



# EWICS TC 7

## SUBGROUP FORMAL METHODS (FM)

### BRIEFING PAPER

#### **Introduction**

EWICS TC7 (European Workshop on Industrial Computer Systems, Technical Committee 7, Safety, Reliability and Security) is an international workshop of experts in the field of dependability of industrial computer systems with respect to safety, reliability and security.

#### **Problem Statement**

Formal methods, that is methods with a formal mathematical basis, are being increasingly recommended where the requirements for safety and security are very high. Emerging national and international standards mandate or recommend the use of formal methods. Although formal methods have been available within the research community for over a decade these methods are still not used in many practical applications. There is a lack of timely, realistic and independent information on the application of formal methods to assist in the procurement, management, design, testing and certification of critical systems.

#### **Progress to Date**

The EWICS formal methods group has been active in developing guidelines and in running workshops. We have now released guidelines on the use of Formal Methods in the Development and Assurance of High Integrity Systems. These are available for download from the EWICS web site at <http://www.ewics.org/docs/document-repository>.

The document provides practical advice for those wishing to use or evaluate formal methods in an industrial environment. As such it is a companion to standards that require or recommend the use of formal methods such as those from the IEC, the UK MoD and in the security field the Information Technology Security Evaluation Criteria. The Guideline is in three Parts. The first contains details for facilitating the use of the Guideline. Part II provides guidance and has three main sections on

- Introduction to Formal Methods
- Impact on Software and Systems Engineering
- Exploitation of Formal Methods

Part III is an evolving directory of formal methods. It contains a summary of the methods included and detailed entries for each of the methods that describe the application of the method, its maturity, the availability of tools. It adopts a classification scheme which addresses issues such as:

- Maturity of the method
- Availability of tools
- Consultancy and case study material
- Application domains for the method
- Properties or approaches which the method addresses
- Skill level required

Method users and developers are encouraged to comment on the directory and to propose additions. The format for additions is defined in an appendix and contributions should be emailed to reb@adelard.co.uk. A Word document containing the skeleton format is available.

The Guideline is intended for project managers, developers, users, assessors and procurers of high integrity computer systems. It assumes a background in existing practice (quality management systems, structured methods) as outlined in other EWICS TC7 Guidelines, and an awareness of existing and emerging standards, e. g. IEC 61508.

The Guideline is intended to provide an introduction for the inquisitive, and an appraisal of the current state of these methods and assistance to those wishing to use these techniques. The document is not a textbook nor does it pretend to be an exhaustive survey: tutorial material and surveys are referenced where available.

### **Future Work**

Future work being planned by the group include:

- Evolution of the Guideline in the light of comments and additions to the techniques directory

We will also be holding discussions and presentations of member projects on a range of themes of importance and interest to the group that will lead to the collaborative development of briefing papers. Topics to be considered are:

- The impact and interrelationship of formal methods and testing techniques.
- The impact of formal methods on the software lifecycle (e.g. omission of module testing by proof).
- The role of formal methods in exploring requirements.
- The use of domain specific formal methods (e.g. to support PLC applications).
- The use of formal methods in forensic analysis of accidents and incidents involving computer systems.

### **Membership**

The formal methods subgroup, as all EWICS subgroups, is an open group and we welcome participation. There are a number of ways you could become involved:

- By commenting on the guidelines from use or by desk top review.
- By adding material to the techniques directory.
- By offering talks or attending the workshops.
- By attending meetings and contributing to the work of the group.

### **Contacts**

For further details or to discuss how you might help please visit the web site [www.ewics.org](http://www.ewics.org) or contact:

- **Robin Bloomfield** (Chairman), e-mail: reb@adelard.co.uk, or
- **Stuart Anderson** (Vice-Chairman), e-mail: soa@dcs.ed.ac.uk