SafSec: Commonalities Between Safety and Security Assurance

Samantha Lautieri, David Cooper, and David Jackson
Praxis Critical Systems
Bath, England
www.praxis-cs.co.uk
www.safsec.com

Abstract

Many systems, particularly in the military domain, must be certified or accredited by both safety and security authorities. Current practice argues safety and security accreditations separately. A research project called SafSec has been investigating a combined approach to safety and security argumentation, and has shown that there can be practical benefits in performing a combined analysis and documenting a combined argument for both safety and security.

1 Introduction

Where a computer-based system is required to meet rigorous standards of dependability, certification and approval costs can form a substantial proportion of the overall development costs. When such a system is maintained in service for an extended period, the cost of maintaining these approvals through in-service modifications and changes in operating environment escalates this element of cost still further. In an effort to manage and reduce certification and approval costs, the Defence Procurement Agency sponsored the SafSec (Safety and Security) project, which aimed to support safety and security accreditation of complex computer-based systems, particularly those now being deployed as Integrated Modular Avionics (IMA) systems.

SafSec focussed on two major issues: identifying and exploiting commonalities between the various disparate certification processes that an IMA system may be subject to, and providing a framework for certification of *modular* systems – those composed of standard components which are re-used in different configurations by a variety of applications.

This paper illustrates how commonalities exist in safety and security certification. When the commonalities are exploited, the effort and cost involved will be reduced and, if undertaken through a modular approach, issues of obsolescence will also be minimised, and possibly removed.

The resulting approach is called the SafSec Methodology and is the result of two years of research and case studies, involving a large number of stakeholders from the development, procurement and approval communities.

2 Background and Motivation

The acceptance into service of an Integrated Modular Avionic (IMA) system (ARINC 1997) presents a number of challenges which are not unique but which are perhaps more stringent in the avionics domain than in many others. The primary challenge is the need to satisfy a number of different accreditation bodies that a system is fit-for-purpose before operational clearance will be granted – this will generally include both a *safety* certification and a *security* accreditation. The second major challenge is the need to support modular certification; where components are shared between applications, we wish to be able to re-use elements of the evidence offered to support their acceptance.

Defence Standard 00-56 (MoD 1996) is the key UK MoD requirement for safety management; security accreditation will typically require meeting an approved standard such as the Common Criteria (ISO 1999). Neither of these standards, as issued at the start of the SafSec project two years ago, was entirely suitable for dealing with modular certification[1]. Methods for certification need to support the certification of modules in isolation and support certification of combinations of such modules, rather than expecting certifiers to handle large complex systems as monolithic items for certification. This becomes a key issue in the on-going maintenance of certification – changing a single element in a modular system should be straightforward, and we do not wish to have to revisit the acceptance case for the whole system whenever a single substitution is made.

Although the detailed requirements of safety and security acceptance are often different, sufficient commonality is visible in the acceptance processes to encourage us to seek cost savings by eliminating duplicate effort. Certifiers need to be presented with convincing, objective arguments that the system has the safety and security properties that are required. The methodology therefore must be based on the presentation of direct arguments, and supporting evidence, that systems have the necessary properties and behaviour, and don't have any undesirable properties, to be safe and secure. Underlying acceptance by either community is a demand for good engineering practice in matters such as requirements traceability, verification and validation, configuration management and change control.

Note that although the SafSec project was initiated in the context of IMA systems, the challenges described here are generally applicable to a much wider domain, and we have already received substantial interest from other domains.

---

[1] The recent drafts of the new issue of DefStan 00-56 adopt a more flexible approach than the current issue, and are thus supportive of the goals of SafSec. The MoD team working on the new issue were included in the stakeholders consulted by the SafSec project.