

SOUP ... Why is it difficult to Cost?

An Assessment of Software Components for Safety Critical Applications

Introduction

The perceived advantage of using pre-existing components is that systems of improved capability and functionality can be developed at reduced cost. However, there may be considerable cost and technical difficulty in establishing with sufficient confidence that SOUP (Software Of Unknown Pedigree) is fit for its intended purpose in the safety application.

Background

Procurement of equipment often involves considering purchases from overseas. Such off-the-shelf (OTS) equipment is usually very competitively and, on the surface, very attractively priced in comparison with bespoke solutions. However, inevitably the equipment offered does not entirely meet the requirements of the in-service authority in terms of operating profile and environment. This leads either to compromise on functionality or modification of the delivered item. In either case, such equipment must pass through a certification process to provide confidence that it is safe to operate in the specified operational conditions. The OTS equipment will doubtless have undergone some form of certification process in its country of origin, but such certification does not necessarily conform to the UK requirements nor does it provide the evidence necessary for acceptance from a safety viewpoint. This is particularly true where software is used to fulfil a safety critical or safety related function.

Within the MOD, a Safety Case is required to provide evidence that equipment is adequately safe and fit for purpose. In the case of OTS equipment, such a Safety Case does not exist, nor is the evidence required readily available. The project office concerned therefore has to spend considerable time in attempting to acquire the evidence required, often being only partially successful. The Certification Authority therefore has to conduct some form of reverse engineering and usually detailed static code and timing analysis to gain the necessary confidence that the software in particular is adequately safe. There are considerable costs involved in undergoing the certification process in addition to an inevitable delay in bringing the equipment into service, which may in itself impose heavy financial penalties. Such additional costs incurred through OTS purchase may not have been considered in the initial tender evaluation process; nor does it appear that there is a reliable accumulation of appropriate data which would allow a realistic estimate of such costs to be made. This situation should be rectified by investigating the actual costs incurred in certifying OTS products and if necessary build in a certification factor into the tender evaluation process.

The complete OTS solution is not the only cause of concern over certification costs. Many projects are multi-national and there is often a compromise as to the standards applicable for development and later certification. Although there is a move towards the presentation of evidence that the end product is safe, the certification process is complicated by the lack of harmonisation of standards used by various suppliers. Furthermore, in a number of instances it is proposed to reuse OTS systems which have been developed and certified for a civilian environment; such certification is unlikely to be acceptable in a military environment and could lead to later cost and delays at the time of acceptance, unless these potential problems are addressed early in the project lifecycle.

In the case of future designs there is an increasing move to using COTS products. This appears very attractive financially and there is evidence of their reliability from a large user base. Even in the move towards Integrated Modular Avionics (IMA) there will be a need to use a COTS operating system. Needless to say, there are ways of reducing the risks associated with the use of COTS, but there is also an, as yet, unquantifiable cost in reducing risk to an acceptable level to meet certification requirements. It is important to investigate the cost of using COTS, particularly in a safety or mission critical situation, and to assess the advantage or otherwise of pursuing such increasing COTS utilisation.

Apart from failing to gain certification, the use of COTS (including OTS) products introduces many other risks for consideration over the lifecycle for the system. In production there is considerable risk that the product will fail to fully meet the technical requirements; this will mean the imposition of some limitations which may not be acceptable for certain operational scenarios. Support risks are numerous eg obsolescence, cost/difficulty of change, enforced change due to upgrades, belated discovery of inadequate reliability or undesired features etc. Over the lifecycle of equipment, the maintenance costs are by far the greatest component of overall cost.

A Study to examine the issues and scope the problem revealed **the following conclusions:**

- It is considered possible to estimate the cost of the elements which constitute the overall DEF STAN 00-55 process and therefore to cost the development of bespoke safety critical software developed in accordance with DEF STAN 00-55. This is subject to the normal constraints which apply to the costing of software generally.
- It is considered possible to estimate the cost of developing safety critical software based on modifying off-the-shelf software originally developed in a manner compatible with DEF STAN 00-55. This is subject to the normal constraints which apply to the costing of software generally.
- It is not considered possible to adequately estimate the cost of developing safety critical software based on modifying off-the-shelf software originally developed in a manner which is not compatible with DEF STAN 00-55.
- The requirement for safety criticality in software must be identified early in the procurement cycle to ensure that the development process reflects this as the 'retro-fitting' of the required integrity levels may not be feasible and is likely to be costly.
- The use of off-the-shelf safety critical software may be cheaper than bespoke development if modifications are confined to a limited proportion of the system and the software was originally developed using DEF STAN 00-55 processes. Otherwise the costs (and risks) of the off-the-shelf approach are likely to exceed a bespoke approach.

Recommendations:

- A methodology to relate the cost of individual elements of the DEF STAN 00-55 process to the analogous non safety critical elements is developed.
- This methodology is extended to encompass the activities required to modify off-the-shelf software originally developed using a DEF STAN 00-55 compatible process to meet safety critical requirements.
- Historical data concerning the costs of aircraft projects where safety critical requirements have been met using re-used software are collected and analysed to assist in the validation of the methodology referred to in the preceding two paragraphs and to establish a database that can be used to provide guidance on the cost of projects wishing to exploit re-used safety critical software.

The SOUP Study

The intention is to identify and propose solutions for practical ways of achieving the assessment, justification (in a safety case) and forecast of costs for SOUP used in safety related applications. Two aspects of SOUP are of interest :

1. Reuse of SOUP which was designed for a different safety application,
2. use in a safety application of SOUP which was not originally designed for safety.

Bob Anderton BSc. MSc. CEng. MRAeS Cert Ed. SPS/CF14c Software Cost Forecaster DPA
Abbey Wood, Bristol UK email: sps-cf14c@dpa.mod.uk Fax : +44 (0) 11791 32922.
Tel : +44 (0) 11791 32792.