

HIGH INTEGRITY SYSTEMS ENGINEERING GROUP

What is the best way to integrate static analysis (formal verification) with dynamic analysis (testing) for cost-effective verification (or re-verification) of software?

How can we do hazard and safety analysis for complex distributed systems? Are there limits to the complexity of what we should build?

Can we achieve reuse of software components in safety critical real-time systems and preserve (arguments of) safety?

The High Integrity Systems Engineering Group (HISE) undertakes research into all aspects of high integrity computer-based systems, with an emphasis on safety critical systems. The broad aim of the work is to provide theoretically sound but practical methods and tools to aid the development and assessment of high integrity systems.

High Integrity Systems

There are an increasing number of situations where we depend on computer-based systems to preserve and protect that which we value. We often use the term dependability to encompass more specific notions:

- safety - where we are protecting human life and health, and the environment;
- security - where we are protecting assets, including information;
- reliability or availability - where we need to ensure the continuity of valuable system functions.

Thus dependability is a form of requirement. Integrity is a means of providing dependability. Systems have to be of high integrity — free from flaws, sound in construction and robust — if we are to depend upon them in such applications.

Background and Aims

The HISE Group is a major academic research centre focusing on high-integrity systems, particularly real-time safety-critical systems. The group is sponsored by the EPSRC, the European Commission and European industry, most notably British Aerospace plc, Daimler Benz and Rolls Royce plc. It also has a wide collaborative base, involving Universities, major industrial companies and software houses around the world. The long-term aim of the group is to build a coherent set of methods and tools for the development and assessment of high-integrity systems, as typified by aerospace applications and to achieve transfer of the methods and tools to industry.

Education and Training

The HISE Group has a major involvement in teaching in the Department, particularly for several specialist post-graduate courses (Safety Critical Systems Engineering, Software Engineering, System Safety Engineering). Thus there is a range of 1-week modules available to support doctoral programmes.

ARCHITECTURES

Research Themes

Research work in the group covers all of the activities listed to the left. More details of all these research areas, and the projects currently being undertaken in them, can be found on the group's Web site (see below). We seek to gain synergy between these areas e.g. improving specifications to aid test automation.

DEPENDABILITY

DISTRIBUTED SYSTEMS

Areas of Application

The major current area of application for our work is the aerospace industry. British Aerospace fund the Dependable Computing Systems Centre (DCSC). Rolls-Royce fund a University Technology Centre (UTC) in Systems and Software Engineering, and some associated activities. We also have links with other aerospace companies, e.g. Lucas and GEC Marconi.

FORMAL METHODS

HAZARD AND SAFETY
ANALYSIS

The group's work is not limited to aerospace. Much of the work is general in nature and can be applied to any high-integrity system. Collaborative work has been carried out with the automotive, railway signalling, telecommunications and nuclear power industries.

REQUIREMENTS

Group Members

Mike Burke, DCSC Research Manager (seconded from BAe).

John Clark, Lecturer. Safety-critical systems. Computer security. Optimisation and evolutionary approaches to design synthesis. Testing.

REUSE

Andy Galloway, Research Fellow. Application of formal software engineering methods to the development of embedded control software for aerospace applications. Integrated formal approaches.

Tim Kelly, Lecturer. Safety cases, particularly change management, maintenance and the possible reuse of safety arguments.

SAFETY CASES

Steve King, Lecturer. Formal methods of system specification and development, and their application to safety-critical systems.

John McDermid, Professor and Head of Group. Software engineering for high integrity systems; real-time systems; safety-critical systems; hazard and safety analysis; formal methods; requirements analysis.

SECURITY PROTOCOLS

Jonathan Moffett, Lecturer and Advanced MSc Course Organiser. Computer systems security; requirements engineering.

David Pumfrey, Research and Teaching Fellow. Hazard identification, risk assessment and safety analysis.

SYSTEMS ENGINEERING

Ian Toyn, Research Fellow. Semi-automated reasoning with Z specifications, especially tool support and user interface issues.

Ian Wand, Professor. Software engineering, in particular software for safety-critical systems.

TEST AUTOMATION

In addition to the above, there are currently 15 Research Associates and 12 Research Students in the group.

TIMING ANALYSIS

Further Information

Further information can be accessed on the World Wide Web at URL <http://www.cs.york.ac.uk/hise>. To discuss educational and research opportunities contact John McDermid (phone: +44 1904 432726), Ginny Wilson, the HISE group administrator (phone: +44 1904 432782), or any members of the Group by email at firstname.lastname@cs.york.ac.uk or at The Department of Computer Science, University of York, York YO10 5DD, United Kingdom.

TRUSTWORTHY
TRANSLATIONS