must ensure the satisfactory resolution of any deficiencies or observations raised through their Safety Committee and ISA.

- In the land sector, JSP 454 currently states, "As part of the IPT's assurance arrangements, it is strongly recommended that an Independent Safety Auditor be appointed by the IPTL at the outset of the project in consultation with the safety committee, to undertake the following tasks of: providing independent assessment and validation of Safety Case work; providing professional support and advice to the safety committee and IPTL."

- In the airworthiness sector, JSP 553 currently states, "The appointment of an ISA is required by Def Stan 00-56 for systems in the higher risk classes and is desirable in other cases if the aircraft, its systems or equipment are novel, complex or high risk. The ISA can also provide general safety advice to the IPT, the industrial Designer and other organisations."

- In the ordnance sector, JSP 520 provides for independence through the review by DOSG and through the OME Safety Advisor assigned to the IPT to provide advice and support. However, overall system safety will normally be covered by JSP 430, JSP 454 or JSP 553 and an ISA will be needed as described above. Also, JSP 520 does provide for other independent technical experts on the OME Safety Review Panel, and the ISA can usefully provide independent audit and advice in areas such as occupational safety.

4) The ISA has no executive authority and the IPT accepts full responsibility for safety. The IPT may overrule an ISA's recommendations but in such cases a robust justification for the decision should be recorded.

5) The ISA role has two other aspects that flow from the need to form an expert, professional opinion:

- The ISA plays an important part in advising the contractor and the IPT on a framework of appropriate standards and good practice. This is of increasing importance in the light of the current trend in defence and civil sectors to "goal-based", as opposed to prescriptive, regulation. A goal-based approach has the advantage that it makes innovation easier, but it does not provide the same degree of certainty as prescriptive regulation. Safety advice is described in more detail in Section 5.3 below.

- According to the SMO's policy, the ISA may assist the SMO to discharge its responsibilities for monitoring effective safety and environmental management by contractors and IPTs, and for the provision of advice and guidance on safety management. The organisational interface with the SMOs is elaborated in Section 6.4 below.

4.2 ISA scopes of work

1) Typically the ISA caries out document reviews, audits against planned arrangements, and additional analyses. The functions carried out by the ISA are elaborated in Section 5 and the detailed scopes of work in Section 9.

2) In developing the scopes of work, the IPT should bear in mind the following.

3) The IPT shall arrange to preserve the ISA's independence and enable them to carry out their duties effectively. An authorised ISA has the right and duty to raise significant concerns directly with the IPT or contractor, even when outside their agreed scope of work or TOR and should raise unresolved concerns with appropriate Authorities and the relevant SMO.

4) The ISA should be given reasonable resources to carry out the tasks. The cost of employing an ISA should be commensurate with the risk associated with the project. A lack of resources is a poor justification for placing limits on the scope of ISA work or level of involvement of the ISA. Experience shows the costs of correcting a deficiency attributed to inadequate Safety Audit significantly outweigh any savings made.

5) It is possible that the ISA and the contractor will become deadlocked over some aspect of the safety argument, and the IPT will wish to seek another opinion. The relevant SMO may be able to provide informal assistance and advice on the way forward (although the IPT remains

responsible for deciding the way ahead). Also, if the ISA has significant concerns that they do not believe are being adequately addressed, the relevant SMO may be approached for assistance. In these cases the SMO might be asked to co-operate in a process similar to the following:

a. The ISA and the party (IPT or contractor) with whom they disagree should each produce a report setting out their position of the disputed area of the safety argument. These reports should be exchanged and also copied to the SMO. The SMO should also be provided with other relevant documents, such as the safety management plan and appropriate elements of the safety case.

b. Having read each other's reports, the ISA and the other party should write an agreed joint report setting out the precise areas of agreement and disagreement. This should be sent to the SMO.

c. The IPT should arrange an arbitration hearing. Generally this will take a half-day but might be longer for a complex dispute. The hearing should be chaired by a member of the SMO. The ISA and the other party should each present their point of view, which may be followed by a general discussion of the issues.

d. Following the hearing, the ISA and the other party should each write a final submission, which should be exchanged and also sent to the SMO.

e. The SMO will consider the reports and points raised at the hearing, and provide written advice with respect to the issues outstanding.

5 Definitions

1) Def Stan 00-56/3 defines *Independent Safety Auditor* as an individual or team, from an independent organisation, that undertakes audits and other assessment activities to provide assurance that safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.

2) This section of the guide expands on this definition by considering the meaning of *independent*, *safety audit* and *safety advice*. Each definition is followed by an interpretation covering any areas of difficulty, and one or more illustrations of the application of the definition.

5.1 Independent

5.1.1 Definition

1) Able to provide an expert, professional opinion without vulnerability to commercial, project or other pressure.

5.1.2 Interpretation

1) Informally, the ISA needs to be sufficiently independent that they are sheltered as far as practicable from pressure to modify their opinion.

2) It is highly desirable for the ISA to be from an organisation totally separate from the contractor. Where it is not possible to achieve total separation, the IPT should justify the acceptability of the arrangements that they authorise. Arrangements that may give sufficient independence include the use of companies in the same group as the contractor, but otherwise independent, or organisations or departments in the contractor's firm that are independent to board level.

3) Contractors may raise commercial or security objections to other companies having access to their proprietary information. These can normally be overcome by selecting the ISA from an organisation that does not compete with the contractor, and putting a non-disclosure agreement in place. Even in very specialised areas, it does not follow that anyone competent to carry out a Safety Audit must be a competitor, since competent personnel are likely to be available who have retired from or left the contractor or a competitor, or who have worked in the same area for MoD. Also, most of the skills that an ISA should have are generic, and the expertise required often does not need to be so domain or technology specific to require a (current or former) competitor.

4) Some contractors may have an in-house safety organisation. Although these organisations may be able to provide scrutiny of the contractor's organisation, they will often be unable to provide scrutiny of the activities of the IPT or other parties. In addition, they are highly unlikely to be involved pre-contract due to their lack of commercial independence from the organisations tendering for work. However, in-house organisations may be able to support the work of the ISA, which may lead to a reduced need for Safety Audits. This also applies to safety auditing carried out in-house, or more general auditing to assess conformance with standards such as ISO 9001.

5) The ISA may give general advice to the IPT and the contractor, but will compromise their independence if they contribute to the specific safety case: see also Section 5.3.

6) In order not to undermine the ISA's independent opinion, the IPT should give the ISA substantial freedom to conduct the Safety Audit as they judge to be appropriate.

7) The need for independence does not mean that every project in an IPT and every subcontractor has to have a separate ISA; reference to the requirements of domain specific JSPs should be made however. A single or small number of ISAs will give a more consistent approach and will acquire domain-specific knowledge more quickly. Of course the ISA or ISAs should be independent with respect to all the organisations that they audit, as defined above.

5.1.3 Illustrations

- *A major defence contractor asserts that a MoD-appointed ISA is unnecessary because it has an in-house safety section with specialist domain knowledge.* An ISA should still be appointed, but their terms of reference should include co-operation with the safety section to reduce duplication of effort and "audit fatigue", and also the making of judgements about the work of the in-house organisation. The ISA should be competent in the domain (see Section 8) although they may not have the same level of depth of specialist knowledge as the in-house safety section.

- *A contractor resists appointment of an ISA from a competitor because it is not prepared to make proprietary information available.* This is a legitimate concern. 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 IPT 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. See also Section 4.

5.2 Safety Audit

5.2.1 Definition

1) Safety Audit is defined in Def Stan 00-56/3 as a systematic and independent examination to determine whether safety activities comply with planned arrangements, are implemented effectively and are suitable to achieve objectives; and whether related outputs are correct, valid and fit for purpose.

5.2.2 Interpretation

1) Safety Audit consists of the activities that enable an expert, professional, independent opinion to be reached on the safety of the system.

2) The safety case is based on a safety argument. Appendix A shows typical safety arguments through the procurement lifecycle. Typically the overall, top-level argument is that:

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 MoD organisations.

The assumptions and prerequisites on which the safety case depends are valid.

3) Safety Audit involves examining each of the components of this safety argument and forming an opinion as to whether it is complete and correct. Safety Audit is targeted at both the contractor and the IPT. Typically, the ISA will form their opinion on the basis of the following:

- Targeted document reviews.
- Independent assessment and analysis. The ISA may utilise techniques such as diverse analysis, witnessing, interviewing, traceability checks, vertical slices[1] and inspection.
- Audits of safety and development processes. These "traditional" audits check for conformance to relevant policy, standards, the SMS or where appropriate the combined SEMS, and the safety management plans.

4) Note that Safety Audit consists of considerably more than "traditional" auditing, and in fact such auditing makes up a fairly small proportion of the ISA's activities. More detailed scopes of work are given in Section 9 below.

5) Note that within the airworthiness sector, the assessment function and the audit and advice function are often carried out by different individuals or organisations.

5.2.3 Illustrations

- *An ISA Report consists of a detailed audit showing compliance to the requirements of Def Stan 00-56.* This is not sufficient to provide an expert, professional opinion to the IPT. Underlying the ISA role is the fact that safety is fundamentally a property of the system, not the process used to develop it. An audit showing simple compliance (i.e. that a process has been carried out) is insufficient and a judgement of the effectiveness of the process, and how it affects the safety of the system, is also required.
- *A contractor refuses 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. If agreement cannot be reached, the IPT should intervene to obtain the data.

[1] Vertical slice analysis traces the mitigation of a hazard throughout the system lifecycle.

5.3 Safety advice

5.3.1 Definition

1) General advice on the acceptability of a proposed safety argument, which facilitates the IPT's or contractor's decision-making.

5.3.2 Interpretation

1) In order to maintain their independence, the ISA cannot give specific advice or contribute directly to the safety argument. However, it is legitimate, and helpful in reducing project risk from safety matters, for the ISA to give general advice that leads to timely production of a satisfactory safety case. General advice is that which would be given to any broadly similar project, and corresponds to the assessment guides produced by the statutory regulators (e.g. the HSE's Approved Codes of Practice and the series of Assessment Guides from the Nuclear Installations Inspectorate). General advice may cover the selection of suitable analysis techniques, the structure of safety arguments and the making of tolerability claims.

2) It is also legitimate for the ISA to provide advice on specific technology, and the consequences of technology choices, providing that the advice is that which would be given in any broadly similar case.

5.3.3 Illustrations

- *The ISA has criticised the contractor's calculation of numerical tolerability criteria, and the contractor asks the ISA to change it to a form that they would find acceptable.* 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 calculation should be performed, by analogy with other, similar projects. It is also legitimate for them to help to derive policy and guidance on safety arguments for classes of systems in association with the SMOs (see also Section 6.4).

- *A cluster IPT is responsible for several interconnected systems, and asks the ISA for one system to write a safety case for another.* This is permissible provided that the scope of the two safety cases is clearly defined and does not overlap. The IPT should engage a second ISA to provide an independent opinion on the safety case for the other system.

