The Nucleus **49**, No. 2 (2012) 149-153

The Nucleus
A Quarterly Scientific Journal of Pakistan
Atomic Energy Commission
NCLEAM, ISSN 0029-5698

FORMAL METHODS ADAPTATION IN PAKISTAN'S SOFTWARE INDUSTRY

S. OSAMA, S.IQBAL and *A. AHSAN

Center for Advanced Studies in Engineering (CASE), Sector G-5/1, Islamabad, Pakistan

(Received April 18, 2012 and accepted in revised form June 2012)

This study has been done to understand the current usage pattern of formal methods in the software industry of Pakistan. The objectives of the study was to ascertain if organizations are using formal methods, what kinds of organizations are using them and what are the challenges associated with their usage. The study is exploratory as very limited literature on formal methods in Pakistan is available. The study employs literature reviews to understand the global trends in formal methods. As per the primary research, there is currently no organizations or projects utilizing formal methods in Pakistan. Key inhibitors in the adaptation of formal methods are also explored and highlighted through the study. As a conclusion to the study, a set of recommendations are delivered for promoting the use of formal methods in Pakistan focusing on regulatory support, academic development and methods to promote the usage in public and private sector.

Keywords: Formal methods, Software industry, Pakistan, Engineering, Management.

1. Formal Methods and its Dynamics

1.1. Introduction

With the advancements in technology, hardware and software systems are becoming more and more complex. But as always every organization strives to develop reliable systems. With the increasing complexity of systems there is a greater chance of errors and some of these errors can cause unacceptable loss of money, time or even human life. In order to gain the goal of producing ever more reliable complex and critical systems, the management methodology of formal methods is being vigorously explored.

Formal methods are mathematically based languages, techniques and tools for the specification, design and verification of software and hardware systems [1]. They don't guarantee the correctness of systems. However, they can greatly increase our understanding of a system by revealing inconsistencies, ambiguities, and incompleteness that might otherwise go undetected [5].

Globally, the formal method adaptation is gaining popularity but majority of potential users still are skeptical and doubt the maturity of tools / techniques for implementing formal methods. Figure 1 shows a chart depicting trend of formal methods adaptation worldwide [3].

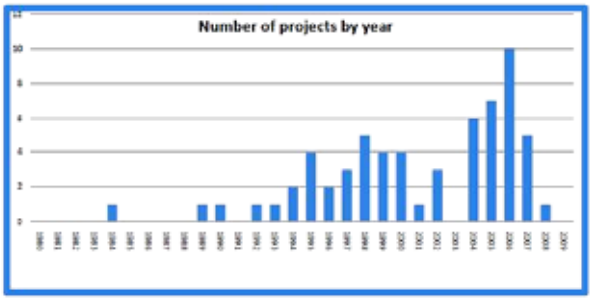

Figure 1. Trend of formal methods adaptation worldwide.

1.2. Usage in Project's Lifecycle

Formal methods can be used during any part of the project lifecycle and to whatever extent is necessary. Using formal methods throughout the system development lifecycle is not recommended because for certain aspects of system development it is just better to use the traditional approaches e.g. for user interface design and for dealing with the resource, time and financial

* Corresponding author : al_ahsan1@yahoo.com

aspects. Experienced researchers and practitioners both agree that formal methods are most effective if used for the important and critical early activities of the system development lifecycle which include requirements analysis, specification and high level design [6].

Formal methods can be used for eliciting, articulating and representing requirements [1]. Their tools can provide automated support needed for checking completeness, traceability, verifiability, and reusability, and for supporting requirements evolution, diverse viewpoints and inconsistency management [2].

In the domain of software development, it allows software engineers to create formal specification of the system using a language with mathematically defined syntax and semantics. The included system properties could be functional behavior, timing behavior, performance characteristics, or internal structure. It is most effective to analyze the formal specifications as early as possible to detect inconsistency and incompleteness. Similarly the architecture can be defined formally and checked early on to make sure that it satisfies all the key requirements.

