Modular Certification of Integrated Modular Systems

James Blow, Andrew Cox and Paul Liddell
BAE Systems, Warton Aerodrome
Preston, Lancashire, PR4 1AX

Abstract

This paper presents ongoing research into the modular certification of Integrated Modular Systems (IMS) within BAE Systems. An IMS is an open systems approach to the construction of systems from a set of standard hardware and software modules. Modular certification is the modular safety assessment of such systems. The aim is to reduce the certification costs of a system following a change to the system. To achieve this, a strategy has been proposed that is based on the concept of change isolation through the use of rely/guarantee contracts. The strategy advocates a more product-oriented approach to the development of safety cases for IMS.

1 Introduction

This paper discusses the modular certification of Integrated Modular Systems (IMS). IMS is an open systems approach to the construction of systems from a set of standard hardware and software modules, each of which has well defined interfaces.

It is often currently the case that the cost of re-certifying a system following a change is related to both the size and complexity of system and the size and complexity of the change. As systems increase in size and complexity the ability to identify and to justify that the minimum re-certification work necessary to ensure the required levels of safety have been maintained following change becomes increasingly difficult. This can prove to be very costly.

In order to address this, BAE Systems has developed a strategy for IMS that is based on the concept of change isolation. Such an approach should enable reduction in the impact of system size and complexity from the cost of re-certification such that, for a majority of change scenarios, the cost of re-certification is proportional to change size. This is achieved by minimising the level of architecture safety analysis required to re-validate and re-verify an IMS architecture within the overall system certification argument following a change.

The strategy proposes to use existing safety assessment techniques but to restructure the safety argument so that the IMS architectural aspects of the safety analysis are insulated from change. The impact of this strategy on lifecycle costs is

expected to be that initial certification costs are not expected to reduce, but the cost of re-certification is expected to reduce.

To be able to restructure the safety argument, however, requires an alternative to the existing process-oriented approach, where safety is determined by appealing to the quality of a recommended or prescribed development process. These techniques, while sufficient, are at the equipment level and consequentially system focused. Following a sizeable change the impact on system safety can only practically be assessed by the re-application of significant elements of the process to ensure all potential safety impacts have been assessed. This is potentially very costly.

To address this issue, the certification strategy primarily, but not exclusively, involves looking at the use of certification evidence, rather than its production, as is currently the case. In other words, a product-oriented approach is more likely to be successful. This is particularly true for military systems given the likely changes in Defence Standard 00-56 Issue 3 (which has not been formally issued at the time of publication) [Def Stan 00-56 1996].

By considering the evidence it is possible to structure the safety argument using modules. The IMS architecture components can then be generic and the safety and certification evidence associated with the architecture inserted into the overall system safety argument without demanding system wide re-validation and re-verification. Product oriented safety assessment is the application of best practice within the safety community.

Due to its product basis, the product oriented safety case will reflect the modularity of the proposed architecture. The safety dependencies that the components place upon each other should therefore be made more explicit to assist identification of a reduced re-qualification activity to support any particular change. This is achieved by the strict definition of interfaces between modular components of the architecture. For safety assessment, these module interfaces are defined in terms of rely/guarantee contracts, which describe guaranteed services to other modules based on assumed receipt of services.

The structure of this paper is as follows. Firstly, an overview of IMS is presented. The paper then looks at rely/guarantee contracts in some detail, including their development, definition, representation, composition, validation and violation. Their use, both by directly by engineers and within the safety argument, is also addressed. Finally, conclusions are made and future work detailed.

2 Integrated Modular Systems

A correctly used IMS architecture should enable effective management of system complexity, obsolescence, system upgrades and improved system availability.

IMS hardware consists of a number of Line Replaceable Modules (LRM) connected to a common backplane that provides electrical power and optical communication paths. The LRMs and backplane are housed in an enclosure called a rack, which provides cooling to the LRMs and a degree of protection from the external environment. For example a set of standard core processing LRMs might