Reincarnation of Def Stan 00-55

Phil Williams, Engineer For Safety Limited; John McDermid, University of York

Def Stan 00-55 Issue 3 was released as an Interim standard in Dec 2014. It is currently under review with the intent of raising it to full extant status. This article presents some of the motivation and rationale behind its resurrection and update.

Why resurrect?

Defence Standard (Def Stan) 00-55 Issue 2 was issued in 1997 and made obsolescent in 2007. Nonetheless, since that time it has remained one of the most popular downloads and is clearly still found to be useful in the defence sector. The Ministry of Defence's (MOD's) Safety Standards Review Committee tasked a working group to investigate the need for a software safety defence standard and to provide options for its scope and approach.

Why change to procurement rather than development standard?

A review of the Def Stan 00-55 Issue 2 concluded that, whilst it was still seen as providing a basis for safety-critical software development, it had not been maintained and in some areas did not reflect current good practice. Also, UK MOD standardisation policy is to utilise civil European/International standards where practical[1], so there is an argument for moving away from Defence Standards where possible.

There are established standards and guidelines, such as DO-178C[2], that are widely adopted within their application domains and subject to ongoing maintenance, informed by a wide user base and scrutiny from regulators such as European Aviation Safety Agency (EASA) and the Federal Aviation Administration (FAA).

It is Secretary of State's policy that defence systems should achieve a level of safety that is at least as good as civil systems and that risks should be reduced as low as reasonably practicable[3]. For many defence systems it makes sense to benchmark against the nearest equivalent civil system, and this can include applying the recognised standards from that domain which, it is reasoned, will have been established to address the dominant risks in that domain. Of course, defence systems will have risks that are unique to the military application that need to be addressed (see 'the military delta' below).

The working group concluded that there were sufficient extant software safety standards and guidelines to cover the MOD's range of systems, and that there was nothing unique about defence software that warranted developing and maintaining a defence-specific standard. However it was recognised that there was a need to define how civil standards should be applied in the context of a military system, and in the context of the parent system safety management standard Def Stan 00-56 Issue 6.

Success Criteria

---

[1] See JSP 920 - MOD Standardization Management Policy: Civil, NATO, European, International or MOD standard; Defence Standard 00-00 Issue 2: A Standard for Defence Standards: Management and Production.

[2] RTCA DO187C, EUROCAE ED-12C, Software Considerations in Airborne Systems and Equipment Certification, 2011.

[3] JSP 815 Defence Health, Safety and Environmental Protection. Part 1: Directive

The working group proposed a number of success criteria for the standard:

Level playing field – Well constructed software should be acceptable, no matter where sourced. There is a perception that UK-sourced software is expected to be developed to higher standards than would be acceptable for software in an 'off-the-shelf' product from an off-shore supplier. Enabling the use of recognised civil (and international military) standards should avoid the risk of such over-expectation (whether real or only perceived). To do this, Def Stan 00-55 Issue 3 should focus on assurance, not development.

Transparency: It is important that the MOD knows what it is getting for its money. It is also important that suppliers know what they need to deliver to have their product accepted. Building on recognised standards and requiring up-front agreement of scope, basis and level of assurance, as well as of deliverables, should provide this transparency and allow both technical and commercial risks to be managed in the right places.

Maintainable: Software engineering is an evolving discipline. Thus, any standard needs to be maintained to ensure that it adopts recognised good practice and adapts to new technologies, or is written so that such advances can be incorporated without the need for change.

Familiar Techniques: A supplier's competence is typically based on experience in a domain where the defence market may only provide a small percentage of its overall business. It is likely that a better product would be obtained by enabling a supplier to apply a safety-management and software-development regime that is familiar, having been honed by their broader experience, rather than a regime that is novel and which requires them to use methods that are, to them, non-standard. It is expected that a competent supplier will have developed safety-management and development processes based around industry standards.

Concepts and Principles

An authoring team was put together to address these objectives. The team was selected to represent a mix of industry practitioner, independent safety audit, academic, scientific and customer perspectives. They agreed on a number of key constructs in the standard:

Software safety in system context: Safety is a property of the system in which the software is executed and in the operational context of that system's use. It is generally recognised, now, that software can only cause harm through its influence on the operational (physical world) context. Thus the standard for software safety assurance should be set in the context of a system safety standard that is used to determine the properties of that software that are important to safety and the degree of reliance on those properties. These translate to software safety requirements and a measure of required integrity/assurance. These need to be assessed coherently with the system-level safety criteria.

It is also necessary to recognise that the software development lifecycle is not necessarily the same as that for the top level system. Re-use of previously developed software, or software elements, means that software that contributes towards system safety has been developed before the system context was known. Further, software that defines the system's capability, or is used to provide system safety mitigation, will often be developed by suppliers to the main contractor, who may not have been selected at the time of main contract award.

4+1 (=5): With the MOD's policy towards use of civil standards, and the goal-based nature of Def Stan 00-56 Issue 6, an approach is needed that specifies what is required without defining how it is

to be achieved. The work performed by Hawkins et al[4] on principled software safety assurance offers a way to achieve this. An inspection of the most frequently used software standards show that they reflect (to a greater or lesser degree) the 4+1 (=5) principles presented in this work, and it is expected that any suitable standard used for the development or assurance of safety-related software should similarly support these principles. Def Stan 00-56 establishes 5 principles for assuring systematic integrity; these are carried forward into Def Stan 00-55 as objectives.

