New MoD ISA Guidelines

Peter Froome
Adelard
pkdf@adelard.com

Background

- The role of ISA is enshrined in MoD safety policy, but with differences between sectors
- There is however no detailed guidance on the ISA's activities, and how to contract for ISA services
- The current work was therefore initiated by the MoD Safety Management Offices Group, managed by the SSMO

Sources

- The guidance took as its starting point:
  - The safety management JSPs
  - Def Stans 00-55 and 00-56 (Issues 2 & 3)
  - QinetiQ guidelines
  - Yellow Book
  - ISA WG minutes

Contents

- The guidance addresses:
  - Basis for the ISA role
  - Key definitions
  - Relationships with other organisations
  - Selection of ISAs
  - Expertise & competence
  - Detailed scopes of work
- Work also addressed options for third-party competence assessment in a separate report

Adelard

Basis for the ISA role

- In all MoD sectors, ISA is mandated or strongly recommended
- IPTs should ensure adequate access etc. through appropriate contract clauses and conditions
- The ISA has no executive authority
  - The IPT accepts full responsibility for safety and may overrule an ISA's recommendations

But in that case, record robust justification

Adelard

Other aspects

- The ISA plays an important part in advising the contractor and the IPT on a framework of appropriate standards and good practice
  - Increasingly important with “goal-based”, as opposed to prescriptive, regulation
- The ISA may assist the SMO to discharge its responsibilities for monitoring effective safety and environmental management

Definitions - independent

- *Able to provide an expert, professional opinion without vulnerability to commercial, project or other pressure*
- Guidance recommends that the ISA is from an independent organisation
  - Common objections are examined and overcome
  - Relationship to in-house safety organisations discussed

Definitions - safety audit

- Def Stan 00-56/3 definition quoted
- Interpretation is: *Safety Audit consists of the activities that enable an expert, professional, independent opinion to be reached on the safety of the system*
- 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 (cont)

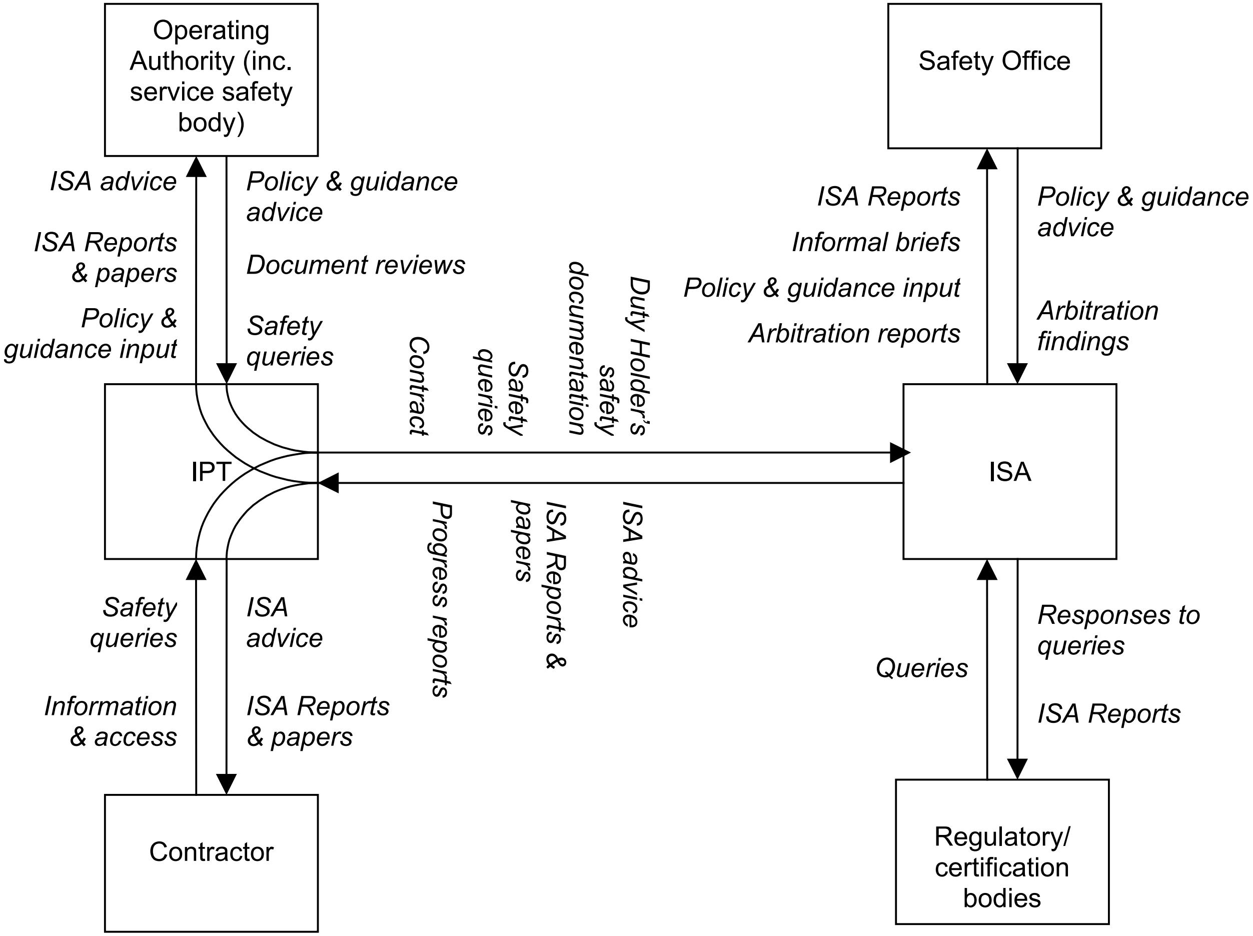
- Typically, the ISA will form their opinion on the basis of the following:
    - Targeted document reviews
    - Independent assessment and analysis
    - “Traditional” audits of safety and development processes
- Safety Audit consists of considerably more than “traditional” auditing
    - In fact such auditing makes up a fairly small proportion of the ISA’s activities

