Exploring the Possibilities Towards a Preliminary Safety Case for IMA Blueprints

Authors
Graham Jolliffe MSc CEng MRAeS;
QinetiQ, MoD Boscombe Down; Salisbury, Wiltshire, UK

Dr Mark Nicholson;
Department of Computer Science, University of York, Heslington, York, UK

Abstract

Keywords: Integrated Modular Avionics, Blueprints, Safety

The Aim of this paper is to show how a safety argument could be constructed for the use of blueprints in platforms using Integrated Modular Avionics (IMA). It is assumed that the IMA system will contain safety-critical elements. Given current safety analysis techniques, there is no certainty that this can be achieved satisfactorily.

Initially there is a need to define a blueprint: once this is done, the blueprints will be considered by looking at the impact of Blueprints on IMA Safety. The ultimate objective of IMA is to produce a reconfigurable system. Whilst this has potential safety benefits, there are substantial problems with the ability to argue that a reconfigurable IMA is safe. Consequently, this project will concentrate on a 3 Step Approach towards developing full IMA capability. The three steps are:

1. Fixed number of prioritised configurations (e.g. lookup table)
2. Ground (static) reconfiguration (between operations)
3. Dynamic reconfiguration

This approach is progressively more complex, but will enable confidence to be gained from success at each step. The safety argument that is produced in this paper is generic and has been produced as part of an MSc project. However, the overall IMA safety argument needs to consider many other issues and factors, which may affect the safety of blueprints. This is not covered in this paper, but is expanded in more detail in the MSc project (Jolliffe 2004).

1 Background

Before describing the background to this paper, it is worth spending some time explaining what IMA is and, importantly, providing a definition for an IMA blueprint. Most current avionic architectures are federated systems with each function located within its own processor or Line Replacement unit (LRU), connected to each other by an avionics data bus. A typical federated system is shown in the diagram below (Fig 1) (Kemp 2000).

IMA is a term to describe a distributed real-time computer network aboard an aircraft. This network might consist of a number of computing modules capable of

supporting many applications, which in turn may have different safety criticality levels.

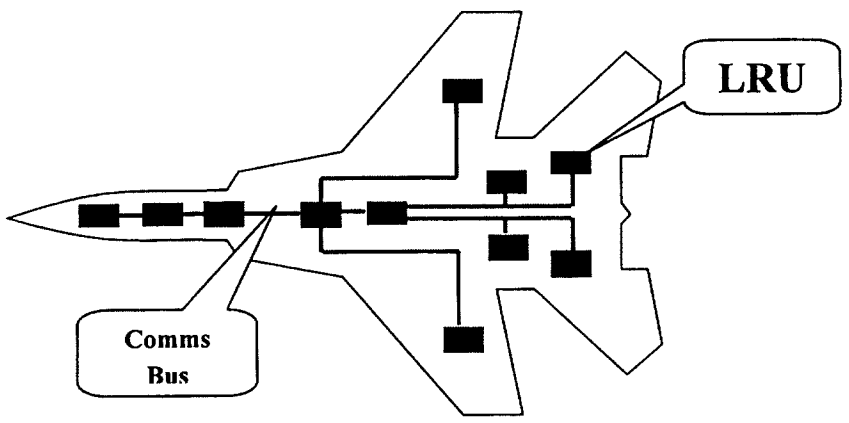

Figure 1 Typical Federated System Architecture

The diagram below (Figure 2) (Kemp 2000) shows what a typical IMA architecture might look like. Each module contains an application that 'services' either a sensor or output or both. A common shared network connects the sensors, modules and outputs.

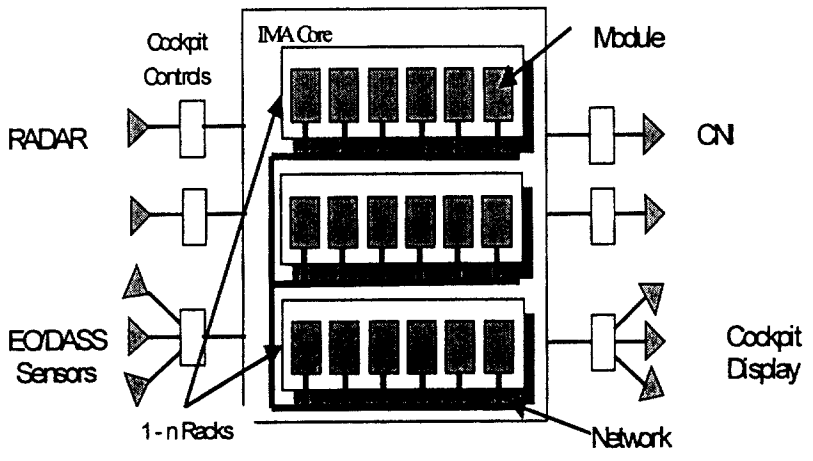

Figure 2 Possible IMA System Architecture

There are a number of benefits in progressing towards this type of architecture compared with that shown in Figure 1. The civil and military sectors have already clearly identified the benefits of IMA and (Kemp 2000, Conmy 2003, Tudor 2002, Aviation Today Magazine Website 2003, MoD ADAS(Air) Website 2002, and