SIG on Formal Methods

NEWS LETTER VOLUME 2 , FEBRUARY 2015

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. Dr. Yoganand Jeepu
11. Dr. Swatnalatha Rao
12. Dr. Aditya Kanade
13. Dr. A. Indira
14. Mr. Dhinakaran Pillai

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

Formal Methods for System/Software Engineering

Compiled by Bhanumathi K S

NASA and Army experiences on Formal Methods:

<u>Problem/Approach:</u>

General Problem	Approach
System/Hardware/Software complexity	Provide accurate and appropriate specifications of required system behavior using Formal Methods
Inadequate requirements specifications / misinterpretation of natural language. Significant number of problems introduced due to vague requirements	Develop requirement specification as Formal Specification (using formal semantics) to eliminate misinterpretation of vague and incomplete natural language requirements
Significant number of safety and reliability problems are traced to incorrect performance or behavior specifications, or incorrect interfaces	Use Formal methods to prove safety properties derived from safety analyses Use Formal Methods and deductive apparatus to prove correctness of system behavior and interfaces

Specific Problem	Approach
Formal Methods Learning Process Difficult for new users	Develop specific project related case studies and provide examples for potential users
Select development tools No time to learn all the tools Inadequate resource	Based on the project size and resources available, select appropriate Formal Methods development techniques and tools
Budget and Schedule constraints	Support program development and in parallel prove potential savings
Differences in priorities between Research and Production Environments	Many researchers focus on development of new techniques and tools Production or development programs are concerned with delivery of a product Need to build bridges between the research and production environments

Challenges

1. High cost of some commercial development tools.
2. Die-hard Systems and hardware Engineers are not convinced of the importance of software
3. Open source free tools do not have adequate training material and support.
4. Formal Methods tools require extensive learning process.

****