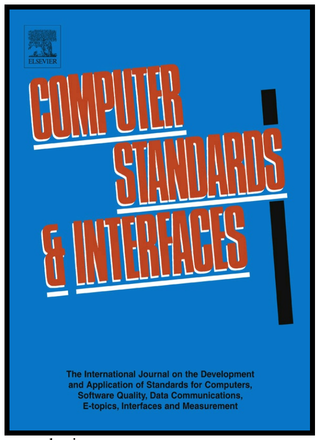
Author's Accepted Manuscript



www.elsevier.com

Handling heterogeneous partitioned systems through ARINC-653 and DDS

Héctor Pérez, J. Javier Gutiérrez

PII: S0920-5489(16)30136-2
DOI: http://dx.doi.org/10.1016/j.csi.2016.10.012
Reference: CSI3158

To appear in: *Computer Standards & Interfaces*

Received date: 20 February 2016
Revised date: 20 October 2016
Accepted date: 21 October 2016

Cite this article as: Héctor Pérez and J. Javier Gutiérrez, Handling heterogeneou partitioned systems through ARINC-653 and DDS, *Computer Standards &* *Interfaces,* http://dx.doi.org/10.1016/j.csi.2016.10.012

Handling heterogeneous partitioned systems through ARINC-653 and DDS

Héctor Pérez *and* J. Javier Gutiérrez
Software Engineering and Real-Time Group, Universidad de Cantabria, Santander, SPAIN
perezh@unican.es
gutierjj@unican.es

Abstract
Many cyber-physical systems in the avionics domain are mission- or safety-critical systems. In this context, standard distribution middleware has recently emerged as a potential solution to interconnect heterogeneous partitioned systems, as it would bring important benefits throughout the software development process. A remaining challenge, however, is reducing the complexity associated with current distribution middleware standards which leads to prohibitive certification costs. To overcome this complexity, this work explores the use of the DDS distribution middleware standard on top of a software platform based on the ARINC-653 specification. Furthermore, it discusses how both technologies can be integrated in order to apply them in mission and safety-critical scenarios.
Keywords—distributed systems; middleware; ARINC-653; hypervisor; DDS; real-time systems.

1. Introduction

Over the last years, the avionics industry has been evolving to adopt the integrated modular avionics (IMA) architecture to simplify the development and certification of onboard software. One important aspect of this architecture is the ARINC-653 specification [1], where the partitioning concept can provide applications with strong temporal and space isolation, thus easing their verification, validation and certification [2]. In this context, the term partition represents a kind of container for one or several applications that is allocated to one or several dedicated time windows during which the partition may execute. Different design alternatives exist for implementing partitioning, but the virtualization approach presents high potential and it is attracting an increasing interest in the community [3]. Virtualization allows different execution environments to be executed in the computing platform or *core-module*, and therefore it provides flexibility in selecting the most appropriate operating system for each partition. For instance, a real-time operating system for partitions with hard real-time requirements, or a general-purpose operating system which enables partitions to take advantage of the high-availability of software resources. As a result, this approach envisages the possibility of using commercial-off-the-shelf (COTS) software (e.g., standard distribution middleware) for improved reuse and cross platform interoperability.

Inter-partition communications often rely on a message-passing mechanism which provides IMA with decoupled and static data communications. However, recent advances in distribution middleware can benefit modern avionics systems with robust, flexible and interoperable communication services [4]. One major effort in this direction is the Technical Standard for Future Airborne Capability Environment (FACE) [5], which aims to standardize approaches based on open standard solutions for airborne systems. Among others, FACE includes the Data Distribution Service for Real-Time Systems (DDS) [6] as a suitable candidate to provide distribution capabilities within avionic systems.

The DDS standard is based on a loosely-coupled, data-centric publish/subscribe communication paradigm with support for a rich set of quality-of-service (QoS) policies. A fundamental benefit of DDS is to facilitate the integration of software applications without concern for the underlying operating system or programming language. This is worth considering when integrating large heterogeneous systems where no single software supplier is sufficient, as usually happens in avionics. Furthermore, the DDSI-RTPS interoperability protocol [7] allows the interoperation of different middleware implementations and the connectivity with open system architectures. These features make this standard an enabling technology for the development of distributed real-time systems in different domains such as cloud environments [8][9] or cyber-physical systems [10]. However, the use of DDS in safety-critical systems is still an open challenge that is currently being addressed through the extension of DDS with a safety-critical profile [11][12] suitable for partitioned systems. When finished, future mixed criticality applications could leverage both standard DDS and certifiable DDS configurations.

The similarities between the DDS messaging service and the one defined by ARINC-653, together with the QoS parameters provided to control non-functional properties, open up the possibility of using both technologies in future distributed real-time embedded systems that may require a more cost-effective software development and integration. An