Objectives, requirements and criteria. The objectives in Def Stan 00-55 need to be demonstrably satisfied. As these objectives are expressed at a high level of abstraction, they need to be developed further into requirements and criteria that can be used as the basis for acceptance that the software satisfies the objectives. The 5th principle relates to the level of assurance appropriate to the desired integrity, and is the most difficult to specify without defining the development and assurance methodology. The standard does not define specific criteria, rather it relies on the criteria in the chosen civil standard.

Relying on the chosen civil standard comes with its own challenges. The correct application of the criteria, along with tailoring that may be permitted by that standard, is normally subject to a domain-specific governance regime. It is therefore important that the roles in that governance regime and the system context for the application of the standard are carried forward into the military domain's use of the standard. This may mean the use of a regulator or proxy-regulator to police the correct application of the civil standard and to provide definitive guidance on interpretation and tailoring, enforced through contracting provisions.

Scope

The working group decided that these 5 objectives applied equally to programmable hardware and, therefore, Def Stan 00-55 applies the term 'Programmable Element' to encompass software and all forms of programmed hardware.

It was also recognised that system safety is dependent on the data used by the system as well as the software that processes it. Further the 'correct' functioning of the software needs to be assured in all operating conditions, including where it is exposed to attack, whether incidental or targeted. The standard therefore includes consideration of cyber-security and data where they may contribute to safety but it does not address system security of itself. Guidance on data safety is still under consideration by the sponsor of the standard.

The Military delta

Employing civil standards maintained by a broad user base works well where the civil and military risks are essentially the same. However, the military tend to use products differently, so the risks may be inherently different. This may be because the operational imperative means that safeguards cannot be afforded (such as landing on sub-standard surfaces away from controlled airfields) or because the civil sector has no legal use for the product (as in the case of precision weaponry). In these cases it is necessary to review requirements of the civil standard. It is conceivable that the military use may permit a relaxation of the civil standard. More likely, the military use would exacerbate risks. In either case, it is necessary to show that the "military delta" has been addressed appropriately.

---

[4] Richard Hawkins, Ibrahim Habli, Tim Kelly: The Principles of Software Safety Assurance, 31st International System Safety Conference, Boston, August 2013.

Adoption of standards

Def Stan 00-55 Issue 3 provides guidance on the adoption of civil standards. It uses the term 'open standard'[5] as it is considered that a foreign military standard may be suitable, but it is also important to the UK MOD that any chosen standard is accessible to all stakeholders and that a supplier cannot hide behind proprietary claims to obscure a deficiency in the standard.

To provide an aid to initial use of the standard, a small selection of the most commonly cited civil standards has been considered further and adoption guidance provided within the Def Stan. Further standards could be addressed by future updates or additions to the MOD's acquisition framework (available to defence contractors through the defence gateway). As there are aspects of Def Stan 00-55 Issue 2 that are still considered to be good practice, especially for novel/complex safety-critical functions, it may be that aspects of that standard will be incorporated in Issue 3, by this means.

Competencies and the Supply Chain

Enabling the supplier to choose their adopted civil standard should facilitate optimum use of that supplier's competencies and experience in developing safety-related software. The flip side is that the customer and their advisors potentially have to be familiar with a broader range of standards. Def Stan 00-55 Issue 3 is intended to help to reduce the burden by providing a common underlying basis for assessing most standards, though it is inevitable that some 'devil will be in the detail'.

The burden for managing the supply chain, with the potential for different standards being selected throughout, rests with the main contractor to the MOD. It may appear that free choice throughout the supply chain enables maximum benefit in terms of flexibility and may be entirely appropriate where there are distinct sets of hazards (e.g. choice of aerospace standards for a host platform, and choice of IEC 61508 for the mission system that is hosted on the platform, or a mix of maritime, nuclear, mission, and aerospace standards on a nuclear powered aircraft carrier). However this introduces potential inconsistencies with the system safety standard and with reasoning about risk where multiple software elements contribute to the same risk. The Def Stan leaves it to the main contractor to justify their choices of standards, and to state how they will manage such potential issues.

Conclusions

Def Stan 00-55 Issue 3 is intended to remove some of the uncertainty that there has been in managing software assurance in the context of the later issues of Def Stan 00-56, as well as meeting some specific objectives such as giving a 'level playing field' for industry. It has done this by providing a framework for the utilisation of existing civil standards. Def Stan 00-55 Issue 3 does not remove the need for competency – it may even increase it – but it is intended that it enables competent staff to achieve and assure safety cost-effectively.

Caveat: The opinions stated here are those of the article authors and do not necessarily represent those of the MoD or the other members of the authoring team.

Phil Williams FIET is an independent system safety consultant having started his own consultancy in 2013 after 27 years with General Dynamics UK, where he held the role of Chief Safety Authority. He has supported a number of cross-industry system safety initiatives and has represented UK defence industry on the MOD's Safety Standards Review Committee and been a core member of the Def Stan

[5] Open Standards Principles Open Standards Principles: For software interoperability, data and document formats in government IT specifications, 1 November 2012

00-56 Issue 5/6 and Def Stan 00-55 Issue 3 authoring teams. He may be contacted at <phil.williams@engineerforsafety.co.uk>

John McDermid OBE FREng has been Professor of Software Engineering at the University of York since 1987, following earlier work for the MoD and in a software house. He has taught and researched extensively on aspects of system and software safety, and acted as a consultant for companies and government departments on several continents. He has undertaken a range of activities for the MoD, including acting as lead author on the production of Def Stan 00-56 Issue 6, and as a core member of the Def Stan 00-55 Issue 3 authoring team. He was awarded an OBE in 2010 for services to the defence industry. He may be contacted at <john.mcdermid@york.ac.uk>