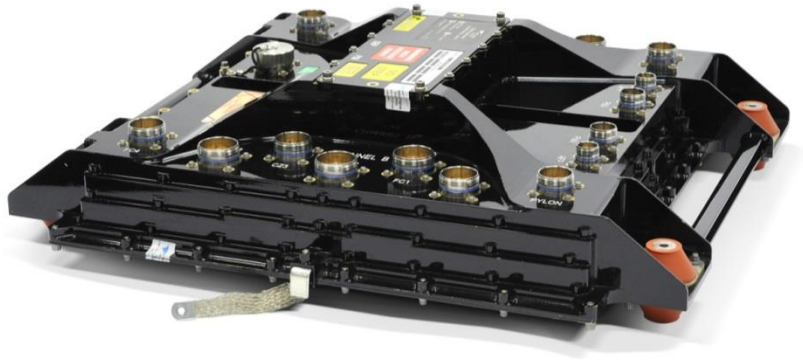
Industrial Application of Measurement Based WCET

Stephen Law

controls and data services
Part of the Rolls-Royce Group

Introduction

- CDS develops aircraft engine control systems, predominantly for Rolls-Royce
- The software, **written exclusively in SPARK-Ada**, is developed according to DO-178B & C guidelines, DAL A
- Worst Case Execution Time (WCET) Analysis is a key verification activity for real-time systems.
  - Static Analysis
  - Measurement Based Analysis



controls and data services
Part of the Rolls-Royce Group

Our History

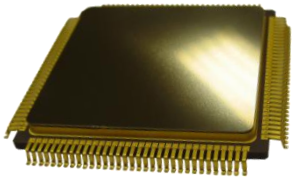
MIPS = Million Instructions per Second

VISIUMCORE
MCM (~100MIPS)

Goodrich GR5 MCM (40 MIPS)

Hi-Core (20 MIPS)

68020 (5 MIPS)



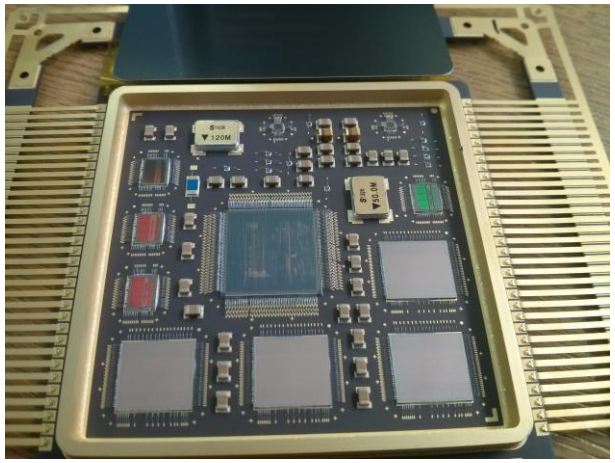
Zilog Z8002 (1 MIPS)

