OASIS formal approach for distributed safety-critical real-time system design

Jean-Sylvain Camier, Damien Chabrol,
Vincent David, Christophe Aussaguès

CEA, LIST
BP 65, GIF SUR YVETTE CEDEX, F-91191 FRANCE
firstname.lastname@cea.fr

Abstract. OASIS provides an environment for real time multitasking and communication design, as well as an execution environment based on a safety oriented embedded real time kernel. The formal approach of real-time design avoids many difficulties: it allows implementing efficient advanced real-time functionalities without any safety loss. The concepts and methodology presented in this paper ensure the most important safety properties. Within this framework, our goal is to rely on formal and algebraic tools that can automatically bring the proof of correctness for safety-critical design issues. Such a constructive approach can easily speed up the system development by the formalization of the off-line analysis.

1 Introduction

In most key industries which require high dependability systems, distributed real time systems have found widespread use to ensure safety critical functions. In a distributed system, consisting of several independent nodes communicating via a network, the architecture of the communication network is the core of the system, and strongly conditions the capability of the system to fulfill the real time and safety requirements (Shin, 1994). It is a major difficulty to obtain a complete deterministic safety critical real time system conforming with very high safety requirements and allowing both rigorous and flexible development, including verification and validation. Providing these properties to a system has often been possible only by the use of specific hardware. Our contribution leads to the definition of a constructive system engineering approach that can deal with deterministic, fault-tolerant, safety critical real time distributed architectures on standard hardware.

To prepare the next generation of sensitive systems or embedded systems in transport and energy domains, our contribution is based on the OASIS approach developed by the CEA (French Atomic Energy Commission) and AREVA-NP (Nuclear Power Firm), in cooperation with EDF (Electricité de France). This approach provides rules and methods to design and implement safety-critical real-time systems over single processor architecture (Aussaguès and David, 1998). Work has been carried out to extend OASIS to distributed architectures. A deterministic and real-time protocol based on TDMA and its optimized version, called A-TDMA have been developed complying with the time-triggered context of OASIS.