- *In accordance with JSP 454, a small IPT asks the ISA to advise and assist in the establishment and development of the Safety Management System and Safety Case, in lieu of a dedicated Safety Officer.* This is permissible provided that the advice and assistance is general and facilitates the IPT's own development of the SMS and Safety Case, rather than influencing their development directly.

6 Relationships with other organisations

1) This section describes the organisational interfaces between the ISA and other organisations concerned with defence safety. The typical interfaces are illustrated in Figure 1 and discussed below. Not all the information flows shown apply to all sectors (for example, only the LSSO currently offers an arbitration service). The ISA tasks related to these interfaces are expanded in Section 9 below.

2) The formal communication route between the ISA and the contractor and the Operating Authority will be defined in the MoD/ISA contract, and will normally be through the IPT as shown. In practice, however, it is usual for the ISA to communicate directly with these bodies, although the IPT should be kept informed of all discussions and given copies of all written communications.

3) JSPs 430, 454 and 553 include the ISA in the membership of relevant safety committees in accordance with Def Stan 00-56/3, and all the organisations shown in the figure will be represented on one or other of these. The meetings of these bodies provide an important means of liaison between the ISA and the other safety organisations.

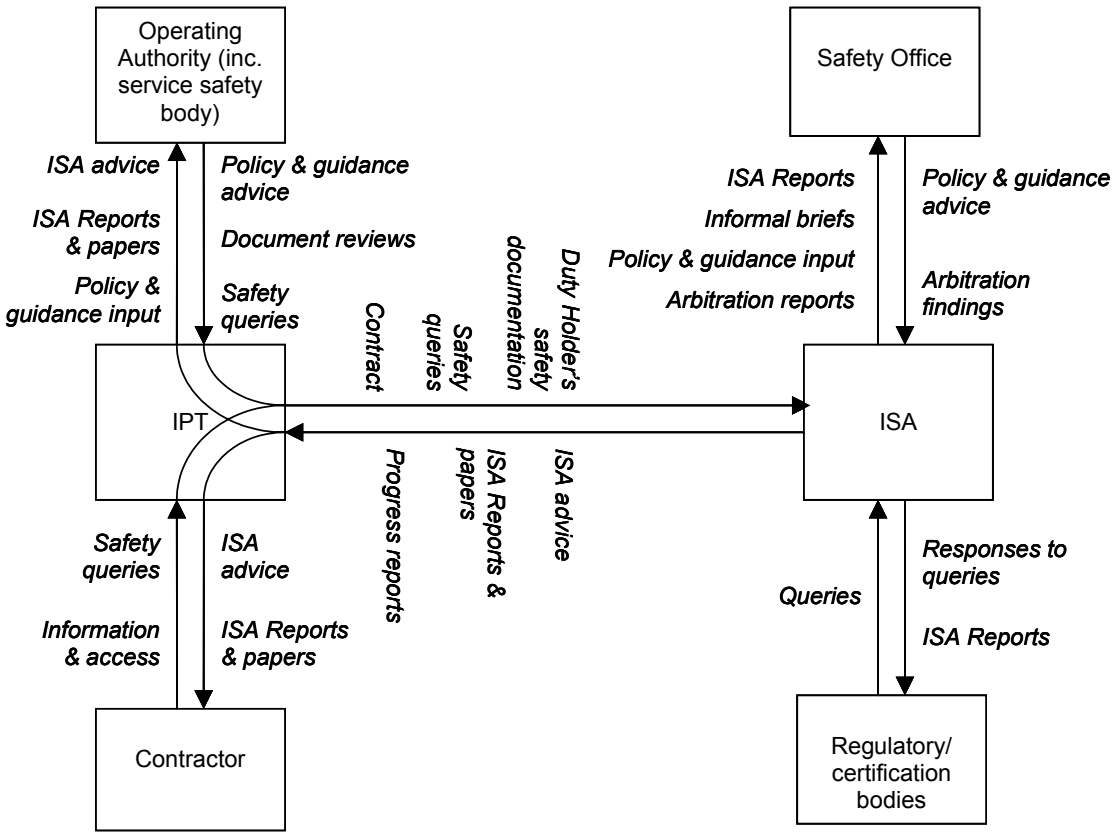


Figure 1: Typical ISA organisational interfaces

6.1 The IPT

1) Where the IPT directly contracts the ISA, they must respect their independence. 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 IPT or contractor, even when outside their agreed scopes of work or terms of reference, and should raise unresolved concerns with the appropriate Authorities and SMO.

2) In the majority of cases, the IPT contracts the ISA on the project. However, the IPT may direct the contractor to contract the ISA instead. In that case the contractor should employ an ISA who is acceptable to the IPT in terms of competence and scope of work as defined in this guide.

3) The ISA interacts with the IPT as follows:

- *Contractually*. The ISA contracted by the IPT has to provide value for money and an IPT should monitor ISA performance against the contract accordingly. Selection criteria for ISAs are given in Section 7 below.

- *Through audits.* The ISA audits the IPT's safety management system and safety records since this forms part of the overall safety argument (see Section 5.2).

- *Through the ISA Report.* The ISA Reports (and supporting review, analysis and audit records) provide the IPT with the independent opinion that they require under MoD safety policy. This covers safety documents and analysis produced by both the contractor and the IPT (e.g. as part of requirements definition prior to tendering for the system).

- *By providing advice.* The ISA may provide independent, general advice on safety matters to the IPT (see Section 5.3).

4) The role of the ISA is basically the same for both single-project and cluster IPTs. Experience shows that ISA work for cluster IPTs is project-based and so there is little difference in practice. It is permissible for ISA personnel to give specific advice for some projects while carrying out independent safety audit in others; see Section 5.2 and Section 5.3.

6.2 The contractor

1) Where the ISA is contracted by the contractor, the interface will include contractual matters.

2) The contractor's relationship with the ISA is set out in Def Stan 00-56. Where the ISA is contracted by the IPT, the ISA should be acceptable to the contractor in terms of competence and scopes of work. They should also be able to safeguard the contractor's IPR and confidential information (see Section 5.1.2).

3) The contractor receives from the ISA:

- *Reports*, including the ISA Report, on reviews, audits and analyses carried out by the ISA as part of the Safety Audit function (see Section 5.2).

- *General advice* on safety matters (see Section 5.3).

4) The ISA receives from the contractor:

- *Access* to the information needed to form an independent opinion, including safety case reports.

- *The contractor's response* to ISA reviews and reports. (See also Section 4 para 1.)

6.3 The Operating Authority

1) There may be discussions between the Operating Authority and the ISA over safety issues. Typically communication originates in safety committees, but may also occur if the Operating Authority raises a safety concern directly to the IPT.

2) In addition, the Operating Authority may have its own safety body, which may liaise with the ISA as follows. The Operating Authority's safety body receives from the ISA:

- *Reports*, including the ISA Report, on reviews, audits and analyses carried out by the ISA as part of the Safety Audit function (see Section 5.2).

- *Assistance* over safety issues, if requested.

3) The ISA receives from the Operating Authority's safety body:

- *Document reviews*.

- *Requests for assistance* on safety issues.

4) In the air sector, the ISA's organisational interface is with the Release to Service Authority rather than the Operating Authority.

6.4 Safety Management Offices

1) The ISA interacts with the relevant SMO in several ways:

- *Through the ISA report*. Some SMOs may require copies of formal ISA Reports. The ISA Reports show that the IPT has received an independent opinion on the quality of the safety case. The reports should also address compliance to safety and environmental management policy, both by the contractor and the IPT.

- *By receiving advice.* The relevant SMO may be able to provide advice on difficult safety issues and areas of policy uncertainty.

- *Over the development of policy and generic advice.* The ISA may encounter safety issues that are not covered by existing policy or guidance. Examples include the development of safety targets for novel situations. They should liaise with the relevant SMO over such issues and if requested assist the SMO in the formation of

relevant policy and guidance. They should also copy the SMO any advice they give to the IPT concerning such issues.

- *Through the need for arbitration.* It is possible that the ISA and the IPT or the contractor will become deadlocked over some aspect of the safety argument. In the Land sector, the LSSO already offers to provide informal arbitration and advice on the way forward. The ISA (together with the IPT or contractor) should provide a report on the areas of agreement and disagreement, on which the SMO can base its advice.

- *Through informal communication.* Especially in complex projects, it is helpful if the ISA informally briefs the relevant SMO from time to time on project safety progress and any areas of difficulty or disagreement.

6.5 Regulatory/certification bodies

1) 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. An example is the Naval Authority or the Naval Nuclear Regulatory Panel in the maritime domain.

6.6 Design Authority

1) Generally, the Design Authority will be either the contractor or the IPT. However the Design Authority may be another organisation. (This case is not shown on the diagram.) In this case, the IPT will need to obtain agreement from the Design Authority to provide access for the ISA and generally to co-operate with them.

2) The Design Authority receives from the ISA:

- *Reports*, including the ISA Report, on reviews, audits and analyses carried out by the ISA as part of the Safety Audit function covering the contractor and the Design Authority (see Section 5.2).

- *General advice* on safety matters (see Section 5.3).

3) The ISA receives from the Design Authority:

- *Access* to the information needed to form an independent opinion, including safety case reports. (See also Section 4 para 1.)

- *The Design Authority's response* to ISA reviews and reports.

7 Selection of ISAs

1) This section considers the criteria that the IPT should apply when choosing an ISA or ISA team. The criteria cover personal (or team) attributes of independence (Section 7.1) and competence (Section 7.2), and project attributes of complexity (Section 7.3), risk (Section 7.4) and lifecycle phase (Section 7.5). Expertise and competence is discussed further in Section 8.

2) It is preferable to employ an ISA team for most projects. The team enables effective peer review of the assessment's outputs and can provide specialist expertise in areas such as human factors and software reliability modelling. It also has the practical advantage that it is easier to cover for normal staff absence and attend concurrent meetings. The guidance for the project criteria explains the circumstances when an individual may be sufficient.

3) Even when an ISA team is employed, the ISA team leader and preferably all the team members should be individually identified.

7.1 Independence

1) The ISA should be independent as defined in Section 5.1.

7.2 Competence

1) The ISA should be competent in Safety Audit skills in the project domain, including knowledge of the safety policy for the domain. This is discussed in detail in Section 8.

7.3 Project complexity

1) Project complexity can take several forms, including:

- *technical complexity*. In this case the safety argument is likely to be complex, with several types of evidence for many of the safety claims, especially in the area of safety of data and commands. Appendix A illustrates the main elements of a complex safety argument. The ISA should have a higher level of competence including proven technical skills applying to any technically difficult safety issues (see also Section 8.1.1).

- *problems with safety evidence*. The Safety Audit will require more effort if there are problems with the safety evidence, such as a lack of historical evidence for safety of legacy equipment, or if the historical evidence shows that the system does not meet its safety requirements.

