Health Monitoring for Reconfigurable Integrated Control Systems

Dr Mark Nicholson
Department of Computer Science, University of York
York, England

Abstract

The next generation of control systems are likely to be characterised by much higher integration, where common / shared computer resources perform multiple system functions. It is possible to reconfigure such systems to provide continued functionality when an element of the system fails. To achieve this aim a number of pre-requisites must be in-place: the ability to determine when a failure has occurred, the appropriate configuration to move to and the ability to safely transfer from one configuration to another. This paper concentrates on the first of these in the form of health monitoring systems for IMS. The approach takes into account the potentially safety critical nature of the applications and the nature of these computer systems.

1. Introduction

Most current control system architectures, such as avionics systems, are federated systems with each function located within its own processor and connected to each other by a data bus. Integrated Modular Avionics (IMA) (EUROCAE 2004) is a term to describe a distributed real-time computer network aboard an aircraft. This network consists of a number of computing modules capable of supporting many applications, which in turn may have different safety criticality levels. One possible IMA architecture is presented in Figure 1 (ASAAC 2002). Each module contains an application that 'services' either a sensor or output or both. A common shared bus network connects the sensors, modules and outputs. Other domains, such as the automotive sector, have also looked at the concept of IMA. Thus, in this paper the more general term Integrated Modular System (IMS) is employed.

Reconfiguration is the capability of a system to adapt its functionality to the changing conditions of its environment (Trapp and Schurmann 2002). One such event could be a change in the mode of operation of the system, such as a move from the initialisation mode to the running mode. Another event that may be addressed via reconfiguration is a failure of one or more elements of the system. This could be a hardware, software or logical failure. This implies that the system has the ability to adapt its behaviour in the presence of faults to achieve continued safe operation and graceful degradation. Limited reconfiguration capability already exists in federated systems but the potential is much greater in IMS. Thus one of the benefits of moving to IMS is the ability to reconfigure the system in response to a range of triggering events.

One current approach to failure management in a federated system is to employ redundancy; that is to employ multiple copies of a system element. In the long term it may be possible to trade-off the level of redundancy employed in a safety related control system with the ability to provide "reconfiguration on failure".

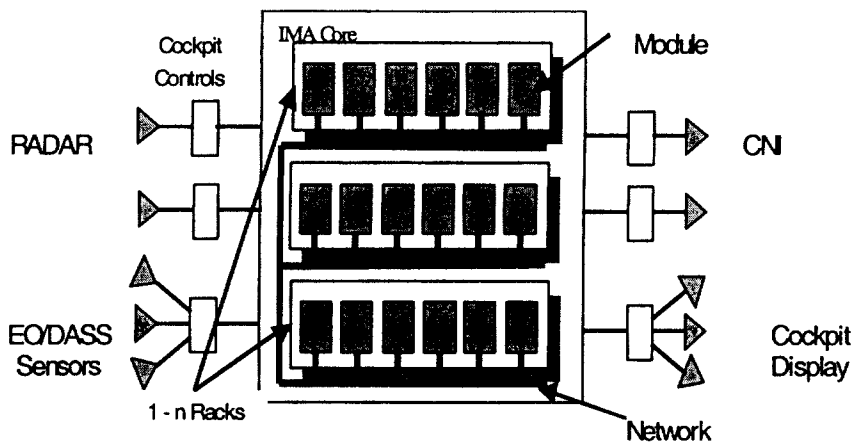

Figure 1: ASAAC Architecture for an IMA radar system

If "reconfiguration on failure" is to provide effective fault-management the ability to determine when a reconfiguration should take place is required. To accomplish this the concept of health monitoring needs to be adapted and extended to take into account the potentially safety critical nature of the applications placed on the IMS platform and the characteristics of IMS computer systems. Health monitoring (HM) is the ability to identify the failure of one or more system elements. Historically, health monitoring has been used to provide maintenance-related failure data for mainly mechanical systems. For instance the F22 flight critical systems have extensive self-diagnostics and built-in testing capability for the various subsystems (Globalsecurity 2004). There are more than 15,000 fault reports available for the avionics systems. Most of these are low-level fault reports that do not result in warnings or degrade the operation of the aircraft.

In IMS health monitoring could be the function responsible for monitoring the system to detect, and report hardware and software (application and operating system) faults and failures. The fault management part of the IMS then uses this information to determine the appropriate system level response, such as reconfiguration. Thus, an ability to detect, and handle failures in such systems become requirements that the system must comply with in order to meet safety objectives. One of the decisions that must be made for instance is which combinations of failure reports will lead to a reconfiguration. Furthermore a decision must then be made as to how extensive the reconfiguration will be. Safety implications accrue if either of these decisions is incorrect.

In Section 2 the concept of a configuration of the elements of an IMS is introduced. Reconfiguration mechanisms are then discussed with reference to the requirement to be able to safely reconfigure a system on failure. The elements of a