Definitions - safety advice

- *General advice on the acceptability of a proposed safety argument, which facilitates the IPT's or contractor's decision-making*
- In order to maintain their independence, the ISA cannot give specific advice
  - However, it is legitimate for the ISA to give general advice i.e. that which would be given to any broadly similar project
  - Can also advise on safety implications of particular technology choices

Relationships with other bodies

- Relationships described with
  - IPT
  - Contractor
  - Operating Authority
  - Safety Management Offices
  - Regulatory/certification bodies
  - Design Authority



Operating Authority (inc. service safety body)

ISA advice

ISA Reports & papers

Policy & guidance input

Policy & guidance advice

Document reviews

Safety queries

Safety Office

ISA Reports

Informal briefs

Policy & guidance input

Arbitration reports

Policy & guidance advice

Arbitration findings

IPT

Contract

Safety queries

Duty Holder's safety documentation

ISA

Progress reports

ISA Reports & papers

ISA advice

Safety queries

Information & access

ISA advice

ISA Reports & papers

Contractor

Queries

Responses to queries

ISA Reports

Regulatory/ certification bodies

Selection of ISAs

- Covers
  - Independence
  - Competence
  - Project complexity
  - Safety risk
  - Lifecycle phase

Project complexity

- Complexity can be due to
  - *Technical complexity* ⇒ complex safety argument ⇒ higher level of ISA technical competence
  - *Problems with safety evidence* ⇒ more effort
  - *Large project scale* ⇒ "systems-of-systems" safety arguments involving evidence for systems hierarchies ⇒ proven experience of interrelated safety cases
  - Converse for very simple systems
  - *PFI/PPP/foreign acquisition* ⇒ need to be able to interpret safety standards in light of UK requirements

Safety risk

- One of ISA roles is to reduce uncertainty in the validity of the safety argument
- 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
- Thus IPT could consider
  - the use of an individual rather than a team
  - less specific experience

Expertise & competence

- Three types of competence required to assess the suitability of an ISA:
  - Technical competence: safety and technical knowledge
  - Auditing competence: skills necessary to perform the Safety Audit
  - Behavioural competence: qualities and attributes of behaviour and character

Technical competence

- Technical competence has two aspects:
  - Technical competence in Safety Audit independent of the specific application domain and technology used (inc. legal framework, principles, methods, standards)
  - Technical competence in the application domain (inc. safety practices appropriate to the organisation and application area, appropriate engineering knowledge & experience, experience of other systems engineering disciplines)

Auditing competence

- By contrast, auditing competence considers the specific activities performed as part of a Safety Audit (that is, document review, process audits and independent analyses)