- *large project scale*. For large-scale projects involving "systems-of-systems", the safety argument will involve evidence provided by safety cases for systems hierarchies aggregating up to macro platform or super-system level. The ISA should have proven experience in Safety Audit of interrelated safety cases and the safety issues that arise due to the interactions between systems, including interfacing to ISAs for other equipment.

Conversely, for small-scale projects, where the amount of concurrent work and number of meetings is reduced, it may be sufficient to employ a competent individual as ISA, rather than a team.

- *PFI or foreign acquisition.* In this case, the ISA needs to be able to interpret the safety standards that have been applied to the development of the system in the light of MoD policy and UK regulatory requirements.

7.4 Safety risk

1) One of the roles of the ISA is to reduce uncertainty in the validity of the safety argument by providing an authoritative second opinion. For low risk systems, the safety argument will be simpler, quicker and easier to assess, and because of the amount of mitigation, the likelihood of fielding an unsafe system is low. Therefore for systems where the risk is low compared to the day to day risks an individual faces, the IPT could consider:

- the use of an individual ISA rather than an ISA team
- less specific experience as an ISA or in the application domain

7.5 Lifecycle phase

1) The major safety effort is typically during the assessment, demonstration and manufacture acquisition phases. During the other phases less safety work is likely to be needed, and hence the ISA team can be reduced in size.

2) If the equipment is near the end of its service life, a much simpler safety argument is likely to be appropriate, centring on maintaining the current level of safety, and on issues of disposal. Safety criteria will be informed by the relatively short “time at risk”, and design changes, if any, are likely to be of low risk. In this case, a limited Safety Audit by an individual is likely to be sufficient.

3) Detailed scopes of work for each lifecycle phase are given in Section 9.

8 Expertise and competence

1) It is obviously of the utmost importance that the ISA should be suitably qualified and experienced. This section describes competence criteria for ISAs, and presents guidance on assessment against the criteria. Where the Safety Audit is carried out by a team, the team as a whole should provide the necessary level of competence.

8.1 Competence criteria

1) There are three types of competence required to assess the suitability of an ISA:

- *technical competence*—safety and technical knowledge (of the application area and technology) required to support the activities of a Safety Audit (this is described in Section 8.1.1)
- *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, as defined in Section 5.2 above (this is described in Section 8.1.2)
- *behavioural competence*—qualities and attributes of behaviour and character needed to successfully perform the task (this is described in Section 8.1.3)

8.1.1 Technical competence

1) Technical competence covers the knowledge and experience needed to underpin the activities of the ISA. This has two aspects:

- Technical competence in Safety Audit independent of the specific application domain and technology used.
- Technical competence in the application domain, where an understanding of the specific technologies used and the context of their use extends the ability to successfully audit the safety of the system.

2) Technical competence in Safety Audit includes:

- Knowledge and experience of the legal and safety regulatory framework.
- Understanding of the principles and concepts of safety management, e.g. ALARP, hazards, risk and safety requirements.
- Knowledge and experience of techniques and methods to determine and analyse safety issues of importance and to make a judgement on the safety of a system. Examples of such knowledge include safety analysis techniques such as Hazops and Fault Tree Analysis, and the ability to estimate the necessary resources to perform such analyses and to judge the scope and depth of analyses carried out.

- Knowledge and experience of specific standards, guidelines or codes of practice relevant for the project, e.g. Def Stan 00-56 and the applicable safety management JSPs.

3) Technical competence in the application domain includes:

- Safety engineering knowledge and experience appropriate to the application area and technology, including safety practices appropriate to the organisation and application area.

- 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 including human factors integration, integrated logistic support and availability, reliability and maintainability would also be advantageous.

4) In the ship sector, demonstration of technical competence requires that all key members of the ISA's team should possess or be working toward an SSMO training certificate.

8.1.2 Auditing competence

1) As discussed in Section 8.1.1, technical competence underpins the knowledge needed to carry out a Safety Audit, independently of the specific activities being performed. By contrast, auditing competence considers the specific activities performed as part of a Safety Audit (that is, document review, process audits and independent analyses). This includes the ability to:

- determine the scope and objectives of the Safety Audit

- develop and maintain a plan for the activities that comprise a Safety Audit

- collect and analyse objective evidence to support a judgement about the safety of the system. This may include: a) interviewing personnel at all levels; b) examining and reviewing documents; c) observing activities

- verify the accuracy of information gathered in interviews by observation, measurements and records analyses

- identify, record and investigate clues suggesting possible problems

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

- make a judgement on the safety of a system

- document findings including producing formal ISA Reports

- verify that any actions necessary to address the results of the Safety Audit activities are appropriately completed

8.1.3 Behavioural competence

1) Behavioural competence describes the attributes of conduct and character needed 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

8.2 Assessment of competence

1) The assessment of competence of ISAs should be in terms of the criteria described in Section 8.1. Where a project requires a team approach, it is the balance of skills that is important, and the team leader should demonstrate the ability properly to manage and co-ordinate the team. Individual team members should provide the in-depth knowledge that is required.

2) The IPT should ask potential ISAs for evidence of competence, supported by verifiable examples, as part of their proposal when bidding for an ISA role. Typically, evidence to demonstrate the competencies is based on training, qualifications and experience. Proven ability is likely to provide the best indicator; and appropriate references to that effect should be obtained wherever possible.

3) Potential ISAs may present evidence of competence 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 IPT 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 [1] or the Network Rail ISA Accreditation Scheme. The IPT 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) scheme, and there are very few registrants under the scheme.

9 Scopes of work

1) This section sets out scopes of work for ISA services. The Safety Audit aspect of the ISA role is defined in Section 5.2 and the generic Safety Advice aspect is defined in Section 5.3. The organisational interfaces with other organisation are described in Section 6.

2) The ISA produces a number of documents during the course of the Safety Audit, and these are listed in Section 9.1.

3) Detailed scopes of work covering the CADMID lifecycle phases are tabulated in Section 9.2. The scopes of work cover both safety and environmental protection. Where the table entries refer to the environment in which the system operates, the term "operating environment" is used.

4) The particular issues relating to legacy systems are described in Section 9.3.

5) Section 9.4 describes how the ISA work items change with the maturity of the contractor's combined SEMS, Section 9.5 addresses the variation with safety integrity requirements, and Section 9.6 discusses the impact of other procurement models.

9.1 General ISA documentation

1) Irrespective of the lifecycle phase, the ISA should produce the following documents:

Deliverable	**Comment**
ISA Plan	This should cover: the scope of the ISA work; a programme of work related to major project milestones; management and control including ISA staff competency; the strategy for the audit; and discussion of any special issues. It should be updated at reasonable intervals, for example at the start of a new project phase.
Progress reports	Reports summarising progress against the ISA Plan as contracted. These will be produced according to the demands of the project but may, typically, be on a quarterly basis.

Deliverable	**Comment**
ISA Reports	These should be produced prior to major programme milestones, such as the start of trials and acceptance into service. Normally they will follow a new version of the safety case. They should typically contain: an assessment of the safety argument; a short summary of the ISA's activities since the previous report; references to the documents produced; references to the documents examined; a discussion of any particular safety issues; and conclusions and recommendations on the safety of the activities covered by the safety case. Reference to the requirements of domain-specific JSPs should be made. In some sectors (e.g. the ship sector), the ISA Report is included within the Safety Case Report. In the air sector, the ISA Report is a customer report that informs Release to Service and provides crew advice.
Document reviews	The ISA's reviews of safety documents should be reported.
Audit reports	Safety audits should be documented.
Analysis reports	Any analyses carried out by the ISA should be documented.
Papers giving advice	Advice should always be generic (see Section 5.3). Advice may be given verbally, but substantive advice should be documented in written papers.

2) According to the sector, the ISA may be asked to sign documents produced by the contractor to indicate that they have been reviewed or endorsed by the ISA. The relevant safety management JSP will provide details. The contract with the ISA should make it clear if this is required.

9.2 Scopes of work by lifecycle phase

1) This section of the guidance sets out generic scopes of work for ISA services according to the phase in the CADMID lifecycle. Lifecycle phase is the main parameter affecting the scopes of work. Individual projects may of course depart from the strict definition of these phases, in which case the ISA scopes should be adjusted according to the safety cases to be produced.

2) The activities that the ISA will undertake at each phase are briefly summarised in Table 1.

Concept	Assessment	Demonstration	Manufacturing	In-service	Disposal
Assess safety and environmental requirements including initial safety case Assist with SOW Audit IPT's SMS or combined SEMS Attend safety committees	Assess safety and environmental requirements including initial safety case Assess tender responses for safety Audit contractor(s) Audit IPT's SMS or combined SEMS Attend safety committees	Assess changes to safety and environmental requirements Assess & audit contractor's safety work including safety case Assess tender responses for safety Audit IPT's SMS or combined SEMS Attend safety committees	Assess changes to safety and environmental requirements Assess & audit contractor's safety work including safety case Assess in-service safety case Audit IPT's/Operating Authority's SMS or combined SEMS Attend safety committees	Assess changes to safety and environmental legislation Monitor in-service performance Assess in-service safety case or legacy safety appraisal Audit IPT's/Operating Authority's SMS or combined SEMS Attend safety committees	Assess disposal safety case Assist with competition for disposal Assess & audit disposal contractor's safety work including safety case Audit IPT's SMS or combined SEMS for disposal Attend safety committees

Table 1: Summary of ISA activities through the lifecycle

3) In the sections below, each lifecycle phase is addressed in a self-contained subsection tabulating the safety evidence, the related ISA work item, the outputs produced by the ISA, and the customer or beneficiary for the outputs. The tables are divided by safety claim, and list the evidence that should be provided by the contractor or IPT to support each claim. The safety claims for each phase are illustrated in Appendix A. Note that the fact that separate safety claims and evidence are shown in the tables does not mean that separate documents are necessarily produced for each.

4) Clearly the ISA's work increases in proportion to the risk and complexity of the system. This is basically because the safety argument is more extensive and detailed for high risk or high complexity systems. Broadly speaking, the level of Safety Audit will vary as follows:

- A safety argument of the complexity illustrated in Appendix A will require comprehensive independent Safety Audit by an ISA team, particularly through the assessment, demonstration and manufacture phases.

- A simpler safety argument is likely to be sufficient if, for example, the safety requirements are entirely codified in standards such as the Display Screen Regulations or the IEE Wiring Regulations. There will then be no functional safety aspects to the safety argument and the occupational safety aspects will simply involve showing compliance to the applicable standards. The ALARP argument will be conformance to good practice. The reduced safety argument that applies in this case means that a higher-level Safety Audit by an individual is likely to be sufficient.

- If the contractor's safety work is poor, or if they have an immature combined SEMS, proportionately more work will be required for a given safety argument, as described in Section 9.4.

- If the system is highly safety-related or safety-critical, deeper independent analysis will be required, as described in Section 9.5.

