Aero Engine Controls

A Rolls-Royce plc and Goodrich Corporation joint venture

GCC GNAT Ada in jet engine control systems

Peter Garbett

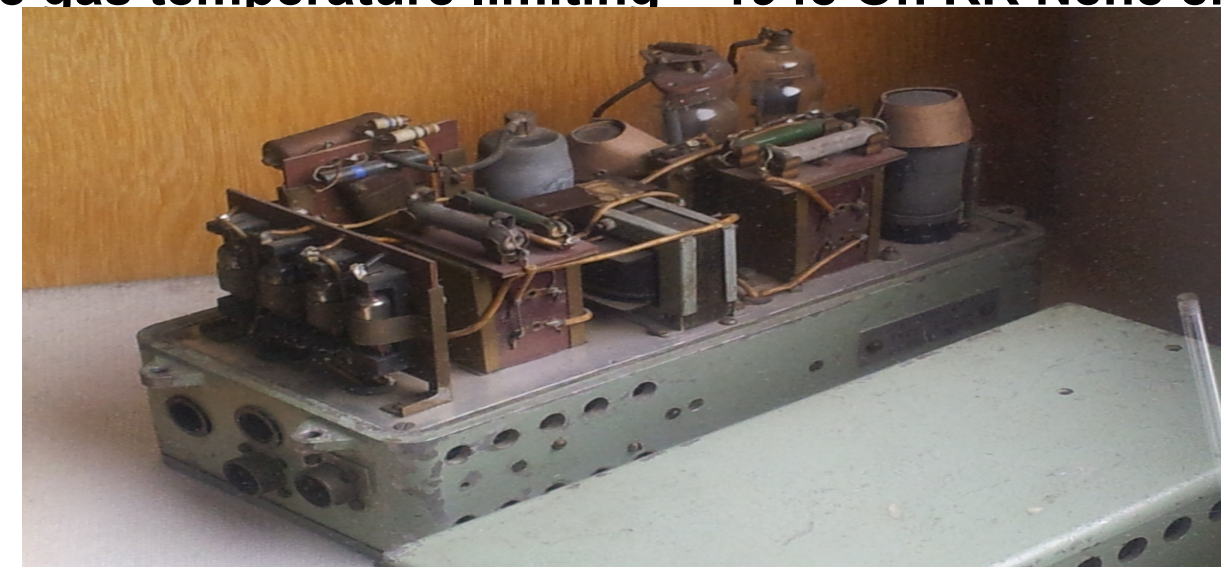
People you can count on, products you can trust.

Historical Background

- Goodrich part of JV in Birmingham U.K used to be part of Lucas industries, founded by Joseph Lucas (1834-1902) [0].
- Lucas Industries solved early (1940's) jet engine combustion problems with help from Birmingham Gas Company. [1,2]
- Birmingham's association with gas burners probably starts with William Murdoch in 1790's. [3], Lucas made paraffin lamps and electrical gear.
- Lucas supplied combustion and fuel system for the world airspeed record by the Gloster Meteor: 615.78 mph 1947 [4]
- From inception, gas turbine engines pose controllability problems
  - Flame out
  - Surge
  - Turbine temperature overshoot

Historical Background

- Many systems implemented using hydro mechanical controls.
- We are interested in the electronic ones, they also have a long history. For example:
- Turbine gas temperature limiting – 1948 On RR Nene engine