Mathematical rigor enables users to then analyze and verify created formal models at any part of the project life-cycle: requirements engineering, specification, architecture, design, implementation, testing (code verification), maintenance and evolution [3].

1.3. Benefits

The benefits of formal methods include but are not limited to the following:

- Formally written specifications are more complete, consistent and unambiguous as compared to those using conventional methods [7]. Thus they provide a precise statement of what the software is to do.
- Since formal methods help us discover errors early in the lifecycle, they actually reduce the overall cost of the project [4].
- They don't need to be applied to the entire system development process. They can be used only for the critical parts [6].
- Formal methods generate mathematical models which can be analyzed or verified at any part of the system development lifecycle.
- They demonstrate responsible engineering and give solid reasons for trust in the product [4].

1.4. Application Areas

Formal methods application areas as surveyed in [3] are as follows:

Figure 2 shows the results of a formal methods survey [3] about the number of projects by application domain that have implemented formal methods. The largest single application domain was transport, followed by the financial sector. Other major sectors were defense, telecommunications, office and administration. Other areas with only one or two responses were: nuclear, health care, consumer electronics, space, semantic web, resource planning, automated car parking, embedded software, engineering and manufacturing. Some 20% of responses additionally indicated that the projects related to software development tools themselves, such as operating systems, compilers and CASE tools and a further 10% related to computing applications within the domain, such as high-performance computing, runtime code optimization, file system replication, access control, communications protocols and microcomputer design.

2. Formal methods and Pakistan's software industry

2.1. Current status

Currently formal methods are not being used by any Pakistani company or organization involved with software development.

2.2. Key inhibitors

The key inhibitors in the use of formal methods in Pakistan's software industry include:

a. Lack of awareness of formal methods, its benefits and its tools.

b. Lack of skilled human resource

c. Lack of confidence in formal methods

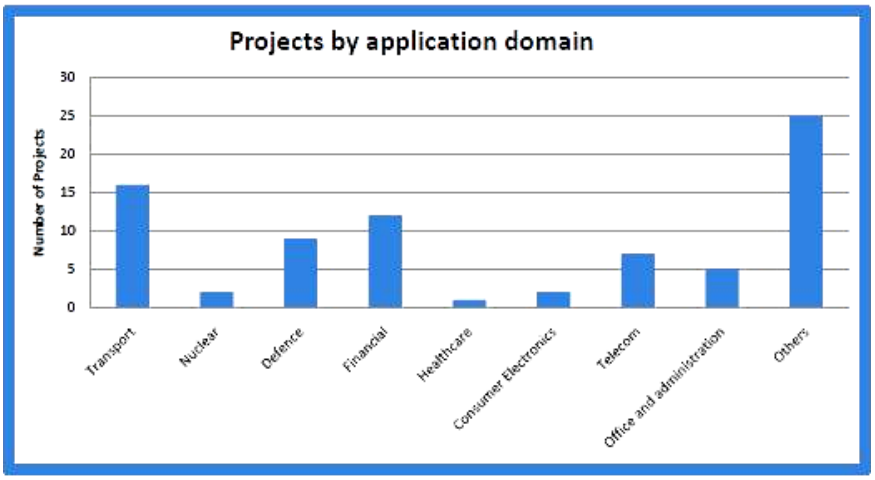

Figure 2. Number of projects by application domain that have implemented formal methods.

d. Fear of the entry cost of formal methods/Hard deadlines that must be met by software organizations

e. Perceived risk of failure or delay.