- For large projects, subsystems will often have their own safety cases. The overall safety argument will be similar to a smaller project, but will need to be assembled from the sections of the argument in the subsidiary cases. This may require extra guidance and review cycles by the ISA, and interfacing with ISAs for super-system or subsystem IPTs.

- Some of the Safety Audit functions can be covered by other organisations. The way that in-house organisations may be able to support the work of the ISA, leading to a reduced need for Safety Audits, is described in Section 5.1.2. Sometimes, an MoD quality assurance representative is assigned to a contractor, and they may be able to liaise with the ISA to carry out some of the "traditional" audit functions.

Especially on large projects, the IPT may receive support from other organisations and contractors in the safety area (e.g. to witness tests), in which case the ISA may reasonably decide to rely on the conclusions of these other organisations rather than form an opinion directly.

5) Some work items (e.g. audit of safety requirements analysis process) are shown at each phase at which they might be carried out. In practice, the ISA might choose not to carry out certain work items at every phase if few problems had been found at previous phases. The rationale for the work items to be undertaken should be recorded in the ISA Plan for the phase.

6) Where ISA outputs (e.g. the ISA Report) are shown as supplied to organisations apart from the IPT and the relevant SMO (e.g. to tenderers or the Operating Authority), it is implicit that they will be supplied via the IPT.

7) There may be domain specific variations in the precise information and evidence that may be provided at each phase, but the information in the tables provides a reasonable summary of what the relationship is between the IPT and the ISA.

8) A table is also provided of the organisations to which the ISA should interface at each lifecycle phase.

9.2.1 Concept phase

1) At this phase, the safety requirements are developed in conjunction with Customer 1, as part of the business case for Initial Gate. Safety should be addressed in the drafting of the URD. The safety committee will typically be set up at this phase.

2) As illustrated in Appendix A, the ISA activities at this phase principally cover the definition of the safety requirements, confirmation that the safety requirements are achievable, and their flow into the URD. The scope of work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Safety and environmental requirements correctly captured and validated			
Safety and environmental requirements analysis (e.g. PHL, PHA)	Check analysis. Review report for correctness, completeness, consistency, achievability, conformance to standards and legislation. Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice.	Documented review. Audit report.	IPT
Safety and environmental tolerability criteria	Check analysis. Review report for conformance to standards and safety management plan. Check for agreement with criteria from similar projects.	Documented review.	IPT
System and operating environment description	Check description is sufficiently comprehensive for the reader to understand the safety argument.	Included in above reviews.	IPT

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Contractual safety and environmental requirements (initial safety case, safety case report and URD).	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.	Documented review.	IPT
Safety claim: IPT's safety management is adequate			
IPT's combined SEMS including Safety Management Plan for concept phase	Audit for conformance to standards.	Audit report.	IPT
MoD's safety organisation	Attend safety committee to discuss safety progress, raise and discuss safety issues, comment on safety case and supporting documents and analyses, agree tolerability of risks.	—	Safety committee members

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.

Organisational interfaces	**ISA work item**
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.2.2 Assessment phase

1) The safety requirements are further developed at this phase. Safety should be addressed in the drafting of the SRD.

2) Some programmes commence work associated with the Demonstration Phase in this phase, and therefore begin to expand the safety case to cover those activities.

3) As illustrated in Appendix A, the ISA activities continue to cover the definition of the safety requirements. The ISA can have a valuable role in assessing the tenders for safety, particularly the proposed safety argument for the safety case in the Development Phase. Following selection of the contractor or contractors, the ISA will assess their work for safety during the assessment phase.

4) See Section 9.5 for additional items that may be required for high safety integrity systems.

5) The scope of the ISA's work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
General items (referring to any/all individual claims)			
Initial (Concept) safety case report	Review report for correctness, completeness, consistency, conformance to standards and legislation.	Documented review.	IPT
Safety case report for Assessment Phase	Review report for correctness, completeness, consistency, conformance to standards and legislation.	Documented review.	IPT, contractor
Samples of evidence	Diverse analysis, witnessing, interviewing, traceability checks, vertical slices and inspection at the discretion of the ISA.	Results documented in working papers or ISA Report	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Safety and environmental requirements correctly captured and validated			
Safety and environmental requirements analysis (e.g. PHL, PHA)	Check analysis. Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice.	Documented review. Audit report.	IPT
Safety and environmental tolerability criteria	Check analysis. Review report for conformance to standards and safety management plan. Check for agreement with criteria from similar projects.	Documented review.	IPT
System and operating environment description	Check description is sufficiently comprehensive for the reader to understand the safety argument.	Included in above reviews.	IPT
Contractual safety and environmental requirements (SRD).	Review for correctness, completeness, consistency, conformance to standards and legislation. Check that evidence likely to be needed for subsequent safety arguments is contracted for.	Documented review	IPT

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Equipment meets safety and environmental requirements			
Tenderers' safety submissions	Review for correctness, completeness, consistency, conformance to standards and legislation. Check tolerability criteria for conformance to standards and safety management plan. Check for agreement with criteria from similar projects. Check analysis. Check that evidence is likely to be forthcoming (e.g. in the light of software development plan). Identify any areas of project risk from safety.	Documented tender assessments.	IPT
Safety analysis adequate	Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice. Review personnel competence.	Documented tender assessments and audit reports.	IPT, contractor
ALARP assessment	Check arguments for compliance with relevant standards and HSE guidance.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets occupational safety requirements			
Occupational design standards	Check for completeness and applicability. Audit for compliance to legislation, standards and safety management plan.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
OHHA and OSHA (if physical design and user/maintainer manuals sufficiently advanced at this phase)	Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit process for compliance to legislation, standards and safety management plan.	Documented review. Audit report.	IPT, contractor
Subclaim: Equipment meets environmental requirements			
Environmental impact analysis	Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management and/or environmental plan.	Documented review. Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets safety requirements for data and commands			
Hardware safety analyses	Check analyses for applicability and correctness. Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management plan. Possibly carry out diverse analyses, e.g. reliability modelling.	Documented review. Audit report.	IPT, contractor
Software safety analyses	Check analyses for applicability and correctness. Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management plan. Possibly carry out diverse analyses, e.g. reliability growth modelling.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
Human factors analyses	Audit human factors workshops etc. to check conducted in accordance with standards and good practice. Review report for correctness, completeness, consistency, conformance to standards and legislation. Possibly carry out diverse analysis of HCI for safety.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
COTS items	Review COTS safety justification. Consider feasibility and sufficiency of proposals for COTS assurance. Possibly carry out reliability analysis.	Documented review. Audit report. Working papers on diverse analysis.	IPT, contractor
Safety claim: IPT's safety management is adequate			
IPT's combined SEMS, including Safety Management (and Environmental Management) Plan for assessment phase	Audit for conformance to standards.	Audit report.	IPT
MoD's safety organisation	Attend safety committee to discuss safety progress, raise and discuss safety issues, comment on safety case and supporting documents and analyses, agree tolerability of risks.	—	Safety committee members
Safety claim: Contractor's safety management is adequate			
Tenderers' combined SEMS	Review for conformance to standards.	Tender assessment.	IPT, tenderer
Selected contractors	Audit for conformance to standards.	Audit report.	IPT, contractor

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
Tenderers	Respond to tender queries and formulate supplementary questions as necessary.
Selected contractor or contractors	Interface as described in Section 6.2.
Design Authority (when not IPT or contractor)	Interface as described in Section 6.6.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.2.3 Demonstration phase

1) Generally the prime contractor will be selected during this phase, and development work will commence. The ISA can have a valuable role in assessing the tenders for safety, particularly the proposed safety argument for the safety case. Following selection of the prime contractor, the ISA will assess their work for safety during the demonstration and manufacture phases.

2) At this phase, the safety requirements will be flowed to subsystems and components, and derived safety requirements identified.

3) See Section 9.5 for additional items that may be required for high safety integrity systems.

4) The scope of the ISA's work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
General items (referring to any/all individual claims)			
Safety case report	Review report for correctness, completeness, consistency, conformance to standards and legislation.	Documented review.	IPT, contractor
Samples of evidence	Diverse analysis, witnessing, interviewing, traceability checks, vertical slices and inspection at the discretion of the ISA.	Results documented in working papers or ISA Report	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Safety and environmental requirements correctly captured and validated			
Safety and environmental requirements analysis	Review changes and derived requirements for correctness, completeness, consistency, conformance to standards and legislation. Check analysis. Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice.	Documented review. Audit report.	IPT, contractor
Safety and environmental tolerability criteria	Review changes and flow to subsystems for conformance to standards and safety management plan. Check for agreement with criteria from similar projects. Check analysis.	Documented review.	IPT, contractor
System and operating environment description	Check description is sufficiently comprehensive for the reader to understand the safety argument.	Included in above reviews.	IPT, contractor
Contractual safety and environmental requirements (SRD).	Review changes and derived requirements for correctness, completeness, consistency, conformance to standards and legislation. Check that evidence likely to be needed for subsequent safety arguments is contracted for.	Documented review	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Equipment meets safety and environmental requirements			
Tenderers' safety submissions	Review for correctness, completeness, consistency, conformance to standards and legislation. Check tolerability criteria for conformance to standards and safety management plan. Check for agreement with criteria from similar projects. Check analysis. Check that evidence likely to be forthcoming (e.g. in the light of software development plan). Identify any areas of project risk from safety.	Documented tender assessments.	IPT
Safety analysis adequate	Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice. Review personnel competence.	Documented tender assessments and audit reports.	IPT, contractor
ALARP assessment	Check arguments for compliance with relevant standards and HSE guidance.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets occupational safety requirements			
Occupational design standards	Check for completeness and applicability. Audit for compliance to legislation, standards and safety management plan.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
OHHA and OSHA	Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit process for compliance to legislation, standards and safety management plan.	Documented review. Audit report.	IPT, contractor
Subclaim: Equipment meets environmental requirements			
Environmental impact analysis	Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management and/or environmental management plan.	Documented review. Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets safety requirements for data and commands			
Hardware safety analyses	Check analyses for applicability and correctness. Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management plan. Possibly carry out diverse analyses, e.g. reliability modelling.	Documented review. Audit report.	IPT, contractor
Software safety analyses	Check analyses for applicability and correctness. Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management plan. Possibly carry out diverse analyses, e.g. reliability growth modelling.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
Human factors analyses	Audit human factors workshops etc. to check conducted in accordance with standards and good practice. Review report for correctness, completeness, consistency, conformance to standards and legislation. Possibly carry out diverse analysis of HCI for safety.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
COTS items	Consider feasibility and sufficiency of proposals for COTS assurance. Review COTS safety justification. Possibly carry out reliability analysis.	Documented review. Audit report. Working papers on COTS issues and diverse analysis.	IPT, contractor
Safety claim: IPT's safety management is adequate			
IPT's Safety Management System, including Safety Management Plan for demonstration phase	Audit for conformance to standards.	Audit report.	IPT
MoD's safety organisation	Attend safety committee to discuss safety progress, raise and discuss safety issues, comment on safety case and supporting documents and analyses, agree tolerability of risks.	—	Safety committee members
Safety claim: Contractor's safety management is adequate			
Tenderers' combined SEMS	Review for conformance to standards.	Tender assessment.	IPT, tenderer
Contractor's combined SEMS	Audit for conformance to standards.	Audit report.	IPT, contractor
Contractor's safety organisation	Attend safety committees to discuss safety progress, raise and discuss safety issues, comment on safety case and supporting documents and analyses, agree tolerability of risks.	—	Safety committee members
Contractor's safety management plan	Review for conformance to standards.	Documented review.	IPT, contractor

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
Selected prime contractor	Interface as described in Section 6.2.
Design Authority (when not IPT or contractor)	Interface as described in Section 6.6.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.2.4 Manufacturing phase

1) In this phase, system development and production is completed and acceptance takes place. The safety case is expanded by developing operating aspects.

