

Call for papers submission – ESA Software product assurance workshop 2023

Title: WCET and Critical Applications: Learning from civil aviation

Keywords: WCET, Worst Case Execution Times, Critical, CAST-32, A(M)C 20-193, Multicore

Abstract:

It is an unfortunate fact of life that the need for radiation hardening means that hardware technological advances are invariably made available to the space sector long after others have seen the benefit. The flip side is that others have typically dealt with many of the downsides before this sector has a need to consider them!

The issues surrounding the use of Multicore Processors (MCPs) for safety-critical applications are typical of that phenomenon. Despite the huge improvements they promise in terms of Size, Weight, and Power (SWaP), the challenge of reliably budgeting for time-critical tasks running on MCPs has long been a bar to their application in civil aviation. CAST-32A and its successor documents (collectively known as A(M)C 20-193) captured the issues faced quite succinctly in terms that are just as applicable in space.

Even for a single core, the calculation of a worst-case execution time (WCET) through static analysis alone can only ever be an estimate. That problem is exacerbated when more than one core is involved, where shared resources such as memory and caches further degrade the theoretical calculation. In an environment where precise timing can be mission-critical, approximations do not sit comfortably.

This paper will argue that adopting the recommendations of CAST-32A & A(M)C 20-193 presents the most pragmatic approach to achieving the necessary assurances, and it will present a pragmatic approach to applying them in practice.

Presenter:

Chris Tapp is a Technical Specialist at LDRA with more than 20 years' experience of embedded software development. He graduated from the University of Durham in 1987 and has spent most of his career working within the automotive, industrial control and information technology industries, mainly as a self-employed consultant. He has been involved with MISRA since 2001 and is currently chairman of the MISRA C++ working group and an active member of the MISRA C working group. He has been with LDRA since 2007, where he specializes in programming standards.