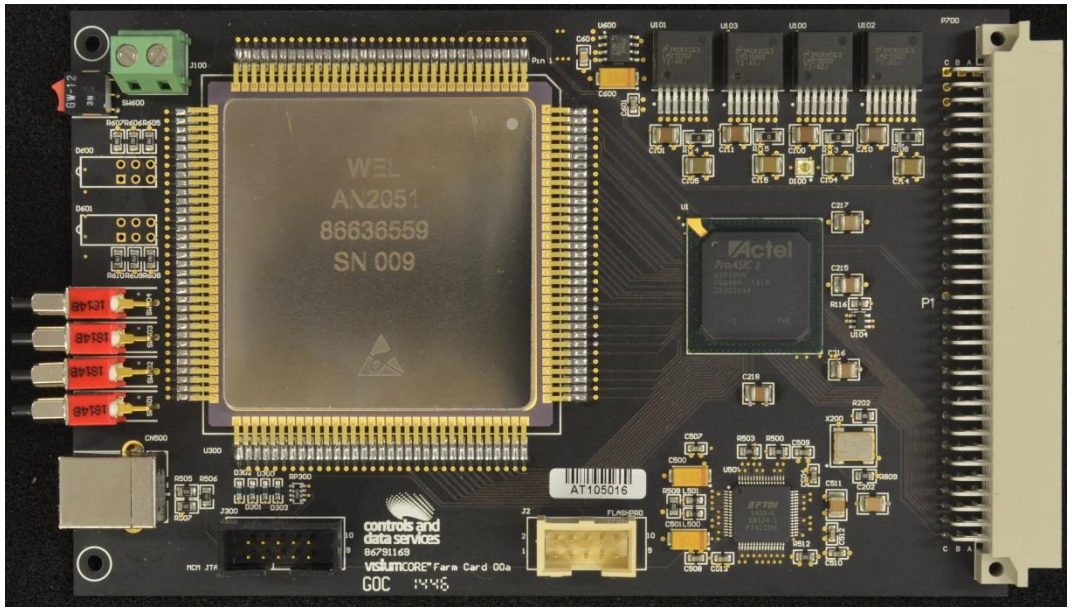
1984 1995 2000 2010 2018

controls and data services
Part of the Rolls-Royce Group

The **VISIUM**CORE

- The **VISIUM**CORE, the latest iteration of the CDS processor, is designed specifically for software development in a DO-178C/DO-254 context





controls and data services
Part of the Rolls-Royce Group

The **VISIUM**CORE

- The **VISIUM**CORE, the latest iteration of the CDS processor, is designed specifically for software development in a DO-178C/DO-254 context

  - Five-stage superscalar architecture featuring managed out of order execution
  - Time invariant instruction execution
  - Static branch prediction logic
  - No instruction or data cache
  - Independent instruction/data memory access/control
  - In-built trace output logic, provided through an independent execution unit and special tracing instructions
    - Each RapiTime instrumentation overhead <1 cycle.

  - Obsolescence avoidance – support for at least the next 20 years
  - Extensive SEU protection, detection and correction.

Industrial WCET Key Challenges

- Accurate WCET results, not optimistic, not overly pessimistic
  - A robust and reliable method, that meets CAA/EASA/FAA requirements
- Integrates into existing test strategy, build process, and able to analyse legacy software
- Scalable to a substantial project*
- Able to analyse at the component level
- Optimised code

**What scale are we looking at?*

A typical project consists of approximately 4000 individual component test scripts, which have been written over a 10 year timeframe

