SIG on Formal Methods

SIG on Formal Methods:

Formal Methods (FM) has been in existence since 1940's, when Alan Turing proved the logical analysis of sequential programs using the properties of program states; and Floyd, Hoare and Naur used axiomatic techniques to prove program correctness against the specifications in 1960's.

These initial successes helped inculcate an interest in applying FM to the field of computer science.

Academia has been instrumental in bringing this field to the forefront, through continued research and development. The use of Formal Methods requires an expert skill-set expertise and therefore, its use is limited to those trained in the field.

Mission Statement:

Computer Society of India wants the field of Formal Methods to have a wider audience and more people to benefit from the application of these methods to all spheres of life. There is a need to use effective, correct and reliable approaches to design, develop and qualify complex, high assurance system software with the rigid schedules and budget. For this we need advanced tools, techniques and methods. Industry standards like RTCA DO-178C (Civil Aerospace), ISO 26262 (Automotive), IEC 61513(Nuclear), EN50126 (Railways) have recommended the usage of formal –method based approach to be used in the various phases of engineering process to achieve the required levels of safety and security.

Today there are proven techniques and tools that can be used in specification, design and verification & validation phases to assure correct requirement-capture, implementation, software functionality and security. This helps in developing high assurance software for applications such as cyber-physical systems, net-centric warfare systems, autonomous robots and Next Generation Air Transportation.

- **One day workshop on FM was conducted during April 2013**

Objectives of the Special Interest Group (SIG) are:

- To bring together scientists, academicians active in the field of formal methods and willing to exchange their experience in the industrial usage of formal methods
- To coordinate efforts in the transfer of formal methods technology and knowledge to industry
- To promote research and development for the improvement of formal methods and tools with respect to their usage in industry.
- To bring out practical engineering methods where formal methods will be integrated with current engineering methods

Some of the known applications of formal methods are:

- Formal verification, including theorem proving, model checking, and static analysis
- Techniques and algorithms for scaling formal methods
- Use of formal methods in automated software engineering and testing
- Model-based formal development
- Formal program synthesis
- Formal approaches to fault tolerance
- Use of formal methods in safety cases
- Use of formal methods in human-machine interaction analysis
- Use of formal methods in compiler validation and object code verification

3. Committee Members

1. Ms. Bhanumathi K S, Convener
2. Mr.Chander Mannar
3. Prof.Anirban basu
4. Mr. Suman Kumar
5. Prof. Shyam Sundar
6. Ms. Manju Nanda
7. Ms. J. Jayanthi
8. Ms. Saroja Devi
9. Prof. Meenakshi D'Souza
10. Yoganand Jeepu
11. Dr. Swatnalatha Rao

Planned Activities:

National Work Shop and Conference on Formal Methods for Software Engineering
Venue: I I Sc , Bangalore, October 15-17, 2014

Convener:

Bhanumathi K S
"Ganadhakshya" #406, 8 C Main,
H R B R First Block
Kalyan Nagar
Bangalore 560043
Email:bhanushekar@gmail.com
 Mobile:+91 95350 92589

Industrial use of formal methods

Compiled by Bhanumathi K S

Formal methods have been applied to railway systems in many countries. In France the first industrial use of formal methods for railways was for the SACEM system of RER Line A in Paris which has been in full operation since 1989.

The SACEM system is an automatic train protection system that continuously controls the speed of all trains on the line. The system permanently ensures the safety of 0.8 million passengers per day

Another industrial use of formal methods in Paris was for the automatic train operation system for metro line 14 (the first driverless metro line in Paris) that has been in full operation since 1998.

The formal method was used to develop and validate safety critical parts of the Roissy Airport shuttle (a driverless light train) that has been in full operation since 2007.

Railway systems in Denmark -The Technical University of Denmark has in collaboration with Kirsten Mark Hansen from Banedanmark, made formal models and verification for a number of case studies of existing interlocking systems in Denmark.

Avionics is a major application area of formal methods. This is exemplified by NASA9 which has about 40 researchers employed in four formal methods groups. These researches evolve and use formal methods dedicated to the development and validation of avionics software at NASA.

NASA used formal methods to verify a component of the Remote Agent software. Remote Agent is the first artificial intelligence control system to control a spacecraft without human supervision. It was one out of twelve technologies that were tested by Deep Space 1, a spacecraft dedicated to testing high risk technologies in deep space to lower the cost and risk to future science-driven missions that use them for the first time. DeepSpace 1 was launched in 1998.

****