

my file

SCIENCE AND ENGINEERING RESEARCH COUNCIL  
RUTHERFORD APPLETON LABORATORY

COMPUTING DIVISION

DISTRIBUTED INTERACTIVE COMPUTING NOTE 801

issued by  
Dr D A Duce

MEETINGS

Minutes of the Review Panel Visit to  
Professor B Randell, Newcastle, 9 February 1983.

14 February 1983

---

DISTRIBUTION:

- R W Witty
- D A Duce
- F B Chambers
- G P Jones
- Investigators/Randell
- DIC Notes file

(see next page)

# DRAFT

IN CONFIDENCE

SCIENCE AND ENGINEERING RESEARCH COUNCIL  
ENGINEERING BOARD

INFORMATION ENGINEERING COMMITTEE  
COMPUTING & COMMUNICATIONS SUB COMMITTEE

DCS Panel  
GR/C 4538.6

Minutes of a Review Panel visit to Professor B Randell,  
Newcastle - 9 February 1983.

## Private Meeting

Professor Randell has a rolling grant entitled 'Reliability and Integrity of Distributed Systems', for £291K which runs until September 1984. Professor Randell has now applied for an extension to September 1986.

The objectives of the review was to formulate a recommendation on the new application for the DCS Panel.

The Review Panel comprised:

K Dixon (Chairman)  
Dr I C Wand  
F B Chambers (DCS Industrial Coordinator)  
Dr D A Duce (DCS Academic Coordinator and Secretary).

In the opening discussion, the following questions were formulated:

1. What are the long term goals for the project? Do the goals stated in the previous application still obtain?
2. How does Randell believe his work has influenced computer science?
3. How much effort in the Newcastle Connection expected to absorb over the period of the grant? How does the connection work fit in with the long term goals?
4. How does VLSI figure in the project. How is Randell's work related to Kinniment's?
5. How does Randell see the relationship between his work and that in other British universities and industry?
6. Are the requested travel funds appropriate?
7. The application includes two and a half unnamed RA's. Will he be able to recruit these?
8. What is the relationship with MARI? Who is the software house mentioned in section 11 of the application?

9. Will the 11/730 requested be adequate for the needs of the project?
10. What equipment is to be covered by the maintenance provisions (section 21).
11. What are the 'hidden costs'? A rough estimate is that Randell requests 4 PERQs with Unix licences and ring interfaces, plus 3 Unix licences for the 11/23's already purchased but which run Unix in the next phase of the project.

#### Discussion with Professor Randell

Randell and his research team were present for the general discussion. Professor Randell gave a general overview of the project which addressed the Panel's questions concerning long and short term goals.

The Newcastle reliability project started in 1972, with an SERC rolling grant supporting four and a half staff. The grant has been maintained at four and a half staff since then. Funding has been received from MoD/SERC project entitled 'Fault Tolerant Software for Naval Command and Control Systems' started in 1981 and employs 2 RAs.

The present project team consists of:

#### Staff

B Randell  
T Anderson  
S Shrivastava

#### RAs

L Marshall (SERC)  
D Brownridge (SERC)  
(E Best) - new appointee 1/4/83 (SERC)  
(F Cristian) - interviews 27/2/83 (SERC)  
F Panzieri (MoD)  
J Black (Waterloo - Nato Fellow)

#### Visitors

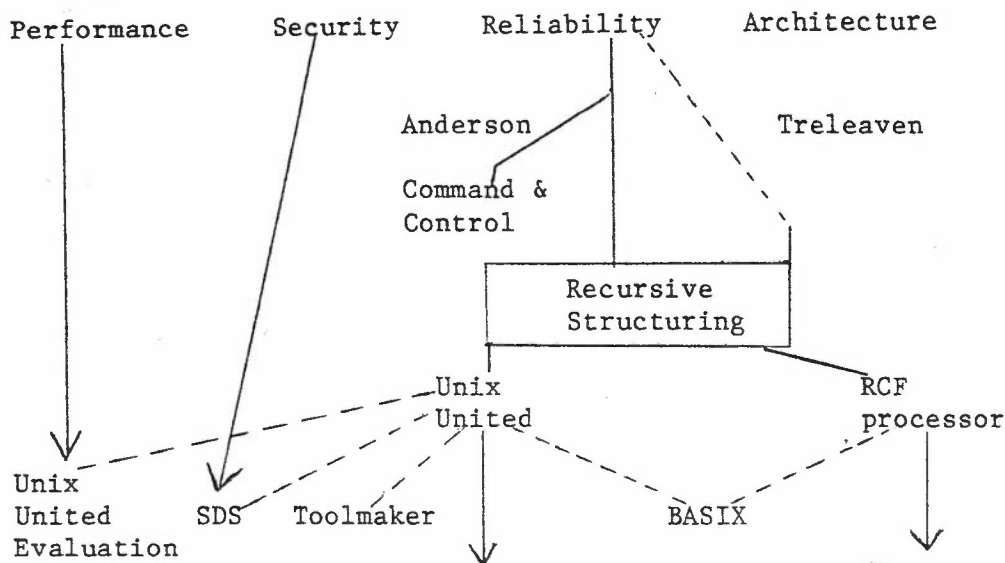
R Campbell (Illinois - SERC VF)  
Li Yi Lu (PEKIN - Royal Society funded)

#### PhD Students

R Stroud  
G Parrington  
J Anyanwu  
M Lynch

E Best and F Cristian left during 1982.