2) The ISA activities are shown in Appendix A. The work concentrates on the detailed safety argument that the system meets its safety requirements.

3) In the air sector, the ISA's organisational interface is with the Release to Service Authority rather than the Operating Authority.

4) See Section 9.5 for additional items that may be required for high safety integrity systems.

5) The scope of the ISA's work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
General items (referring to any/all individual claims)			
Safety case report	Review report for correctness, completeness, consistency, conformance to standards and legislation.	Documented review.	IPT, contractor
Safety case report for operation (or In-service Phase)	Review report for correctness, completeness, consistency, conformance to standards and legislation. Check adequacy and coverage of SOPs and training.	Documented review.	IPT, Operating Authority
Samples of evidence	Diverse analysis, witnessing, interviewing, traceability checks, vertical slices and inspection at the discretion of the ISA.	Results documented in working papers or ISA Report	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Safety and environmental requirements correctly captured and validated			
Safety and environmental requirements analysis	Review changes and derived requirements for correctness, completeness, consistency, conformance to standards and legislation. Check analysis. Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice.	Documented review. Audit report.	IPT, contractor
Safety and environmental tolerability criteria	Review changes and flow to subsystems for conformance to standards and safety management plan. Check for agreement with criteria from similar projects. Check analysis.	Documented review.	IPT, contractor
System and operating environment description	Check any changes to description.	Included in above reviews.	IPT, contractor
Contractual safety and environmental requirements (SRD).	Review changes and derived requirements for correctness, completeness, consistency, conformance to standards and legislation. Check that evidence likely to be needed for subsequent safety arguments is contracted for.	Documented review	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Equipment meets safety and environmental requirements			
Safety analysis adequate	Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice. Review personnel competence.	Documented tender assessments and audit reports.	IPT, contractor
ALARP assessment	Check arguments for compliance with relevant standards and HSE guidance.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
Subclaim: Equipment meets occupational safety requirements			
Occupational design standards	Check for completeness and applicability. Audit for compliance to legislation, standards and safety management plan.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
OHHA and OSHA	Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit process for compliance to legislation, standards and safety management plan.	Documented review. Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets environmental requirements			
Environmental impact analysis	Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management and/or environmental plan.	Documented review. Audit report.	IPT, contractor
Subclaim: Equipment meets safety requirements for data and commands			
Hardware safety analyses	Check analyses for applicability and correctness. Review report for correctness, completeness, consistency, conformance to standards and legislation. Audit for compliance to legislation, standards and safety management plan. Possibly carry out diverse analyses, e.g. reliability modelling.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
Software safety analyses	Check analyses for applicability and correctness. Audit for compliance to legislation, standards and safety management plan. Review report for correctness, completeness, consistency, conformance to standards and legislation. Possibly carry out diverse analyses, e.g. reliability growth modelling.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Human factors analyses	Audit human factors workshops etc. to check conducted in accordance with standards and good practice. Review report for correctness, completeness, consistency, conformance to standards and legislation. Possibly carry out diverse analysis of HCI for safety.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
COTS items	Consider feasibility and sufficiency of proposals for COTS assurance. Review COTS safety justification. Possibly carry out reliability analysis.	Documented review. Audit report. Working papers on COTS issues and diverse analysis.	IPT, contractor
Safety claim: IPT's and Operating Authority's safety management is adequate			
IPT's Safety Management System, including Safety Management Plan for Manufacturing Phase	Audit for conformance to standards.	Audit report	IPT
MoD's safety organisation	Attend safety committee to discuss safety progress, raise and discuss safety issues, comment on safety case and supporting documents and analyses, agree tolerability of risks.	—	Safety committee members
Safety claim: Contractor's safety management is adequate			
Contractor's combined SEMS	Audit for conformance to standards.	Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Contractor's safety organisation	Attend safety committees to discuss safety progress, raise and discuss safety issues, comment on safety case and supporting documents and analyses, agree tolerability of risks.	—	Safety committee members
Contractor's safety management plan	Review changes for conformance to standards.	Documented review.	IPT, contractor

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
Selected prime contractor	Interface as described in Section 6.2.
Design Authority (when not IPT or contractor)	Interface as described in Section 6.6.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.2.5 In-service phase

1) In this phase, the IPT maintains the levels of performance agreed with its customers and carries out approved upgrades or improvements, refits or acquisition increments. The ISA may be contracted in a stand-by role on a limit of liability contract, or engaged only when a safety issue emerges. The ISA's role is to monitor in-service performance to see if the system meets its safety requirements, and to identify weaknesses in the preceding work that only become apparent in service.

2) Further development work or a change of role will involve changes to the safety argument, which will require ISA action as described for the previous phases.

3) Safety and environmental requirements may change in-service due to changes to the system, its role, legislation, policy, etc.

4) Depending on the sector, the IPT may not be able to contract for Safety Audit of the Operating Authority's combined SEMS. In that case, the ISA's interface with the Operating Authority and DRACAS/FRACAS data will be through the in-service safety committee.

5) In the air sector, the ISA's organisational interface is with the Release to Service Authority rather than the Operating Authority.

6) The scope of the ISA's work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
General items (referring to any/all individual claims)			
Safety case report for operation (or In-service Phase)	Review report for correctness, completeness, consistency, conformance to standards and legislation. Check adequacy and coverage of SOPs and training.	Documented review.	IPT, Operating Authority, CLS contractor (if applicable)

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Safety and environmental requirements correctly captured and validated			
Contractual safety and environmental requirements.	Review the light of new or revised legislation, "grandfather rights".	Documented review.	IPT, Operating Authority, CLS contractor (if applicable)
Safety claim: IPT's safety management is adequate			
IPT's Safety Management System, including Safety Management Plan for In-service Phase	Audit for conformance to standards.	Audit report.	IPT
MoD's in-service safety organisation	Attend safety committee to discuss in-service safety issues from DRACAS, raise and discuss safety issues, comment on updates to safety case and supporting documents and analyses, agree continued tolerability of risks.	—	Safety committee members
Safety claim: Operating Authority's safety management is adequate			
DRACAS/FRACAS	Review data. Audit process for conformance to standards. Monitor corrective action.	Audit report.	IPT, Operating Authority, CLS contractor (if applicable)
Safety claim: CLS contractor's safety management is adequate (where appointed)			
Contractor's combined SEMS	Audit for conformance to standards.	Audit report.	IPT, CLS contractor
Contractor's safety management plan	Review for conformance to standards.	Documented review.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
If upgrades or improvements, refits or acquisition increments	**ISA work item**		
Safety argument changes	As for preceding phases.		

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
CLS contractor (if applicable)	Interface as described in Section 6.2.
Design Authority (when not IPT or contractor)	Interface as described in Section 6.6.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.2.6 Disposal phase

1) Planned disposal involves the efficient, effective and safe disposal of the system. Disposal should consider both end-of-life and post-accident cases. Both should be addressed by the original plans but, where these were produced some time previously, they should be reviewed for adequacy prior to disposal or periodically as appropriate. Where disposal is simple and there are no changes to the applicable legislation, it may not be necessary to employ an ISA.

2) The scope of the ISA's work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety case report for disposal	Review report for correctness, completeness, consistency, conformance to standards and legislation.	Documented review.	IPT, Operating Authority, disposal/CLS contractor (if applicable)
Safety claim: Disposal is safe			
IPT's Safety Management System, inc. Safety Management Plan for disposal phase	Audit for conformance to standards.	Audit report.	IPT
Disposal follows plan	If competition for disposal, review SOW and tender responses. Review disposal safety case. Audit disposal contractor's SMS.	Documented review.	IPT, Operating Authority, disposal/CLS contractor (if applicable)

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
Disposal/CLS contractor (if applicable)	Interface as described in Section 6.2.
Design Authority (when not IPT or contractor)	Interface as described in Section 6.6.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.3 Legacy systems

1) This section considers the ISA role for legacy systems, and specifically where a retrospective safety appraisal is to be carried out by a contractor.

2) The scope of the ISA's work is as follows:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
General items (referring to any/all individual claims)			
Retrospective safety appraisal/ safety case	Review correctness, completeness, consistency, conformance to standards and legislation. Check that report is proportionate to risk from system and remaining time in service.	Documented review.	IPT, contractor
Samples of evidence	Diverse analysis, witnessing, interviewing, traceability checks, vertical slices and inspection at the discretion of the ISA.	Results documented in working papers or ISA Report	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Safety and environmental requirements correctly captured and validated			
Safety and environmental requirements analysis	Review for correctness, completeness, consistency and conformance to standards. Review against applicable legislation bearing in mind time of introduction into service. Check analysis. Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice.	Documented review. Audit report.	IPT, contractor
Safety and environmental tolerability criteria	Review for conformance to standards and safety management plan. Check for agreement with criteria from similar projects. Consider application of "grandfather rights" for equipment in service for several years or more. Check if "time at risk" is properly considered. Check analysis.	Documented review.	IPT, contractor
System and operating environment description	Check description is sufficiently comprehensive for the reader to understand the safety argument.	Included in above reviews.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Equipment meets safety and environmental requirements			
Safety analysis adequate	Audit analysis process for conformance to standards and safety management plan. Attend analysis meetings to check conducted in accordance with standards and good practice. Review personnel competence.	Documented audit reports.	IPT, contractor
ALARP assessment	Check arguments for compliance with relevant standards and HSE guidance.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
Subclaim: Equipment meets occupational safety requirements			
Occupational design standards	Check for completeness and applicability. Audit for compliance to standards and safety management plan. Review against applicable legislation bearing in mind time of introduction into service.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
OHHA and OSHA	Review report for correctness, completeness, consistency and conformance to standards. Review against applicable legislation bearing in mind time of introduction into service. Audit against standards and safety management plan.	Documented review. Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets environmental requirements			
Environmental impact analysis	Review report for correctness, completeness, consistency and conformance to standards. Review against applicable legislation bearing in mind time of introduction into service. Audit for compliance to standards and safety and/or environmental management plan.	Documented review. Audit report.	IPT, contractor
Subclaim: Equipment meets safety requirements for data and commands			
Hardware safety analyses	Review report for correctness, completeness, consistency and conformance to standards. Audit for compliance to standards and safety management plan. Check analyses for applicability and correctness. Possibly carry out diverse analyses, e.g. reliability modelling.	Documented review. Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Software safety analyses	Audit for compliance to standards and safety management plan. Review report for correctness, completeness, consistency and conformance to standards. Check analyses for applicability and correctness. Possibly carry out diverse analyses, e.g. reliability growth modelling.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
Human factors analyses	Review report for correctness, completeness, consistency and conformance to standards. Review against applicable legislation bearing in mind time of introduction into service. Possibly carry out diverse analysis of HCI for safety.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
COTS items	Review COTS safety justification. Possibly carry out reliability analysis.	Documented review. Audit report. Working papers on COTS issues and diverse analysis.	IPT, contractor
Safety claim: IPT's safety management is adequate			
IPT's Safety Management System, inc. Safety Management Plan for in-service phase	Audit for conformance to standards.	Audit report.	IPT