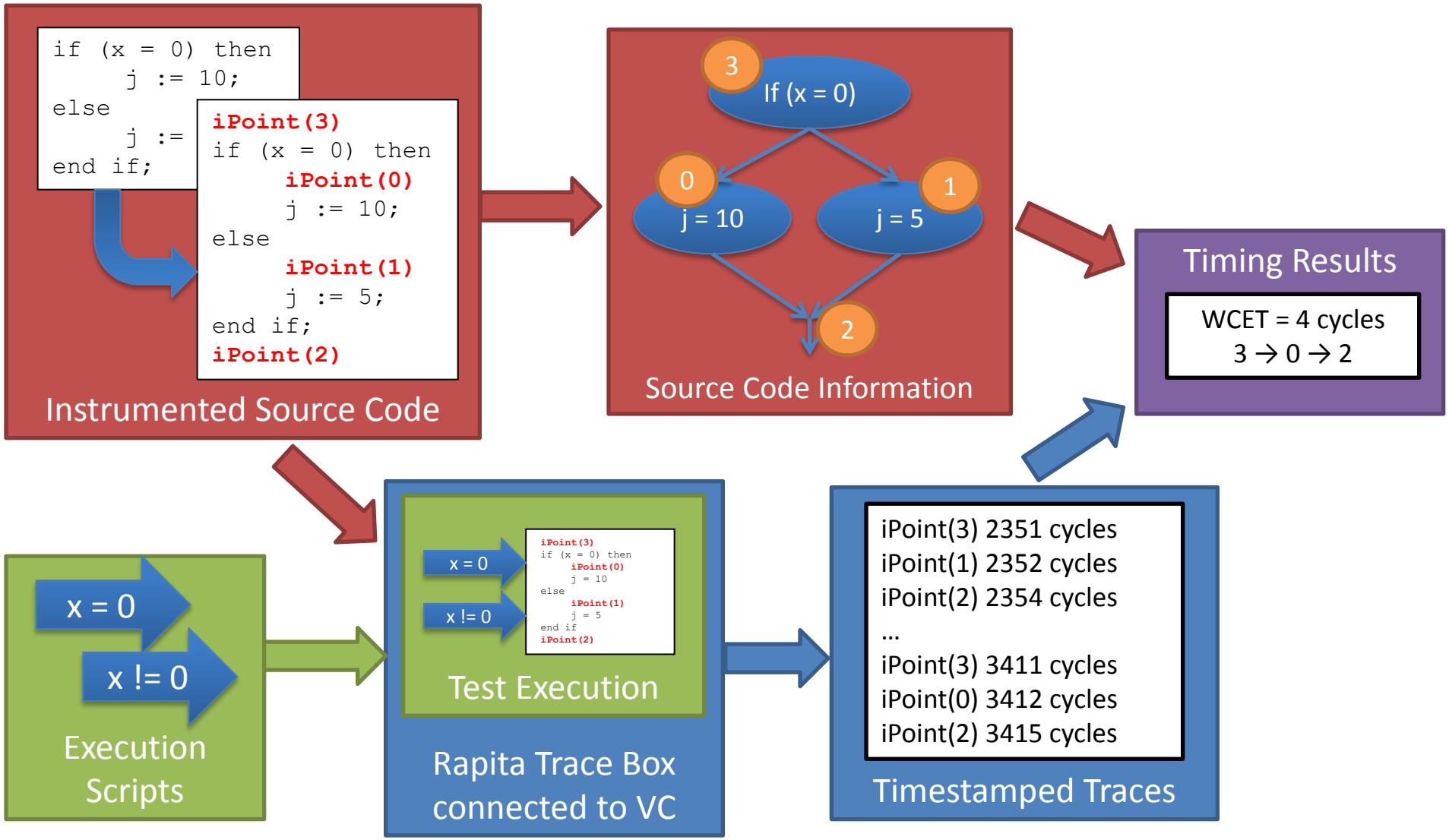
CDS Chosen Approach

- Software targeting the **VISIUM**CORE will be analysed using RapiTime, developed by Rapita Systems Ltd

- The solution offered easy integration with our processor, and our existing processes and software

- The tool is integrated with our existing low level testing (LLT) infrastructure
  - Completely automatic execution, controlled by existing LLT scripts
  - This allows testing to be performed on a single processor, long before full target hardware is available

- Minimal changes required to existing components:
  - Less than 1% of code items had to be altered
  - Less than 5% of test scripts required updates



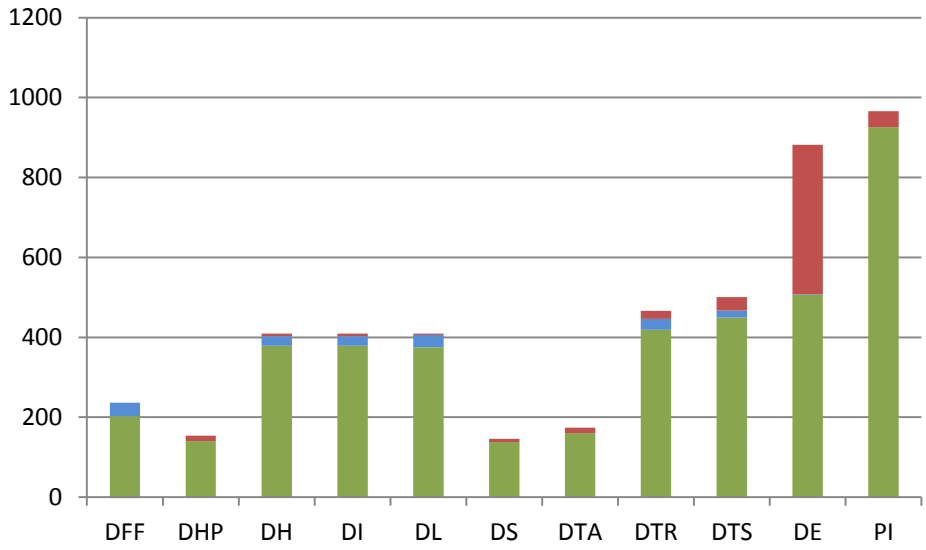
controls and data services
Part of the Rolls-Royce Group