The following diagram illustrates the main themes in the project and their interaction.



The Unix United evaluation project is a continuation of Mitrani's work on stochastic modelling. A grant application is currently before CCSC.

The SDS project (Secure Distributed Systems) is a continuation of the Newcastle Security work (MoD funded). The project involved MARI and SDL. John Rushby who has been instrumental in establishing this line of research is going to SRI, but will act as a consultant to Newcastle. The security and reliability themes are now linked.

The Toolmaker project is a very large project being undertaken by MARI and a number of companies to build tools for the distributed development of distributed systems in the industrial control area. Further details are commercial in confidence. Unix United plays a large role in this project. The Computer Laboratory act as consultants to MARI. Randell emphasised that the Laboratory are not on the critical path of the project.

BASIX is a language emerging from the architecture project. RCF stands for Recursive Control Flow, essentially a synthesis of the control flow architecture and the notions underlying dataflow and reduction schemes - an evolutionary approach to new architectures.

Landmarks in the reliability project have included:

1. recovery cache 1975, (1979 hardware version on PDP 11/45)
2. recoverable concurrent Pascal 1978
3. Distributed recoverable filestore 1981
4. Unix United 1982.

Randell regards these as by products rather than as the real substance of the research. The latter is contained in books, papers and courses. Newcastle now give a regular course on reliability to ICL and other companies. The forthcoming Springer-Verlag volume of collected papers will be a major product of the research. Anderson and Lee's book is a good summary of the work to 1980.

The continuing theme of the project is the quest for system structuring techniques that can reduce system complexity even when fault tolerance is required.

Unix United is now operated at 3 sites (Logica and Keele externally) in a pre-release version. It is being marketed by MARI to Unix and Unix look-alike distributors. The official launch is on 17 March. NRDC will own Unix United, but MARI will have an exclusive licence to market the system for some number of years.

MARI is a separate legal and financial entity jointly owned by the University, Polytechnic and CAP. For taxation purposes it is recognised as a scientific institute. MARI has no rights to research done in the University. MARI was established in 1979 with a grant of £300K over 3 years from Tyne and Wear Council. In the last financial year turnover was £200K, this year it will be £380K and next year an estimated £600K, half of which is already committed. MARI employs 35 people.

MARI intakes many projects for local industries, mainly in the process monitoring and control areas. Work is also done for MoD/DoI and DoE and several large companies including 2 UK computer manufacturers. The aim is to concentrate on the networking and VLSI (strong links exist with Kinniment's project) areas. MARI will be the Newcastle Connection design authority.

ESPRIT are funding a study by CAP and MARI of the relevance of Unix United to the proposed Information Exchange System.

A number of experimental extensions to Unix United are being undertaken in the Computer Laboratory:

- TMR version (Liu)
- Stable storage (Anyanwu)
- Atomic actions (Perrington)
- Terminal concentrator (Whitfield et al)
- CP/M Facade (Gerrard)

The Newcastle Connection release 1 will link Unix V7 systems connected by a single network. Release 2 for V7/System III(?) will link systems connected by a multiplicity of LANs/WANs. Maintenance, and enhancements (for other versions of Unix and other network interfaces) will be handled by MARI.

### Short-term objectives

The short-term objectives are mainly related to Unix United and include:

- complete design and implementation of internetworking
- provide rested atomic actions
- improved naming and linking
- continuing investigation of the provision of hardware
  - fault tolerance (TMR, Stable storage, replicated files etc)
- reconsider Unix kernel interface
- continue study of general atomic actions
  - (forward as well as backward error recovery, dynamic as well as planned).

The short term objectives are expected to occupy at least 2 years.

### Long-term objectives

The long term objectives continue to be to synthesise:

- (1) fault tolerance and formal verification areas
- (2) software and VLSI design.

The synthesis of fault tolerance and formal verification stems from a paper by Anderson and Witty on "Safe Programming". Their ideas were taken much further by Flaviu Cristian. Concerns include:

1. a methodology for deriving acceptance tests and their optimal placement.
2. formal specification of security properties
3. formal verification of (several) distributed algorithms.

The aim is "to gain a better understanding of, and develop methods and tools for the design and implementation of systems, based on formal verification and verification guided fault tolerance and the certification of such systems".

On the VLSI side there are very close links with Kenniment (Electrical Engineering) who is looking at the application of software design techniques to control the complexity of VLSI design. Randell's group are looking at the complexity of VLSI design. Randell's group are looking at linguistic approaches to VLSI design, and architectures for VLSI. The reliability project has looked at redundant processor organisation (how to use acres of silicon) and a VLSI based recovery cache.