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
MoD's safety organisation	Attend safety committee to discuss in-service safety issues from DRACAS, raise and discuss safety issues, comment on updates to safety case and supporting documents and analyses, agree continued tolerability of risks.	—	Safety committee members
Safety claim: Contractor's safety management is adequate			
Contractor's combined SEMS	Audit for conformance to standards.	Audit report.	IPT, contractor
Contractor's safety management plan	Review for conformance to standards.	Documented review.	IPT, contractor

Organisational interfaces	**ISA work item**
IPT	Produce plans and reports listed in Section 9.1. Supply generic advice. Attend ad-hoc meetings and respond to general queries.
Contractor	Interface as described in Section 6.2.
Design Authority (when not IPT or contractor)	Interface as described in Section 6.6.
Customer organisations	Interface as described in Section 6.3.
SMO	Interface as described in Section 6.4.

Organisational interfaces	**ISA work item**
Regulatory/certification bodies (where applicable)	Interface as described in Section 6.5.

9.4 Variation with maturity of contractor's combined SEMS

1) The major effect of an immature contractor's combined SEMS or poor safety culture is that the ISA work items listed above will take longer to complete, rather than that new work items will be required. Areas that have been found to be generally problematic are:

- The safety argument is implicit rather than explicit, and poorly structured. The ISA then has to participate in more document review cycles, especially for the safety case report, and also has to provide generic guidance on applicable standards and acceptable safety arguments.

- Tolerability of risk is inconsistent with comparable projects. This involves the ISA in additional work negotiating changes in the tolerability criteria.

- Technical aspects of the safety analysis are poorly done. Particular problems are confusion between hazards and accidents, judgements of ALARP, and completeness of hazard analysis. This involves the ISA in more document review cycles and detailed analysis of issues such as software reliability.

9.5 Variation with safety integrity requirements

1) The ISA role will be proportionately more extensive for high safety integrity systems. This is because the safety argument will be more involved, with each claim typically being supported by several diverse forms of evidence. For example, very high integrity avionics software would normally have its safety claim for correctness of data and commands supported by analysis, extensive testing and process evidence. On the other hand, a low integrity command and control system might rely on a smaller amount of testing plus process evidence.

2) The ISA work items cannot be accurately scoped until the safety argument is clear and therefore it is highly desirable for tenderers' safety submissions to include an outline of the safety argument.

3) Additional ISA work items for high safety integrity systems typically include:

Safety evidence	ISA work item	ISA output/deliverable	Customer/beneficiary
Subclaim: Equipment meets safety requirements for data and commands			
Software static analysis or proof	Technical review. Possibly selected diverse analyses.	Documented review/ working paper.	IPT, contractor
Automated testing	Technical review of test report. Check coverage and realism.	Documented review/ working paper.	IPT, contractor
High quality development process	Audit for conformance to standards. Check evidence for effectiveness.	Documented review/ working paper.	IPT, contractor
Fault tolerant or fail safe design	Technical review of design description. Check evidence for effectiveness and coverage.	Documented review/ working paper.	IPT, contractor
Safety monitor provided for COTS items	Analyse for coverage of failure modes.	Documented review/ working paper.	IPT, contractor
Hardware manufacturing process	Audit for correspondence between hardware items and design.	Documented review/ working paper.	IPT, contractor

9.6 Other procurement models

1) The basic safety argument illustrated in Appendix A is the same for all procurement models. However, the evidence is likely to be different for other procurement models such as foreign procurement, especially where it supports the safety argument for development. Also, for such procurements,

it may not be possible to negotiate the same degree of ISA access as for a bespoke development. The safety case for the system should explain how the different types of evidence adequately support the safety claims.

2) Possible procurement models are:

- Foreign procurement—The emphasis will be on issues of translation of the safety argument to the UK regime.
- Joint procurement—There will be interactions with the other procuring authorities who may have their own particular concerns, in order to place a single set of demands on the contractor. This may start at an early phase: "safety requirements captured and validated".
- PPP/PFI—The safety argument is basically unaffected in this type of procurement. If a system is being procured, the contractor develops the system and then leases it to the Customer rather than transferring it outright, but the contractor should provide a safety case as in the basic procurement model. If a service (e.g. training) is being provided, the contractor should produce a safety case covering buildings, equipment and procedures; depending on the specific situation, this may be the same as for a basic procurement or for a legacy system.
- Off-the-shelf-systems—This is an extreme example of COTS components.

3) In these other procurement models, the ISA work items for development may include the following:

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
General items (referring to any/all individual claims)			
Safety case report	Review report for correctness, completeness, consistency, conformance to standards and legislation.	Documented review.	IPT, contractor
Samples of evidence	Diverse analysis, witnessing, interviewing, traceability checks, vertical slices and inspection at the discretion of the ISA, but limited by the contractual arrangements for access.	Results documented in working papers or ISA Report	IPT, contractor, SMO (ISA Report only) where applicable

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Safety claim: Equipment meets safety and environmental requirements			
Safety analysis adequate	Review of development standards for compliance with UK, European and international regulations applicable in the UK. Review any activities undertaken to make up shortfalls. Review personnel competence.	Documented reports.	IPT, contractor
ALARP assessment	Check arguments for compliance with relevant standards and HSE guidance.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
Subclaim: Equipment meets occupational safety requirements			
Occupational design standards	Review of design standards for compliance with UK, European and international regulations applicable in the UK. Review any activities undertaken to make up shortfalls.	Included in document reviews or ISA Report.	IPT, contractor, SMO (ISA Report only) where applicable
OHHA and OSHA	Review for compliance with UK, European and international regulations applicable in the UK. Review any activities undertaken to make up shortfalls. Review activities to make up shortfalls.	Documented review. Audit report.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Subclaim: Equipment meets environmental requirements			
Environmental impact analysis	Review of environmental standards for compliance with UK, European and international regulations applicable in the UK. Review any activities undertaken to make up shortfalls. Review activities to make up shortfalls. Review report.	Documented review. Audit report.	IPT, contractor
Subclaim: Equipment meets safety requirements for data and commands			
Hardware safety analyses	Review hardware development plans and standards against UK, European and international regulations applicable in the UK. Review any activities undertaken to make up shortfalls. Check analyses for applicability and correctness. Possibly carry out diverse analyses, e.g. reliability modelling, COTS hardware reliability.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor
Software safety analyses	Review software development plans and standards against UK, European and international regulations applicable in the UK. Review any activities undertaken to make up shortfalls. Check analyses for applicability and correctness. Possibly carry out diverse analyses, e.g. reliability growth modelling, COTS software reliability.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor

Safety evidence	**ISA work item**	**ISA output/deliverable**	**Customer/beneficiary**
Human factors analyses	Audit human factors workshops etc. to check conducted in accordance with standards and good practice. Review report for correctness, completeness, consistency, conformance to standards and legislation. Possibly carry out diverse analysis of HCI for safety.	Documented review. Audit report. Working papers on diverse analyses.	IPT, contractor

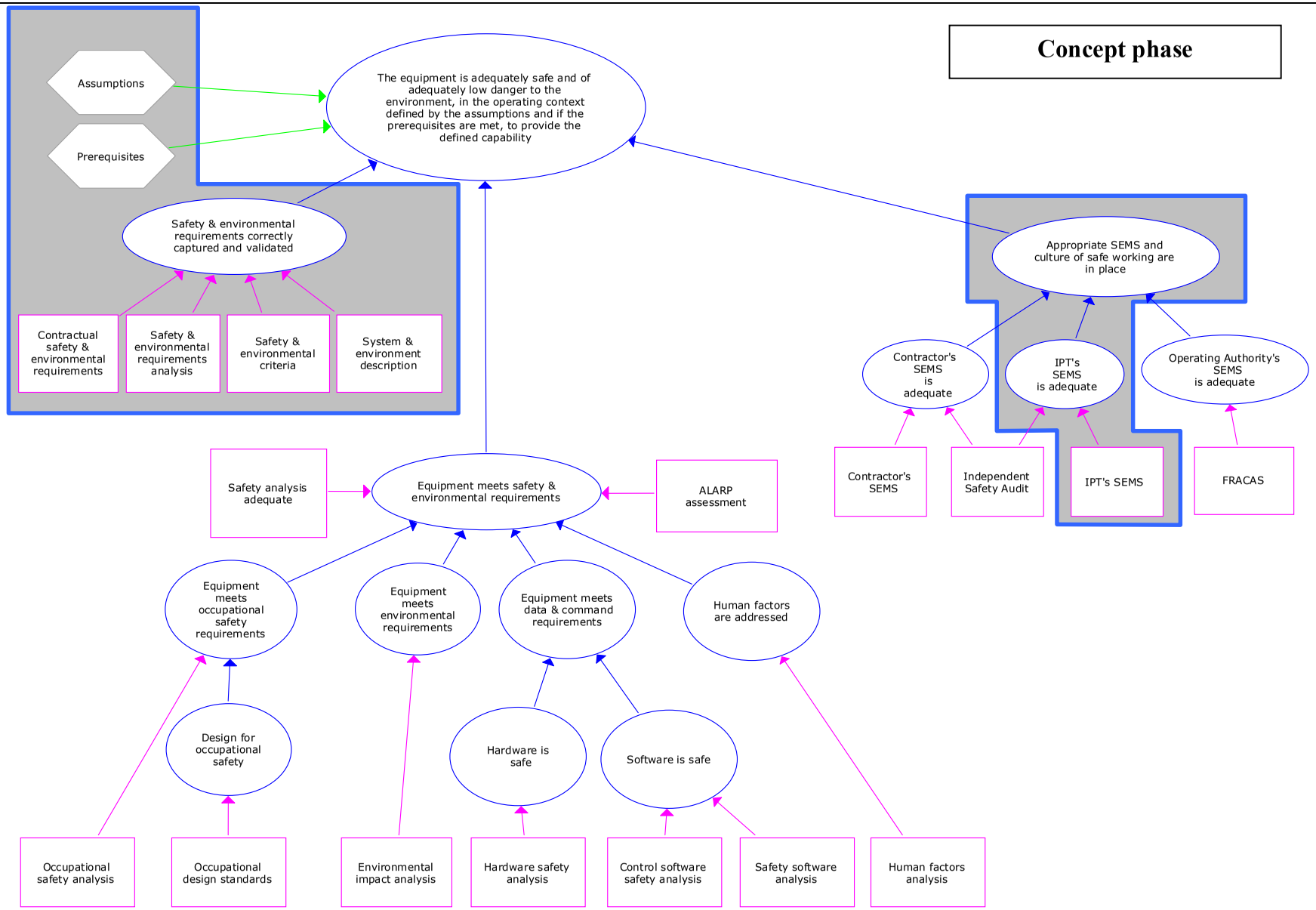
Appendix A Safety argument over the lifecycle