Behavioural competence

- 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

Competence assessment

- Competence assessment should be in terms of the criteria described above
  - Where a project requires a team approach, it is the balance of skills that is important
- The IPT should ask potential ISAs for evidence of competence, supported by verifiable examples
  - Typically, evidence is based on training, qualifications and experience
  - Proven ability is likely to provide the best indicator

Evidence of competence

- Three types of evidence:
  - *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*, according to a scheme such as the IEE/BCS Competency Guidelines or the Network Rail ISA Accreditation Scheme
    - The IPT should ask for any third-party audit of the scheme

Evidence (cont)

- *Assessment by a third-party independent organisation* that designs a scheme and independently assesses the ISA

- Options for third-party assessment are discussed in a supporting report to the SMOs

Detailed scopes of work

- Documents
- Scopes of work over CADMID lifecycle
- Legacy systems
- Changes with the maturity of the contractor’s SMS
- Variation with safety integrity requirements
- Impact of other procurement models

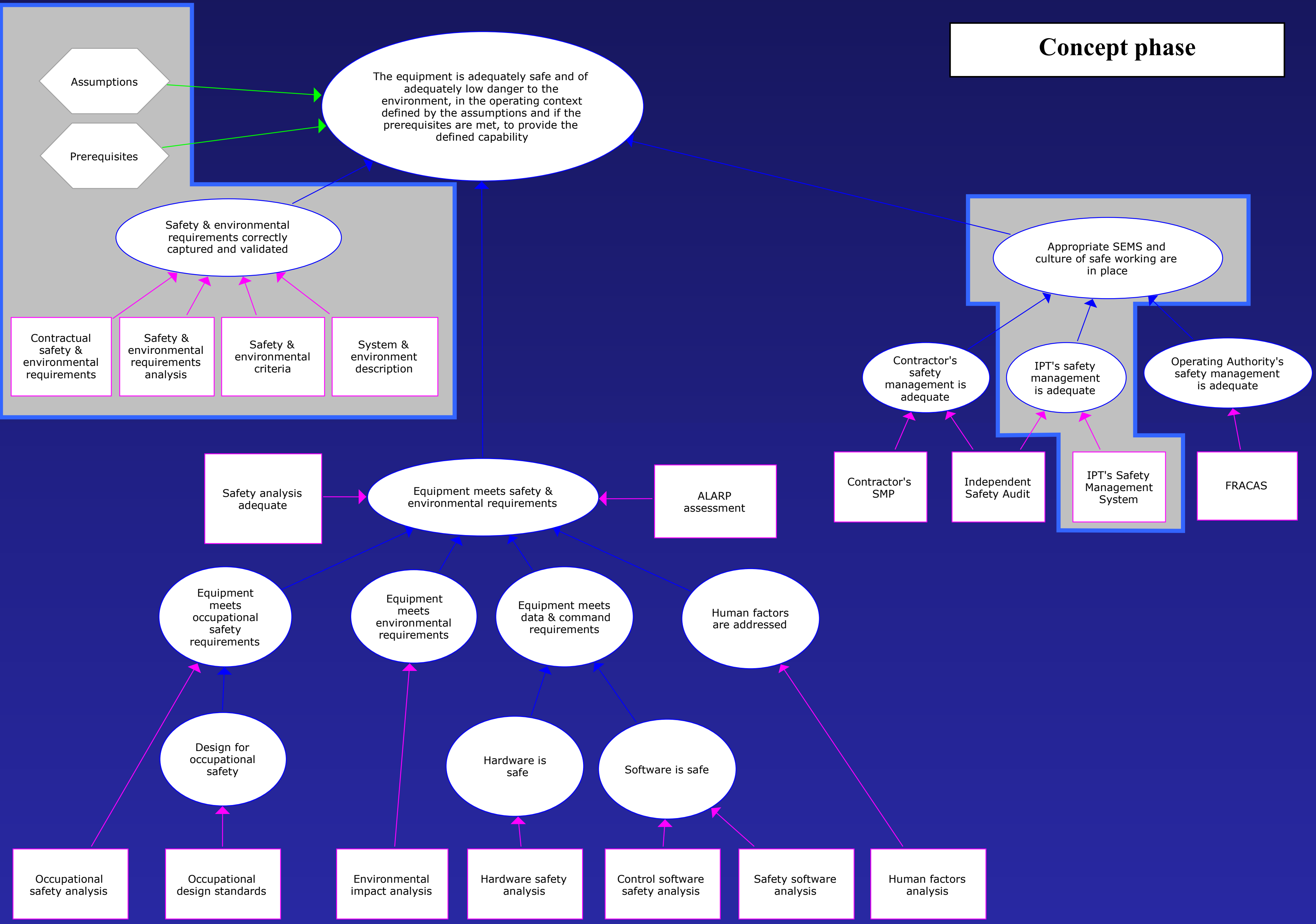
ISA document outputs

- ISA Plan
- Progress reports
- ISA Reports
- Document reviews
- Audit reports
- Analysis reports
- Reports giving advice

Scopes of work over the lifecycle

- The ISA tasks are related to typical safety arguments for each lifecycle phase
  - Concept
  - Assessment
  - Demonstration
  - Manufacture
  - In-service
  - Disposal

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 safety management is adequate

IPT's safety management is adequate

Operating Authority's safety management is adequate

Contractor's SMP

Independent Safety Audit

IPT's Safety Management System

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

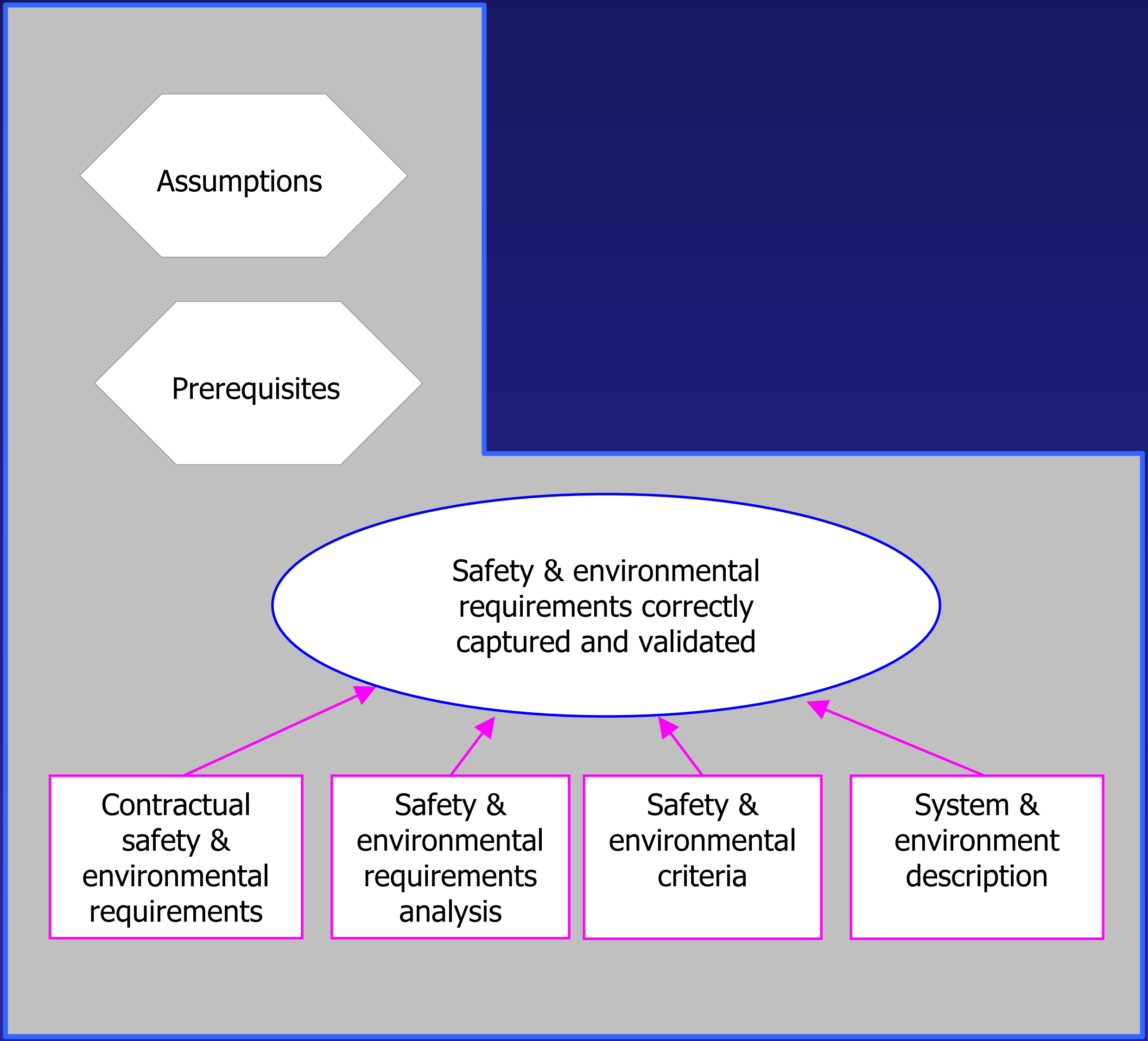
Environmental impact analysis

Hardware safety analysis

Control software safety analysis

Safety software analysis

Human factors analysis



Assumptions

Prerequisites

Safety & environmental requirements correctly captured and validated

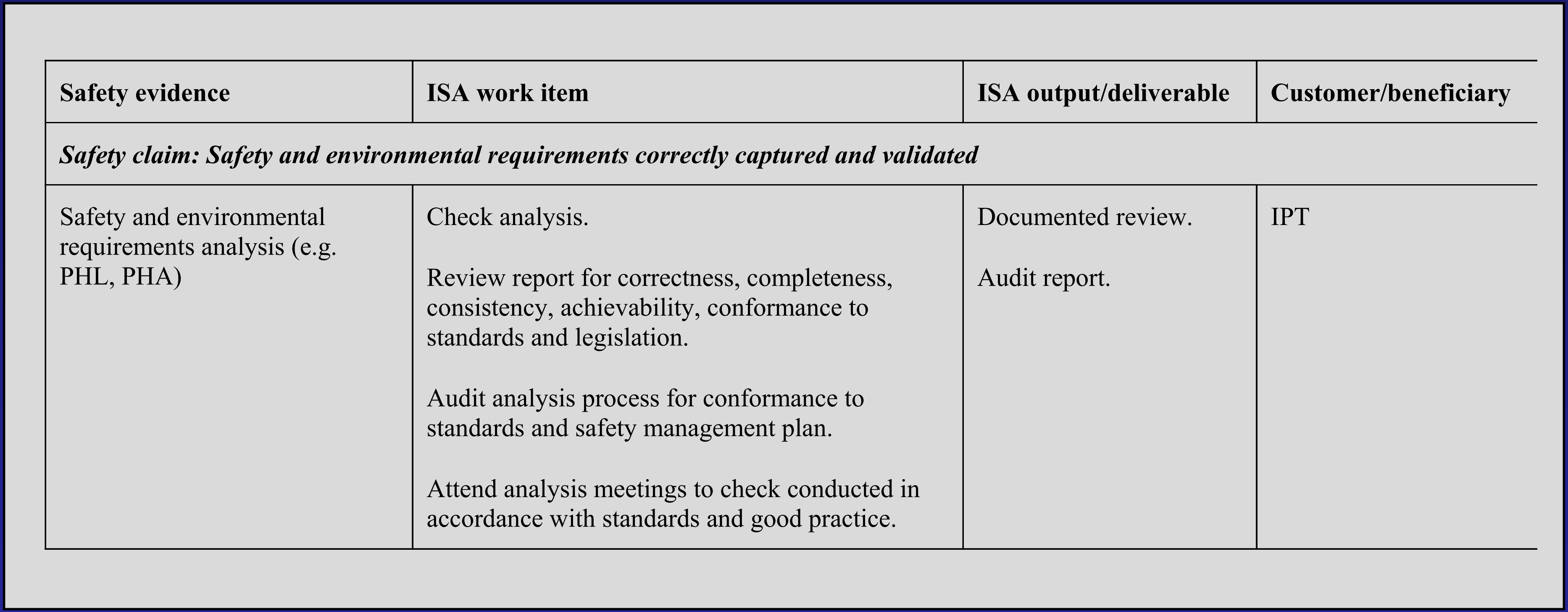
Contractual safety & environmental requirements

Safety & environmental requirements analysis

Safety & environmental criteria

System & environment description

Example table - Concept Phase



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

Variation with risk

- Guidance addresses how ISA’s work increases in proportion to the risk and complexity of the system
    - This is because the safety argument is more extensive and detailed for high risk or high complexity systems

Summary

- Guidance on contracting for ISAs has been produced for IPTs covering
  - Basis for the ISA role, in policy & standards
  - Key definitions: *independent*, *audit* & *advice*
  - Relationships with other organisations
  - Selection of ISAs
  - Expertise & competence
    - technical, auditing & behavioural competence
  - Detailed scopes of work linked to safety argument for lifecycle phase