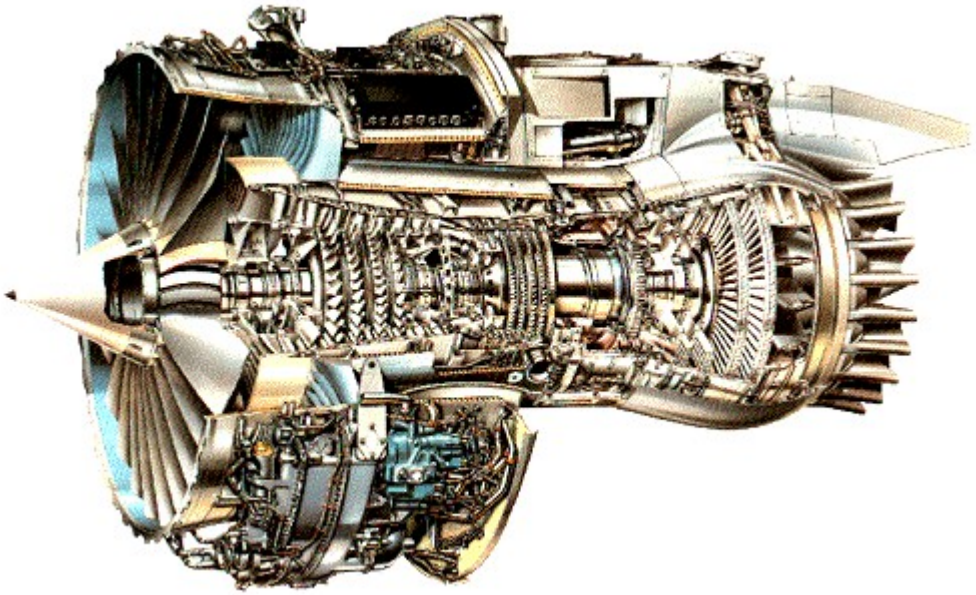


Development of digital controls

- Lucas Aerospace did Analog and later digital engine controls for MRCA tornado (as did MTU [5])
- World's first flight of digital control with 'full authority' on Olympus 593 powering Concorde [6]
- More control aspects - Afterburner pressure matching and resonance damping
- Dual lane with multiple levels of redundancy. Complex input data validation.
- Large scale introduction of civil engine controls circa 1989 with 747-400,and 737-300 on RB211-524G, and others in USA.