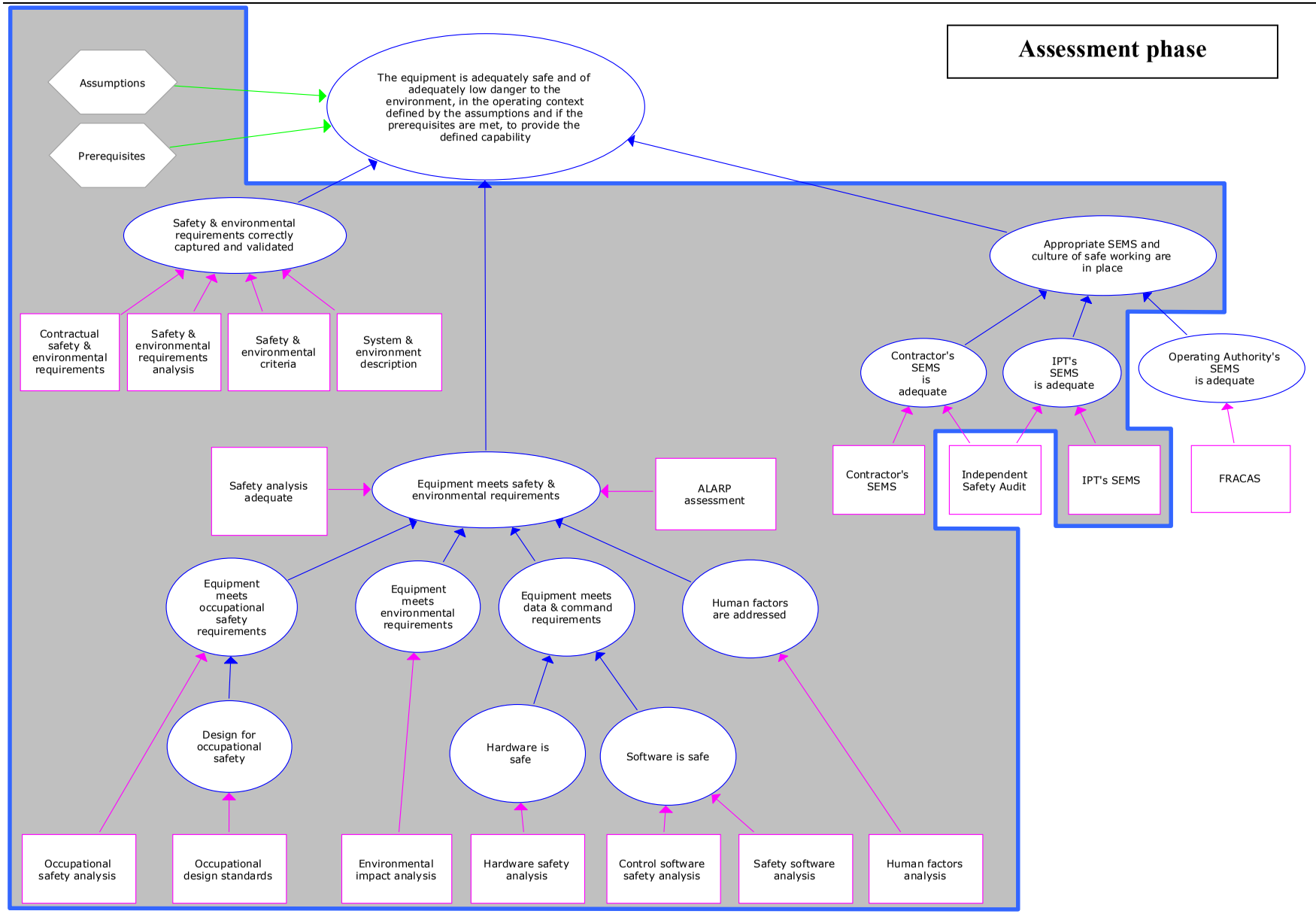
1) The diagrams on the following pages illustrate a typical, complex safety argument in terms of safety claims (blue ovals) and evidence (purple rectangles). For "systems of systems", some of the evidence will be contained in subsidiary safety cases.

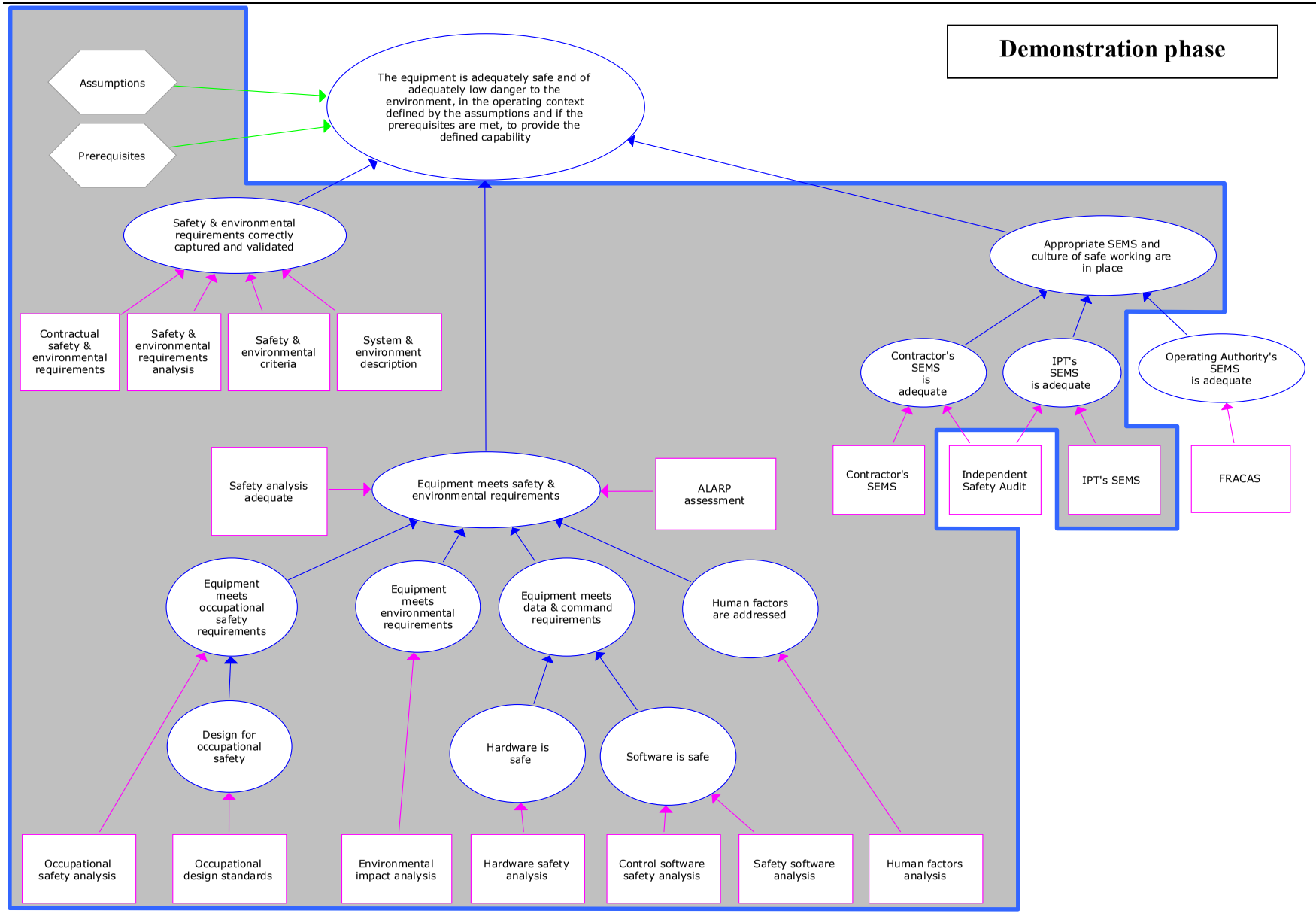
2) The Disposal Phase is omitted for clarity. It is best treated as a small separate project, building on the disposal aspects of main safety case.

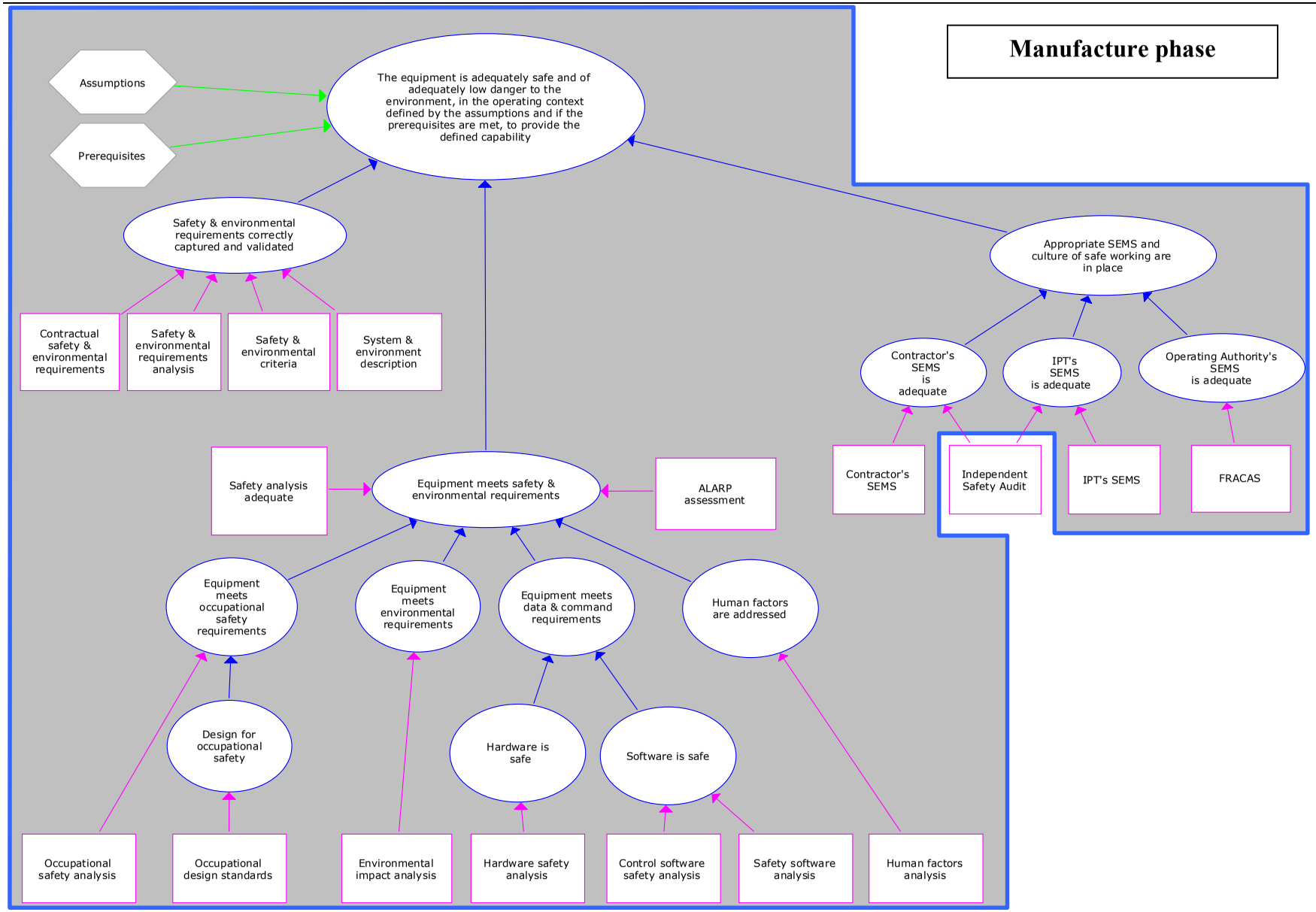
3) The term SEMS is used in the diagrams to refer to the relevant Safety Management and Environmental Management Systems or where appropriate the combined SEMS.