2.3. Industrial Applications

Formal methods are typically used for critical applications for which the cost of failure is really high. In Pakistan, Industries or projects that can benefit from their use include and are not limited to the following.

a. Defense and Defense Production

b. Nuclear

c. Avionics

d. Telecom / Media

e. E-Government / Government Records

f. Healthcare

g. E-commerce

h. Banking systems/Electronic finance

i. Security applications

2.4. Steps Towards Successful Industrial Adoption and Adaptation

In Pakistan, there are only a handful of people who are actually aware of what formal methods are, how they are implemented and what positive impact they could have on the industry. The main issue that needs to be addressed is the lack of awareness and expertise.

2.4.1. Education & Research

In Pakistan, universities need to take steps to embrace the concepts of formal methods at all levels starting from under-graduate level. This would help us to develop the human capital which is necessary to promote formal methods.

In addition, universities also have to take up formal methods research. Formal methods is one of the fastest growing research areas in the domain of engineering and computer science. A lot has been done but formal methods are still not mature. Methods need to be improved, they need to be made practical, new methods need to be invented, tools need to be improved and new tools need to be built [5]. There is a need for formal methods notations and tools to become more user friendly as currently formal specification and descriptions are only understandable by the practitioners who implement them. Tools also need to be improved so that they can be easily integrated with other programming tools and environments. The potential benefits of reduced defect densities in specification, design and code have to be achieved at a reasonable cost and within the constraints of real industrial settings [3].This is required for a wider acceptance and in our case initial acceptance and adaptation of formal method techniques.

Research in this field needs to be promoted in Pakistan. We have observed positive steps in this direction. Universities including MAJU and NUST have developed formal methods research labs but they currently have limited scope and have produced little success.

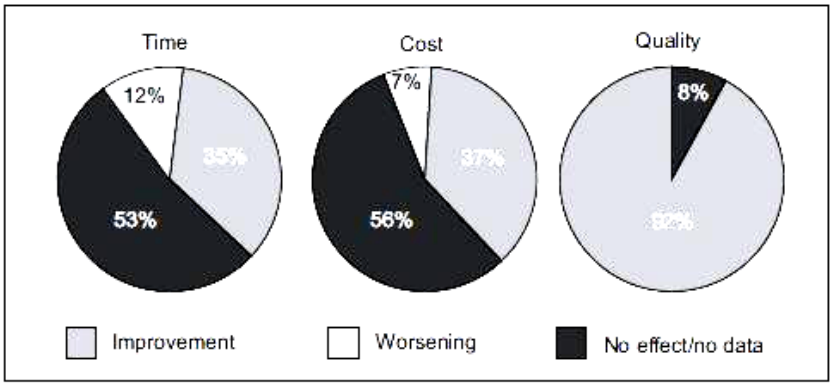

Figure 3. Effects of the use of formal methods on time, cost and quality.

2.4.2 Awareness of Practitioners

There is a need for the researchers to educate the professionals in the industry regarding the use, implementation and application of formal method techniques. Industrial professionals worry about the initial cost of implementing formal methods. They need to know that within a project formal method techniques can used to the extent to which they are required e.g. they can be used only for the critical parts of the project . They need to be aware of the advancements and accomplishments made in the field. Initially they would need to be convinced by successful implementations in the west. They would need evidence of the fact that since formal methods help us discover errors early in the lifecycle, they actually reduce the cost of the project. Governmental regulatory and quality assurance organizations like National Productivity Organization or Pakistan Software Export Board also need to get involved in raising awareness.

2.5. Possible Benefits of Adapting Formal Methods in Pakistan

While the use of formal methods does not guarantee bug free software, various case studies have shown that the use of formal methods significantly reduces the occurrence of bugs in the developed product. Even though the use of formal methods is still scarce worldwide a number of industries and organizations in the west involved in the development of critical systems are using existing formal method based tools and thus getting more reliable software e.g. IBM, Praxis, Motorola, NASA.

Figure 3 shows the results from a survey regarding the overall effects of the use of formal methods on time, cost and quality [3].

