Verification of embbeded systems with preemption: a negative result

Jérôme Ermont*, Frédéric Boniol*

*IRIT-ENSEEIHT, 2 rue C. Camichel. F31071 Toulouse, France
{frederic.boniol,jerome.ermont}@enseeiht.fr

Abstract. The aim of this article is to explore the problem of verification of preemptive communicating timed processes, i.e., timed processes which can be suspended and resumed by an on-line scheduler. The contribution of the article is to show that this problem is unfortunately undecidable. We discuss then an alternative verification method to overcome this negative result.

1 Introduction

Embedded systems often are characterized by the two following properties. Firstly they are an information processing sub system of their embedding systems. Secondly they are reactive, i.e. they interact with their physical environment at a speed imposed by the environment. Consequently, they have to meet both real time and safety constraints. These characteristics make writing embedded software a substantially different and more difficult task than classical software. To overcome this complexity, the avionics architectures traditionally being implemented are of federated, which means that each avionics system has its own independent and dedicated computing and communicating resources. Federated architectures have great advantage of inherent fault containment. Systems implemented by dedicated resources are loosely coupled allowing modular design and verification.

However, federated architectures are penalizing due to massive use of isolated resources, and results in increase in weight, maintenance costs, power consumption, etc. Due to these drawbacks, the aviation industry is gradually moving towards the use of Integrated Modular Architectures (IMA) for both civil and military aircraft programmes. Instead of using individual resources, IMA uses generic computing and communicating platforms. This allows multiple applications to share and reuse the same computing and communicating resources concurrently. This facilitates a reduction in the number of deployed subsystems which are not fully utilised and provides a more efficient use of system resources, leaving space for future expansion. This is the case of modern aircraft such as Airbus A380, Boeing B777, or Euro Fighter aircraft. Each function is allocated to a shared computer. Scheduling of functions is managed by an embedded real time operating system. Communications between computers are supported by multiplexed data buses (Boeing B777), or by switched communication networks (Airbus 1380), and are scheduled by real time communication protocols. The main advantage of such an organisation is to offer a modular view of the global system. However, the use of shared computing and communication resources introduces non-deterministic jitters and delays, which can affect the global behaviour of the system.