Reflexive Foundations for Computer Science

A talk by Roger Jones
of
ICL Defence Systems, Winnersh

In the defence market over recent years there has been an increasing emphasis on the need for very high levels of assurance that computer systems meet their critical requirements.

For the very highest levels of assurance it is generally understood that the relevant requirements must be formally specified, that the design of the computer system should be formally proven to conform to the requirements, and that the proof should be checked in detail by computer.

In order to achieve this, fully formal mathematical foundations suitable for applications in computer science are needed, together with effective computer based tools for developing and checking proofs.

In the talk the distinction will be drawn between mathematical foundation systems and other logical systems, arguing that the distinction is even more important to software engineers than it is to mathematicians.

The further distinction will be made between classical, hybrid and fully reflexive foundation systems, the latter class appearing the most appropriate to computer science.

An outline will be given of one approach to the development of fully reflexive foundation systems.

The talk will be light on technical detail, the emphasis on conveying an informal understanding of the basic issues. The connections between these foundational problems and the techniques currently practised in the formal methods group at ICL Winnersh and elsewhere, and the relationship between the proposed approach and other current research in the area, will be touched upon.