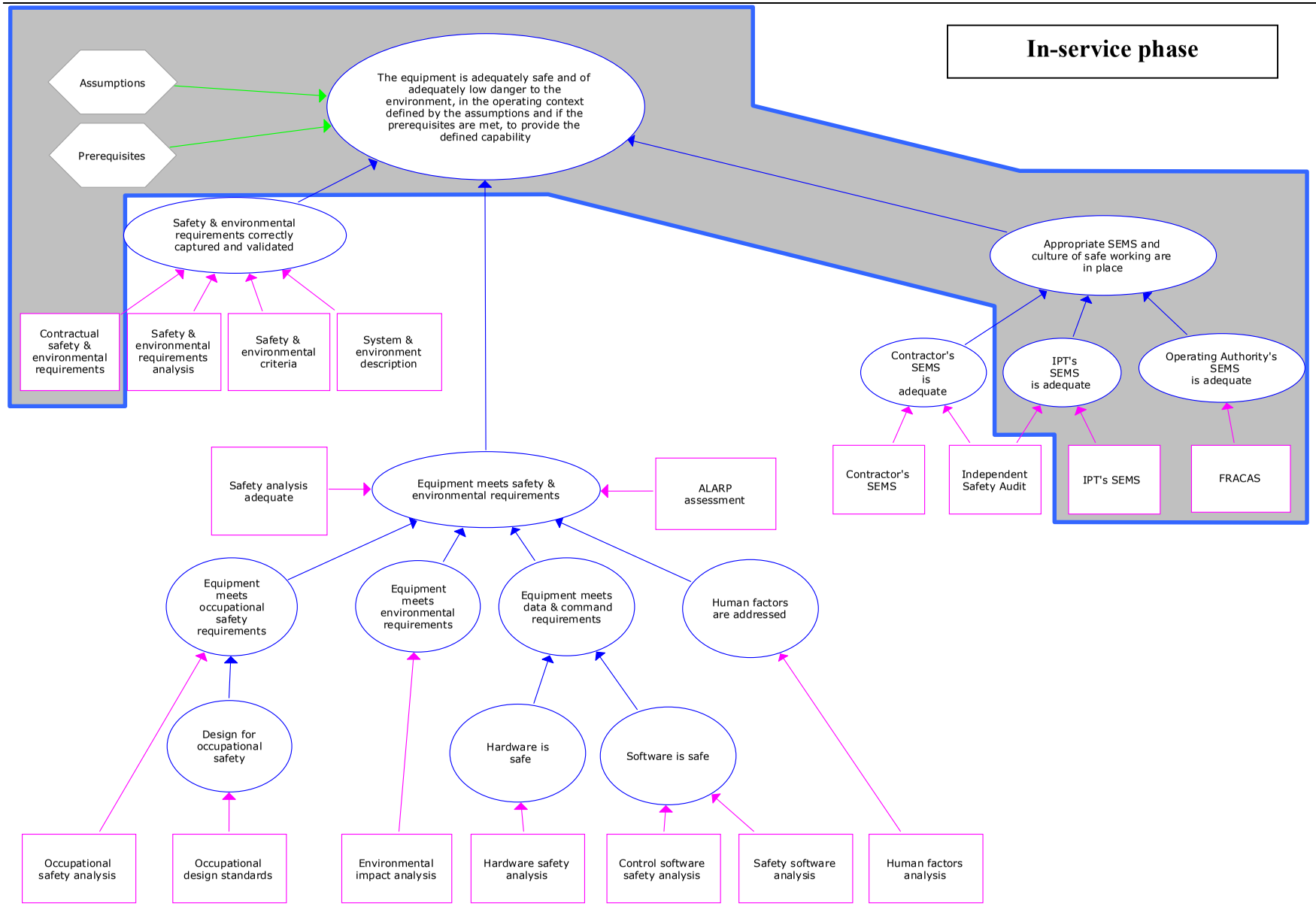
4) The diagram is repeated for each lifecycle phase with the sections that require ISA assessment shaded. The diagram for the In-service phase does not cover new development work; the ISA activities in that instance are shown in the Manufacture Phase diagram.


Concept phase
Assumptions
Prerequisites
The equipment is adequately safe and of adequately low danger to the environment, in the operating context defined by the assumptions and if the prerequisites are met, to provide the defined capability
Safety & environmental requirements correctly captured and validated
Contractual safety & environmental requirements
Safety & environmental requirements analysis
Safety & environmental criteria
System & environment description
Appropriate SEMS and culture of safe working are in place
Contractor's SEMS is adequate
IPT's SEMS is adequate
Operating Authority's SEMS is adequate
Contractor's SEMS
Independent Safety Audit
IPT's SEMS
FRACAS
Safety analysis adequate
Equipment meets safety & environmental requirements
ALARP assessment
Equipment meets occupational safety requirements
Equipment meets environmental requirements
Equipment meets data & command requirements
Human factors are addressed
Design for occupational safety
Hardware is safe
Software is safe
Occupational safety analysis
Occupational design standards
Environmental impact analysis
Hardware safety analysis
Control software safety analysis
Safety software analysis
Human factors analysis


Assessment phase
Assumptions
Prerequisites
The equipment is adequately safe and of adequately low danger to the environment, in the operating context defined by the assumptions and if the prerequisites are met, to provide the defined capability
Safety & environmental requirements correctly captured and validated
Appropriate SEMS and culture of safe working are in place
Contractual safety & environmental requirements
Safety & environmental requirements analysis
Safety & environmental criteria
System & environment description
Contractor's SEMS is adequate
IPT's SEMS is adequate
Operating Authority's SEMS is adequate
Safety analysis adequate
Equipment meets safety & environmental requirements
ALARP assessment
Contractor's SEMS
Independent Safety Audit
IPT's SEMS
FRACAS
Equipment meets occupational safety requirements
Equipment meets environmental requirements
Equipment meets data & command requirements
Human factors are addressed
Design for occupational safety
Hardware is safe
Software is safe
Occupational safety analysis
Occupational design standards
Environmental impact analysis
Hardware safety analysis
Control software safety analysis
Safety software analysis
Human factors analysis


Demonstration phase
Assumptions
Prerequisites
The equipment is adequately safe and of adequately low danger to the environment, in the operating context defined by the assumptions and if the prerequisites are met, to provide the defined capability
Safety & environmental requirements correctly captured and validated
Appropriate SEMS and culture of safe working are in place
Contractual safety & environmental requirements
Safety & environmental requirements analysis
Safety & environmental criteria
System & environment description
Contractor's SEMS is adequate
IPT's SEMS is adequate
Operating Authority's SEMS is adequate
Safety analysis adequate
Equipment meets safety & environmental requirements
ALARP assessment
Contractor's SEMS
Independent Safety Audit
IPT's SEMS
FRACAS
Equipment meets occupational safety requirements
Equipment meets environmental requirements
Equipment meets data & command requirements
Human factors are addressed
Design for occupational safety
Hardware is safe
Software is safe
Occupational safety analysis
Occupational design standards
Environmental impact analysis
Hardware safety analysis
Control software safety analysis
Safety software analysis
Human factors analysis


Manufacture phase
Assumptions
Prerequisites
The equipment is adequately safe and of adequately low danger to the environment, in the operating context defined by the assumptions and if the prerequisites are met, to provide the defined capability
Safety & environmental requirements correctly captured and validated
Contractual safety & environmental requirements
Safety & environmental requirements analysis
Safety & environmental criteria
System & environment description
Appropriate SEMS and culture of safe working are in place
Contractor's SEMS is adequate
IPT's SEMS is adequate
Operating Authority's SEMS is adequate
Contractor's SEMS
Independent Safety Audit
IPT's SEMS
FRACAS
Safety analysis adequate
Equipment meets safety & environmental requirements
ALARP assessment
Equipment meets occupational safety requirements
Equipment meets environmental requirements
Equipment meets data & command requirements
Human factors are addressed
Design for occupational safety
Hardware is safe
Software is safe
Occupational safety analysis
Occupational design standards
Environmental impact analysis
Hardware safety analysis
Control software safety analysis
Safety software analysis
Human factors analysis


In-service phase
Assumptions
Prerequisites
The equipment is adequately safe and of adequately low danger to the environment, in the operating context defined by the assumptions and if the prerequisites are met, to provide the defined capability
Safety & environmental requirements correctly captured and validated
Contractual safety & environmental requirements
Safety & environmental requirements analysis
Safety & environmental criteria
System & environment description
Appropriate SEMS and culture of safe working are in place
Contractor's SEMS is adequate
IPT's SEMS is adequate
Operating Authority's SEMS is adequate
Contractor's SEMS
Independent Safety Audit
IPT's SEMS
FRACAS
Safety analysis adequate
Equipment meets safety & environmental requirements
ALARP assessment
Equipment meets occupational safety requirements
Equipment meets environmental requirements
Equipment meets data & command requirements
Human factors are addressed
Design for occupational safety
Hardware is safe
Software is safe
Occupational safety analysis
Occupational design standards
Environmental impact analysis
Hardware safety analysis
Control software safety analysis
Safety software analysis
Human factors analysis