Where our computer lives

- **An RB211-524G, gearboxes, pumps at bottom, our control unit on top. [7]**



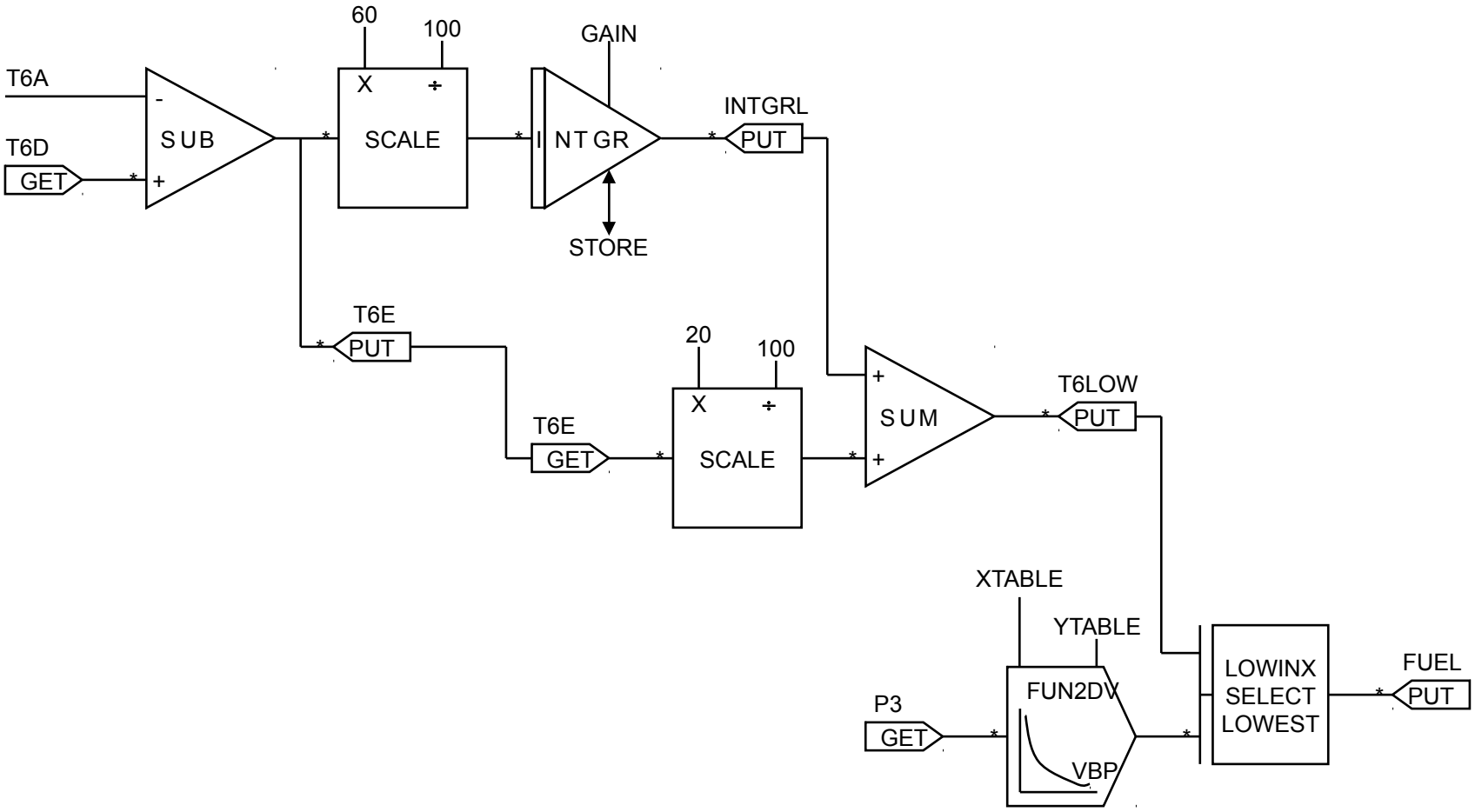
Where our computer lives

- **Our units face environmental challenges [9]**

Digital controls pre-Ada

- Custom tools for software development – LUCOL. Threaded translation from control oriented language, building blocks 'modules' of assembler with extensive dynamic testing and also formal proofs of correctness. [10,11]
- Properties of the system:
  - Object code stability. Software changes could be localised and analysed as delta changes.
  - Amenable to timing analysis; loops hidden in proved components.
  - Easy to interface to external test harnesses; variables in fixed addresses, limited use of local variables.
  - Easy to ascertain level of structural coverage.
  - Trivial mapping between control requirements and software.
  - Trivial stack analysis
  - Targeted at a particular domain.

Target domain for LUCOL



Aero Engine Controls

Development of Safety critical Ada engine control

- Why adopt Ada?
- Control part of systems becoming less dominant. More maintenance information input validation , communications etc.
- DoD pushing adoption of Ada.
- SPARK makes adoption more realistic.

- MTU did engine control for Eurofighter in Ada.
- LHX (Light Helicopter Experimental) use of Ada in engine controls. XD Ada.
- 1st Civil use of Ada investigated in 1990 on HOLD demonstrator, Mod project. Essentially a rewritten Tornado control.
- 1st large scale civil application is TRENT 1000, Boeing Dreamliner.
- Uses a cross compiler based on GCC 3.4.4

Aero Engine Controls

Development of Safety critical Ada engine control

- Tools and techniques adapted from existing test methods. Emphasis on testing at low level, items as intended to ship.
- Toolset capable of certification of software within a system to DO178-B/C.
- Host emulation
- RAM based monitors for in target testing.
- Powerful scripted test languages suitable for regression testing, production and presentation of certification evidence.

Problem area 1 – symbol tables

- Tools need a “outside observer” view of the component under test, and this does not fit well with information provided for debugging. DWARF information about variable location depends on the program counter. DWARF assumes first address is entry point. Last address is one of the exit points – perhaps.
- Need to map addresses to implementation of statically defined code structures. Structures now potentially complex.
- Indirection may be added in for Ada language purposes e.g. when aliasing. Need to know when to de-reference
- Need calling sequence information – including in/out status in Ada source
- Need to test on the basis of pre and post conditions – GDB provides test points post prologue, pre epilogue;
- Parsing DWARF is awkward [12].

Aero Engine Controls

Problem area 2 – Worst case execution time

- Currently theoretical WCET figures are produced using the executable as input.
- Have to reconstruct basic blocks and information and control flow.
- Need loop count information.
- Uses simulated execution and a cycle accurate timing model of the processor including processor and memory state effects.
- Need memory type being accessed, RAM and PROM timings differ.
- Data always used to be accessible to us, now spread across the compiler and some not propagated through. E.g. max loop counts, CFG.
- One of the potential values to us of open source is the possibility of obtaining this information as it is generated.

Questions for developers

- Can the data streamed out to be used for LTO be used to furnish some or all of the required information (The place it takes place looks promising to a novice ; post initial link but still in the compiler . i.e. GIMPLE + exact memory layout.)
- Can we annotate sources with maximum loop count assertions and preserve the information though the compiler. (with and without a switch to trust these values for optimisation?)
- Can we propagate Ada in-out information.
- Can we stream out the CFG – once it's not invalidated by the delay slot schedule? Can someone mentor me on the delay slot scheduler changes we would require?
- Any comments re the suitability of DWARF information vs LTO data. Complementary or is one redundant?

References

- [1] http://www.thefreelibrary.com/Men+behind+Rolls-Royce%27s+entry+t
- *[2] www.google.com/patents/US2586751.pdf*
- [3] http://en.wikipedia.org/wiki/William_Murdoch
- [4] http://www.britannica.com/EBchecked/media/147356/Group-Captain-E
- [5] http://www.mtu.de/en/products_services/military_business/programs/
- [6] http://www.goodrich.com/Goodrich/Businesses/Engine-Control-Systems/Innovation-and-History/1960s-to-1970s
- [7] http://www.aircraftenginedesign.com/pictures/RB211-524.gif
- [8] http://www.ccaonline.cn/e/2006/5574.html

References

- [9] http://התעופה.co.il/
- [10] http://digital-library.theiet.org/getabs/servlet/GetabsServlet?prog=normal&id=IEESEM00199600009600006000001&idtype=cvips&gifs=yes&ref=no
- [11] I.M. O'Neill, D.L. *Clutterbuck*, P.P. Farrow, P.G. Summers, and W.C. Dolman. The *formal* verification of safety critical *assembly* code
- [12] http://www.chromium.org/nativeclient/sdk/vsx-plugin/vsx-plugin-investigations/proposed-changes-to-symboldatabase-and-related-types