Pakistan can also significantly benefit from the advantages of formal method but we need to be wary that we cannot expect a good success rate during first few years of adaptation. This is because there is no skilled manpower, lack of support, cost risks and fear of the failure/delay. However, if organizations are committed to using formal methods, they will reap the benefits in the longer run as evident from research conducted in more developed countries.

3. Findings/Conclusions

Outcomes presented in this section are based on exploratory research conducted for local industry.

There is a lack of awareness and implementation of formal methods in Pakistan due to the following reasons:

a. Students are not properly introduced to formal methods in universities.

b. In the private sector there is hardly any work being done very critical or complex software systems that would promote the use of formal methods. Complex and critical software is generally imported from abroad.

c. In public sector, there is work being done on complex and critical software which can benefit from the use of formal methods. But due to the lack of awareness, will to improve and vision of the future there is no acceptance or acknowledgement of formal methods.

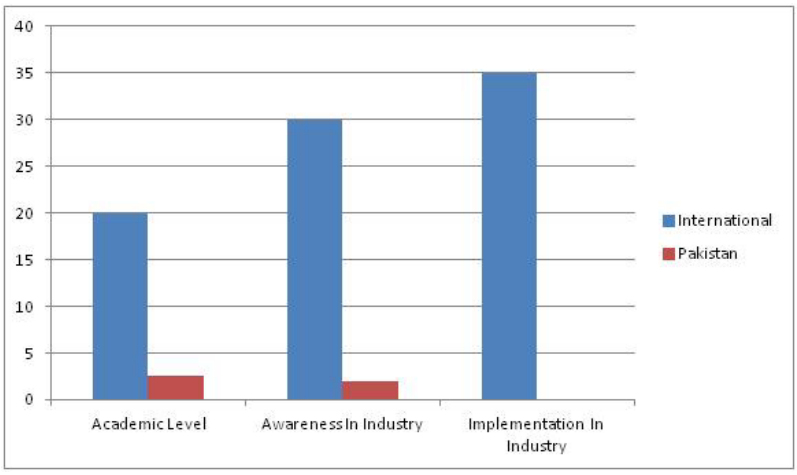

Figure 4. Comparison of the implementation of Formal Methods (International vs. Pakistan).

4. Recommendations

The following steps should be taken to effectively introduce and promote the acceptance of formal methods in Pakistan's software industry:

a. In universities formal methods should be introduced in the curriculum and research in this field should be encouraged.

b. Knowledge should be transferred between researchers and practitioners.

c. International private companies involved in critical and complex software development should be given some incentive to set up their development centers in Pakistan so that our developers gain training and experience of the implementation of formal methods. Over time this knowledge will spread within our own software industry and we will benefit from it.

d. In the case of our public sector needs to be motivated towards improvement and acceptance of modern techniques. For the increase in knowledge and awareness they should send people abroad for trainings, send people to gain hands on experience from global companies implementing formal methods and hire consultants who can guide them regarding the implementation of effective modern processes.

Acknowledgements

The author would like to express his gratitude to Dr. Aamer Nadeem, Dr. Osman Hasan and Mr. Muhammad Taimoor Khan for fruitful discussions.

References

[1] V. George and R. Vaughn, The Journal of Defense Software Engineering **16**, No. 1 (2003) 30.

[2] A. Ghose. Formal methods for requirements engineering. International Symposium on Multimedia Software Engineering (ISMSE 2000), Taipei, Taiwan, 11-13 December (2000).

[3] J. Woodcock, P.G. Larson, J. Bicarregui and J. Fitzgerald, ACM Computing Surveys **41**, No. 4 (2009) 1.

[4] Anthony Hall, Journal of Universal Computer Science **13**, No. 5 (2007) 669.

[5] E. M. Clarke et al., ACM Computing Surveys **28**, No. 4 (1996) 626.

[6] J.P. Bowen and M. G. Hinchey, Ten Commandments of Formal Methods… Ten Years Later, IEEE Computer Society, (January 2006) p. 40-48.

[7] J.P. