Defence Standard 00-56 Issue 5: Concepts, Principles and Pragmatics

John A McDermid*, Phil Williams†

** University of York and McDermid Associates, York, UK, john.mcdermid@york.ac.uk*
† Engineer for Safety Limited, Hastings, UK, phil.williams@engineerforsafety.co.uk

Keywords: Safety Standards; Defence; Safety Management; Contracting for Safety.

Abstract

Defence Standard (DS) 00-56 is the UK MoD's primary contracting safety management standard, used to govern the safety aspects of work undertaken by industry under contract to the MoD. The MoD is going through a period of unprecedented change and this is impacting the way in which MoD and its suppliers manage safety, as well as many other aspects of the defence enterprise. The paper explains some of the drivers for updating DS 00-56 from issue 4 to issue 5 and explains the rationale for the key changes in the standard.

1 Introduction

The UK Ministry of Defence (MoD) acquires a wide class of systems for the Armed Services. These systems can impact the safety of military personnel and of the general public. Defence Standard (DS) 00-56 was developed to address safety management on contracts. Initially published in 1991 DS 00-56 has evolved over the years, with Issue 4 [1] being published in 2007. The change from Issue 4 to Issue 5 [2], published in 2014, may be perceived as substantial, but the core concepts have been preserved. The aim of the paper is to explain the major changes between Issues 4 and 5, with a focus on concepts and principles, but also considering the pragmatics of adopting the latest issue of the standard.

For many years, MoD's policy has been that standards should be "as civil as possible, and only as military as necessary" [3]. This was the case when DS 00-56 Issues 3 and 4 were issued, but feedback indicates that this was too implicit, and probably not adequately understood. Thus the definition of DS 00-56 Issue 5 has sought to make this policy more explicit.

Further, MoD's policy states a preference for using off-the-shelf (OTS) systems or products [4], but noting that there may be a need for modified OTS products or systems, specifically "to meet:

- UK standards of airworthiness or health & safety;
- UK communications or other interoperability needs, such as radios; or
- Higher standards for particular aspects of operational advantage, such as force protection, electromagnetic spectrum management, or cyber security."

One of the major challenges for development of the standard is the range of products which are acquired, e.g. from ration packs to aircraft carriers, or parts thereof. The standard also has to address a range of acquisition scenarios, including purchase of bespoke equipment, acquisition of OTS products, both modified and unmodified, and provision of services.

A core team was set up to develop DS 00-56 Issue 5. This team had representation from industry practitioners, the ISA community and academia, in order to obtain a broad view of the policy context and other relevant challenges; the team was managed and guided by Dstl/MoD. The core team took into account a number of specific requirements and other drivers in developing DS 00-56 Issue 5; these are set out in section 2. The standard embodies a number of key concepts some of which were implicit previously and have now been made explicit, whereas others are new for Issue 5; this is discussed in section 3. Section 4 completes the rationale for the approach adopted by DS 00-56 Issue 5 by setting out the principles on which the standard is based.

Section 5 discusses the pragmatics of working to DS 00-56 Issue 5 including the ability to tailor the standard. Observations on the development of the standard and lessons identified are set out in section 6, which also briefly considers the links with the programmable element (PE) standard, DS 00-55, which is being re-developed (a public draft at the time of writing). Finally, section 7 sets out our conclusions.

2 Requirements and Drivers

The core team developing DS 00-56 Issue 5 were given four high-level requirements by the MoD, but also took into account a number of other important factors, referred to here as change drivers, reflecting the organisational changes and other pressures on the MoD. We discuss each in turn.

2.1 Requirements

The MoD set out four key requirements for the update to the standard. First, it had to address situations where contractors cannot make ALARP decisions, typically because they only deliver parts of systems to the MoD, e.g. an aero engine separately from the aircraft. In such cases, contractors cannot judge the level of risk or its acceptability, as they do not have sufficient knowledge about the broader system or the context of use. This requirement arose in response to feedback about the difficulties of working to DS 00-56 Issue 4.

Second, MoD buys services, e.g. supply of communications, from contractors as well as systems and subsystems. Thus the standard has to be usable to govern acquisition of services.

Third, the standard must address the acquisition of systems of systems (SoS), or parts thereof. For example, the MoD might acquire a Naval vessel and a set of unmanned underwater vehicles (UUVs); the safety management processes need to consider the range of configurations of the vessel and UUVs.

Fourth, DS 00-56 Issue 5 had to address the use of non-MoD standards. Whilst this reflects a policy which has been in force for more than a decade, as indicated above it has not been widely understood and needed to be addressed more explicitly in Issue 5.

The use of non-MoD standards is intended to allow the MoD to use OTS equipment designed for commercial markets to gain benefits in terms of cost, maturity, support, etc. However it is also intended to enable industry to work with standards with which they are familiar, and that are under continuous use and maintenance in the commercial world, maintaining pace with changes in legislation and technology. This is expected to both reduce cost for the MoD and to reduce risk for MoD and contractors alike.

2.2 Other Change Drivers

The main change drivers relate to organisational change in the MoD, but there are a number of other factors. The major MoD organisation and policy changes are as follows.

There have been changes in regulation, especially the formation of the Military Airworthiness Authority (MAA) following the Haddon-Cave Report [5] and the subsequent establishment of the Defence Safety and Environmental Authority (DSEA), i.e. the introduction of new regulators, a new regulation framework, and new/revised regulations and changes to safety-related Joint Service Publications (JSPs).

The MoD has been reorganised, including changing the legal standing of Defence Equipment and Support (DE&S) to a bespoke trading entity, and the transfer of some equipment responsibilities to Front Line Commands (FLC). These, along with the regulatory changes, have had an impact on where safety responsibility lies, particularly in some sectors.

Following the Secretary of State's Policy statement [6], there is a clearer focus on Risk to Life (RtoL) in the broad sense of covering injury and illness as well as fatality, but not considering equipment loss or environmental impact except where they have a measurable effect in terms of RtoL.

Some other important drivers are progress in recognised good practice in safety engineering and recognition that it is unusual for contractors to have complete design visibility. This latter point arises because most systems involve OTS elements and there may be access constraints, e.g. due to the International Trade in Arms Regulations (ITAR).

2.3 Observations

Although the requirements and these drivers were specific, the standard was developed against a background of ongoing change and this influenced the concepts and principles.

3 Concepts

The concepts introduced here are new "constructs" in the standard introduced to deal with the requirements and drivers. These can be divided into four main areas, as outlined below. In contrast the principles, set out in section 4, are ways of using both the new concepts and the other elements of the standard to manage safety in a given project.

3.1 Product/Service/System (PSS)

Whereas DS 00-56 Issue 4 referred to systems (and to derivatives thereof such as system-of-systems (SoS)), Issue 5 distinguishes between products, services and systems, using the acronym PSS when no distinction needs to be made. A product is a smaller-scale element than a system, e.g. a winch for a warship, which cannot be fully assessed for safety outside its context of use. This concept is introduced to address the first and, to a lesser extent, the third requirement.

Systems have the same meaning as in DS 00-56 Issue 4, and a service is used in the normal dictionary sense. A service might be the operation of a system, or the conduct of work on a system, e.g. maintenance, but excludes auditing, manpower substitution, etc. The introduction of services is significant. The MoD normally operates systems and has the responsibility for safety (amongst other things). However, where contractors provide services they have responsibility for safety of that operation (note that this doesn't mean that MoD is free of all responsibility). This is one of the few cases where contractors need to address the full implications of ALARP due to their increased operational responsibility.

This directly addresses the second requirement.

3.2 Hazard and Failure Modes

The term hazard is used with the same sense as in DS 00-56 Issue 4, although it should be noted that it is difficult to define the concept, and other standards use different definitions. This is pertinent when we discuss civil standards in section 4.2.

Issue 5 uses the term failure modes, in the same sense as in failure modes and effects analysis (FMEA), where product suppliers cannot judge whether or not the failure modes are, or contribute to, hazards given limits on their knowledge of the way the product will be used. Similarly, failure modes are used in relation to systems where they are not hazards in themselves, but may contribute to hazards in an SoS.

In general, contractors would be expected to identify both hazards and failure modes for products and systems. For example, the contractor should be able to identify intrinsic hazards due to materials used and hazards from maintenance.

This supports the first and third requirements.

3.3 Scope of Contract

Implicitly a contract has a scope in terms of the things which are to be done and delivered by a contractor for a customer;

DS 00-56 Issue 5 makes this explicit and identifies two sub-elements: the scope of supply and the scope of analysis.

The scope of supply is what is being purchased, both tangible PSS and supporting deliverable documents, e.g. a safety case report (SCR). The scope of analysis is that which is to be analysed for safety. This is an important distinction, as the scope of analysis may not match the scope of supply.

The scope of analysis may exceed the scope of supply, e.g. if an aircraft manufacturer is replacing equipment on an aircraft that he designed, then it would be reasonable for the scope of analysis to include aircraft-level hazards. On the other hand, supply of a new version of existing equipment, for a new use, may involve no analysis (if the contractor has insufficient knowledge about the use) or analysis limited to the new use, not the existing uses.

The MoD and the contractor will normally have to work together to establish the scope of contract, see section 4.4.

This supports the first and third requirements.

3.4 Information Set and Summary

In DS 00-56 Issue 5 the concepts of safety cases and SCRs are the same as in Issue 4, but there are two new concepts: the information set and information set safety summary (ISSS) that help to address the first three of MoD's requirements.

The information set is the collection of safety-relevant design and analysis information produced in development and during sustainment. DS 00-56 Issue 5 has requirements to identify and maintain the information set. This is not imposing new work (or costs); the information set is simply a name for the (virtual collection of) work products that arise from design and analysis. Amongst other things it will be a source of evidence for the safety case.

The ISSS is an extract from, or an index into, the information set. It contains the core information which third parties, e.g. the MoD or system integrators, need to know in order to discharge their safety responsibilities. The ISSS would normally contain information about failure modes, but also other properties, e.g. maximum surface temperature that can arise in operation, and limitations and assumptions, which are needed to safely use the product (or system in an SoS).

The ISSS also contains an argument (like a safety case and an SCR) but the intent is different; to give the rationale for the selection of information. It is different from an SCR in that an SCR deals with those issues where the contractor can make a judgment about acceptability of risk, and the ISSS deals with other aspects of system safety. In general an SCR and ISSS would be expected for all PSS, but the balance between them would vary very much with the scope of supply, and scope of analysis. Whilst they are different concepts it is possible to make the SCR and an ISSS a single document – indeed some of the reviewers of early drafts of DS 00-56 Issue 5 observed (correctly) that good SCRs already cover both roles; thus this is a clear case where DS 00-56 Issue 5 has made explicit the intent of Issue 4 by the introduction of specific concepts.

4 Principles

The principles mainly articulate the way in which DS 00-56 Issue 5 is expected to be used, and links together key aspects of the standard. The first group of principles relates very strongly to the fourth requirement; the remainder are more consequences of the way the standard has been written and are meant to aid interpretation and application of the standard.

4.1 Flexibility and Compliance

For many standards the notion of compliance is very clear-cut but it is much more subtle with DS 00-56 Issue 5, due to the need to enable the use civil standards as a means of achieving and assuring safety. There are a number of related factors that inform the compliance principle.

DS 00-56 Issue 5 is a goal-setting standard, saying what is to be achieved, and not how. Many standards are relatively prescriptive, e.g. IEC 61508 [7], but the use of goal-based approaches is not unprecedented; for example DO 178C [8] is objective-based. DO 178C does not define how the objectives should be satisfied, however the evidence needed to show compliance is quite specific, in part due to the use of a relatively large number of objectives (around 70 for the highest criticality). Arguments of satisfaction are either implicit or constructed with the regulator, by building on the available evidence (information set). In contrast, DS 00-56 Issue 5 has fewer goals, and a much wider scope.

The principle is that compliance with DS 00-56 Issue 5 is not (fully) established directly, but rather through defining and complying with a safety management plan (SMP). The SMP is intended to give a level of detail so that compliance to the plan is relatively clear-cut. However the word "fully" appears above because contractors cannot produce an arbitrary SMP; it must address all the relevant clauses of the standard.

To assist in its interpretation the standard includes, for the first time, data item definitions (DIDs) setting out the expected scope and content of the deliverables. In this context the SMP DID is the most important, but those for other deliverables, e.g. the SCR, help in interpretation.

This approach gives flexibility to the MoD and to contractors but also gives a clear way of judging compliance, once the SMP has been defined and agreed. This should be done, in part, by invoking relevant civil standards. Pragmatically this is essential to deal with the broad scope of acquisition scenarios, whilst giving a means of reducing uncertainty, and thus risk, for both MoD and industry.

4.2 Civil Standards

As indicated above, one of the key requirements for DS 00-56 Issue 5 is for contractors to be able to work to civil standards; this is an example of the way in which DS 00-56 Issue 5 is flexible, but also gives a way of being clear about "what is good enough", and what should be costed for in a bid. DS 00-56 Issue 5 requires that the use of such standards should be defined through the SMP, including dealing with any "gaps"

between the civil standards and the remainder of DS 00-56 Issue 5. For example, use of the key civil aerospace standards, e.g. ARP 4761A [9], would not result in the production of an SCR. Thus the SMP would need to include additional tasks to ensure (full) satisfaction of DS 00-56 Issue 5, see also the discussion of the "military delta" in section 6.

The use of civil standards has advantages, as outlined above, but also brings a number of constraints. In general, it means that the project has to adopt the "philosophy" of the chosen civil standard, e.g. the allocation of safety integrity levels (SILs) in terms of probability of failure on demand of a safety function in IEC 61508, or decomposition and allocation of development assurance levels (DALs) in ARP 4761A. Also, the civil standards often have explicit or implicit governance frameworks, and equivalent regulatory involvement/oversight is needed to avoid inappropriate use of the standard out of its normal context of application. Thus, whilst there are benefits of working to the familiar standards appropriate to a sector both in terms of economics and project risk, their choice is significant as it will shape the project, and give the effective basis for the judgement of compliance.

4.3 Risk Management and Safety Cases

In general, risk management and safety cases are the MoD's responsibility, and the contractor's role is to provide the information necessary to enable the MoD to discharge those responsibilities. This is one of the reasons for the introduction of the ISSS in Issue 5 of DS 00-56 but even where the contractor produces an SCR this is likely to be input to a larger safety case produced by the MoD, not stand alone.

The standard recognises that contractors have a broad obligation to reduce risk even where the scope of supply does not include a "complete" system and/or the contractor cannot make judgments about risk acceptance (e.g. under HASAW [10] section 6). This is stated explicitly to ensure that there is no difference in understanding between UK and overseas contractors. The standard also allows MoD to impose explicit safety requirements to enable it to address its obligations as an employer to, so far as is reasonably practicable, reduce risks (e.g. under HASAW section 2). This may include safety performance targets or targeted risk reduction obligations. The contractor would be expected to use recognised good practice, e.g. in terms of redundancy/diversity, built-in-test, etc. to manage failure modes. Clearly there may be debate about what is recognised as good practice, so it is important that the proposed approach is defined in the SMP.

It is envisaged that contractors will usually produce an ISSS and an SCR, with the balance depending on the scale of the PSS, the contractor's knowledge about operations, etc. For services, the contractor may need to produce an SCR (it is likely, but will depend on the scope of contract). The SCR would be expected to address the reduction of risk ALARP; in operating a service the contractor is taking (at least some) responsibility for operational risk, hence the need to comply with the ALARP principle. It is unlikely that contractors can demonstrate ALARP in other cases – although they should always consider risk reduction, as outlined above Note that, in some cases, e.g. CE marking, showing that risks are reduced ALARP is purely qualitative and does not require quantitative risk assessment.

4.4 Contract Definition

Contract definition will need to cover issues such as balance of risk/cost, access to competent skill sets, access to data, and so on. These issues are important, but outside the scope of the paper; we focus instead on those issues that are specific to the concepts and principles of DS 00-56 Issue 5.

As DS 00-56 Issue 5 is a very flexible instrument contract definition is crucial to effective application of the standard. The standard is designed for tailoring. For example, clauses can be removed if they are inapplicable. Unlike Issue 4, DS 00-56 Issue 5 covers the in-service phases of a system's life; thus if the contractor is not operating a system (providing a service) clause 15 would be removed; similarly clause 14 would be removed if there is no support (maintenance).

In order to work pan-domain, e.g. land, sea and air, DS 00-56 Issue 5 is quite generic and does not reflect sector-specific JSPs, nor does it reflect particular regulatory requirements, e.g. those imposed by the MAA or the DSEA. Thus it has been found useful to admit tailoring annexes to map the general requirements of DS 00-56 Issue 5 into domain-specific terms, and to adjust the details of the standard, as necessary. At present only an air sector annex is provided, although one for the naval sector is anticipated. The air sector annex includes the notion of a safety assessment report (SAR), which is used rather than an SCR or an ISSS (the SCR is viewed as being fully within MoD's sphere or responsibility, and it addresses the entire air system).

Technically, defence standards only apply on contract, but it is very important to consider the standard pre-contact in order to reduce project risk. In the case of DS 00-56 Issue 5 the key issues are the SMP and contract scope.

In tender documents it is to be expected that MoD will define both the scope of supply and scope of analysis. It would be reasonable for the contractor to suggest modification to these scopes, e.g. if they can expand the scope of analysis because of their domain knowledge. Thus the scope of contract is likely to be negotiated with the final decision on detailed definition resting with the MoD.

It is expected that a bidder will provide a draft SMP that will form the basis for running and monitoring the contract, if they are the successful bidder. At bid time it may not be possible to produce a complete SMP; for example the contractor may not know the full sub-contract chain, or they may not have visibility of government furnished equipment or information (GFX). Nonetheless, the more complete/definitive the SMP can be at bid time, the lower the risk for both parties.

4.5 Auditing

As with DS 00-56 Issue 4, the new issue of the standard places requirements on auditing, but the emphasis is different. Issue 5 introduces the notion of a contractor safety auditor

(CSA). The CSA will audit both the contractor and the supply chain, however there is still a requirement to allow reasonable access for an independent safety auditor (ISA). This is intended to be a specialisation of role, not replication of work.

There are two primary motivations for this change. First, the contractor has responsibility for the quality of his work (and that of his subcontractors), so should audit "internally" in any event. Second, if the CSA focuses on compliance with the SMP this allows the ISA to act in a more "value adding" role, considering the appropriateness of the SMP, including the way in which civil standards are used.

The standard does not seek to define or govern the ISA role (that is an issue for the MoD). However it is intended to help with the concept of reasonable access, as the ISA should, in principle, be able to access any aspect of the information set (not just the ISSS). This might be desirable, for example, to see which alternatives were considered in deciding that the chosen design was best, from the ALARP perspective.

4.6 Collaboration

Some systems are acquired in their entirety, but it is more common for systems to be acquired using multiple contracts. The standard has explicit requirements about collaboration dealing with situations where the development activities are being carried out contemporaneously, and where a contractor is relying on earlier work (e.g. acting as system integrator) or providing information for future work. The key requirements are in clause 9 of DS 00-56 Issue 5 and they are much more extensive than the equivalent clauses in Issue 4.

Issue 5 also deals with collaboration between contractors providing services, again largely via clause 9.

In all cases there will also be a need for collaboration with the MoD, see also section 6.

5 Pragmatics

There are a number of pragmatic issues involved in the use of DS 00-56 Issue 5; the aim of this section is to address two of the pragmatic issues that may significantly "shape" projects.

First, as MoD wishes to use OTS equipment so far as is practical, there may be cases when the OTS does not meet up to MoD's expectations for safety, or there is insufficient evidence that it does. The standard uses the term "shortfall" for the difference between achievement and expectation, whether it is in terms of product attributes or safety evidence, and includes explicit requirements about reducing shortfalls. This concept is also used for dealing with immaturity in design, in general, not just when dealing with OTS.

Ultimately there is a judgment whether or not a residual shortfall is acceptable. The position should be documented in an ISSS or SCR (or both), reviewed by the safety committee and escalated if necessary. The standard does not propose criteria for accepting or rejecting shortfalls; it cannot do so as it must be useable for all classes of system, in all domains. Again the SMP should be used to indicate how such issues would be addressed, but it is unlikely that the SMP can do more than clarify the decision-making mechanisms.

Second, some systems are acquired against multiple standards perhaps because they contain OTS elements from different domains, they include legacy elements initially acquired using now obsolete standards, or because they are pan-sector SoS which necessarily involve multiple standards. In all cases a means of mapping and resolving potential conflicts is needed, e.g. by making one standard or family of standards primary, by mapping SILs, by building separate compliance matrices against DS 00-56 Issue 5, etc. This again is a critical aspect of the SMP.

Finally there may be a "military delta", i.e. a significant difference between civil systems/standards and military needs or uses. Whilst resolving such differences is a pragmatic issue we return to it under observations, in the next section.

6 Observations and Lessons Identified

This section makes some observations on the issues in developing a standard such as DS 00-56 Issue 5 and presents some lessons which may help developers of other similar standards. It also makes some observations about the links between DS 00-56 Issue 5 and DS 00-55 Issue 5 (draft) [11].

Perhaps the biggest challenge relates to the boundary of applicability of the standard. It would be easier to write a safety standard for the "defence enterprise" relevant to any one system. Whilst it would be desirable to keep the standard goal-based, it would be possible to be much more specific and there would need to be less flexibility in the standard as all safety-relevant activities would be encompassed, and some of the subtleties about scope of analysis, ISSS, etc. would not be needed (or could be made much more focused). In short, the standard could be simpler and therefore easier to interpret and apply. As all defence standards are intended for contractual use there seems no obvious way around this issue.

Words are a problem. In principle, it is best to agree concepts first, then decide how they are best expressed afterwards; but it is hard to define concepts non-verbally, and considerable time was spent having apparently reached agreement on a key issue then realising that we hadn't. There were also concerns about introducing definitions or changing those used in previous versions of the standard, even where they could be made clearer. There is no simple solution to this, but using the Oxford English Dictionary and avoiding the temptation to be amateur lexicographers was found to minimise the issues.

Further it had been hoped that it would be possible to explore "scenarios", e.g. acquiring a modified OTS system for the air sector, to validate the standard whilst it was in development. Whilst a range of scenarios were captured, and were used implicitly to inform thoughts on the development of the standard, they were not used to explicitly test out the standard or provide examples of how the standard could be applied. It would not have been appropriate to include these exemplars in the published standard itself due to size considerations and the potential to misinterpret the exemplar as being definitive,

however the authors are of the view that the standard would be easier to interpret/apply if such scenarios were available as a separate resource. It is also believed that the risk of any shortfalls in the clarity of obligations in the standard could be reduced by exercising the standard on a benign test case rather than discovering it "live" on contract.

Standards should, ideally, be self-explanatory but they cannot be tutorials. (One of the difficulties with earlier versions of DS 00-56 was that people tried to treat them that way.) The use of the standard needs supporting via appropriate training (education should not be necessary, as only individuals and organisations with appropriate competencies should use the standard). Presentation material has been made available to interested parties, but this is an area where more needs to be done – although it is hoped that this paper will help.

DS 00-55, the MoD's software safety standard, was made obsolescent after Issue 3 of DS 00-56 was produced, but it continued to be one of the most widely downloaded defence standards. For this, and other, reasons it was decided to define a new version of DS 00-55 (Issue 3) to complement DS 00-56 Issue 5 which treats integrity quite generally, through five principles. DS 00-55 Issue 3 builds on these principles, and introduces some other concepts pertinent to DS 00-56 Issue 5.

DS 00-55 Issue 3, in its current draft form, talks about the "military delta" between civil and military use of PSS which generally results in shortfalls in product capability or safety evidence, when the military need is considered. It identifies the intrinsic shortfalls in using some civil safety standards, and sets out generic ways of dealing with such shortfalls. The same principles apply to the use of civil standards in the context of DS 00-56 Issue 5, and it may be that this will be addressed at Issue 6 (Issue 5 is interim, and the normal MoD process is to update from interim to full status after a period of time, e.g. a year).

Also, the current draft of DS 00-55 Issue 3 includes "open" as well as civil standards and provides guidance on their adoption in satisfaction of the DS' requirements, facilitating use of company standards where they are sufficiently open to scrutiny, e.g. by an ISA. Again there would be merit in "lifting" this idea to the parent standard, DS 00-56 Issue 5.

7 Conclusions

Developing standards is difficult; ensuring that the intent is communicated to the users of the standard is perhaps even harder. The aim of this paper was to set out some of the ideas behind the development of the standard to try to help in this regard. Whilst it does not act as a "clause-by-clause" guide it aims to clarify the core concepts and principles that underlie DS 00-56 Issue 5; it is believed that this is more conducive to understanding of the standard than a detailed commentary.

The paper has outlined some of the difficulties in developing the standard as well as explaining concepts, principles and pragmatics. One challenge not mentioned above was the large number of stakeholders – particularly different groups within the MoD – who had a view on key requirements, use of terms, etc. This made it difficult to progress certain concepts, and it was necessary to include the tailoring mechanisms to address different regulatory environments. With hindsight, issues such as the ability to tailor the standard are a significant benefit. The final conclusion is that it is desirable to engage all stakeholders as early as possible in a stable context. Greatest clarity was achieved when the whole stakeholder community was able to come together and agree on the objectives for the standard. However the changing nature of the organisations that comprised the community meant that some objectives evolved over the course of development. A more complete set of requirements sooner would have enabled faster progress towards a workable standard. The end result may have been little different although it may have been clearer.

Acknowledgements

The UK MoD funded the development of DS 00-56 Issue 5. The views and opinions expressed in this paper are those of the authors, not those of the MoD. The authors are grateful to the other members of the core team, Graham Joliffe and David Smith, the MoD, especially Paul Caseley and Peter Law, for their input, and to the broader community who made many useful comments on the evolving standard.

References

[1] UK Ministry of Defence, "Safety Management Requirements for Defence Systems", Defence Standard 00-56 Issue 4, June 2007.

[2] UK Ministry of Defence, "Safety Management Requirements for Defence Systems", Defence Standard 00-56 Issue 5 (Interim), January 2014.

[3] J. A. McDermid, "Evolution of the UK Defence Safety Standards", *in F Redmill et al (Eds), Current Issues in Safety-Critical Systems*, Springer Verlag, 2003.

[4] UK Ministry of Defence, "National Security Through Technology: Technology, Equipment, and Support for UK Defence and Security, Cm 8278, 2012.

[5] C. Haddon-Cave, "The Nimrod Review: An independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 Aircraft XV230 in Afghanistan in 2006, HC 1025, The Stationery Office, October 2009.

[6] Secretary of State for Defence, "Health, Safety and Environmental Protection in Defence", June 2013.

[7] International Electrotechnical Commission, "Functional safety of electrical/electronic/programmable electronic safety related systems". IEC 61508, Issue 2, 2009.

[8] Radio Technical Commission for Aeronautics, "Software considerations in airborne systems and equipment certification", DO 178C, December 2011.

[9] Society of Automotive Engineers, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment", ARP 4761a, 2009.

[10] Health and Safety at Work etc Act, available at: http://www.legislation.gov.uk/ukpga/1974/37/contents.

[11] See: https://www.dstan.mod.uk/drafts.html (draft of DS 00-55 Issue 3 for comment).