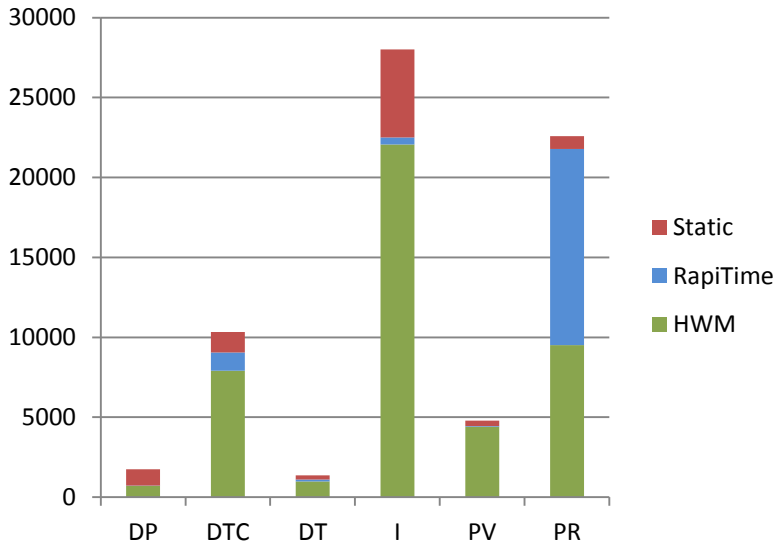
Argument for Suitability and Correctness

- ***A software architecture amenable to analysis***
- ***Extensive coverage provided through low level component tests***
- ***A processor architecture designed for analysis***
- ***Comparison between code under test, and code in the final system***
- ***Combining unit tests to provide a system level result***

Initial Results

- An initial study tested the tool against an in house static analysis tool, targeting a previous version of the CDS processor





- Following the initial study the tool was trialled on the **VISIUM**CORE processor targeting two CDS engine controller projects
  - 8000 tests, all compared to HWMs

controls and data services
Part of the Rolls-Royce Group

Conclusion

- RapiTime has been integrated as part of the CDS build and test process with minimal change required
- First adopting project now using the tool to generate certification artefacts
- The technology has been validated through a extensive study that has demonstrated acceptable WCET results and a viable process in a representative environment
- Future work:
  - Automatic software execution, aiming to reduce the tool's reliance on test scripts
  - Working with Rapita investigating ways to reduce the overhead introduced by instrumentation

Questions … and Our History

MIPS = Million Instructions per Second

Lucas

TRW

GOODRICH

Rolls-Royce

Aero Engine Controls

Osys

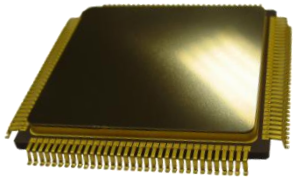
controls and data services
Part of the Rolls-Royce Group

VISIUMCORE
MCM (~100MIPS)

Goodrich GR5 MCM (40 MIPS)

68020 (5 MIPS)

Hi-Core (20 MIPS)



Zilog Z8002 (1 MIPS)

1984 1995 2000 2010 2018

controls and data services
Part of the Rolls-Royce Group