Newcastle have close links with groups at MIT, Edinburgh and Berkeley working in or close to these areas.

### The Command and Control Project

Tom Anderson gave an overview of the MoD/SERC funded command and control project.

This project is looking at the application of software fault tolerance techniques to a real problem and aims to measure utility, cost effectiveness etc.

The particular system being built is a naval command and control system. The specification was developed in conjunction with ASWE and naval officers to be an effective demonstration but with a limited set of sensors and weaponry.

A professional programming team (MARI/CAP) is being used. The software is being constructed using Mascot Coral. The technical work to map the fault tolerant constructs of recovery blocks and conversations (the latter enable state restoration in multiprocessor systems) into Mascot has been done. A very large proportion of the software has now been written.

Standard techniques for handling real time in Mascot/Coral are used - i.e. the system does not cope with real time constraints! Roy Campbell has proposed a scheme, the deadline mechanism, for handling real time constraints, but this cannot be fitted into the Mascot framework.

The command and control project may possibly use the ASWE serial data highway to link the processors.

### Demonstrations

The Panel were shown demonstrations of the command and control system and Unix United.

### Further Discussion

The second discussion session was conducted with Professor Randell alone.

1. There are no other university groups in the UK working on fault tolerance. Littlewood at City University is investigating quantitative models of reliability and Anderson has close links with this group. Hanna at Kent made some very promising suggestions for very high reliability networks with guaranteed response time etc, but has not pursued these ideas.

There are good links with industry, facilitated by MARI.

2. It is likely that a grant application will be forthcoming from Keith Bennett at Keele for collaborative research with Newcastle into networking partitioning with particular reference to Unix United. Keith Bennett recently spent a week at Newcastle discussing Unix United in detail.
3. The management and political problems with SERCnet are now being resolved. There is nothing the DCS Panel can usefully do to help here.
4. Newcastle would like to involve York in experiments to use the Newcastle Connection over X25. Dr Wand said he would be happy to be involved in such work.
5. Mr Chambers was concerned to what extent MARI would draw on the Computer Laboratory for maintenance and development of Unix United. Professor Randell reassured Mr Chambers that maintenance and development would be handled entirely by MARI, the Computer Laboratory merely acting as consultants.
6. The Panel agreed that the travel request was reasonable.

7. The Panel were concerned whether Randell could recruit suitable people to fill the vacant RA posts. One vacancy has been filled from 1 April and an adequate field of candidates have presented themselves for the second. Professor Randell is however concerned that further vacancies arising could not be filled unless funds are guaranteed until 1986. The half RA post is on the hardware side. Recently these funds have been used for contract construction work outside the Laboratory which has worked very well. The Panel agreed that the requested clerical support was necessary.
8. The maintenance funds are required to cover the 3 LSI 11/23s purchased under the existing grant and 2 x 11/45s. No funds have been included for PERQ maintenance.
9. Randell is asking for an 11/730 on the assumption that some of the workload of the present 2 x 11/45 configuration will be offloaded onto the 4 PERQs. The role of the 11/730 will be that of file server and safety net. The Panel felt an 11/750 would be more appropriate, but Randell felt an 11/730 was adequate.
10. Randell urgently requires a replacement for the 11/45s. A machine with a real Unibus is necessary because of the specialised i/o devices (of the recovery cache) that Newcastle have constructed and are essential to the future work.
11. Randell is assuming that the PERQs will come equipped with Cambridge Ring interfaces. He needs a number of identical machines for hardware fault tolerance experiments (TMR etc) hence the request for PERQs.
12. Randell expressed a number of concerns. The 11/45s are now very old, (about 10 years) and both Newcastle and DEC are concerned about reliability and maintainability. Randell is also concerned about the Unix licencing position - especially relating to commercial exploitation.

#### Hidden Costs

The following items are not explicitly costed in the proposal:

4 PERQs with Unix licence and Cambridge Ring interfaces.	74,800 17,250
Maintenance	16,560
3 Unix licences for 11/23s	<u>15,000</u>
Total	123,610

Thus the overall value of the award being sought is

348,740
<u>123,610</u>
472,350



### Private Meeting

The Panel felt that Newcastle were a wide ranging group, with a good publication record and excellent contacts. Whilst there were some worries about the exaggerated claims being made of the Newcastle Connection, the Panel felt the group fully merited continuing support.

The Panel felt strongly that the existing PDP 11/45s should be replaced as a matter of urgency and also that a machine with a real unibus was required as replacement. Whilst the Panel would have felt happier recommending a VAX 11/950, if Randell insisted he only required a 730 then so it should be.

The Panel were concerned that the delays in reporting back their views to the next DCS Panel would seriously hinder the project, especially with regard to replacement of the 11/45s the difficulty of recruiting further staff if anyone else were to resign. The Panel therefore agreed that the question of considering the application at the next CCSC should be taken up with the DCS Panel Chairman.

### Feedback

Randell was appraised of the Panel's views.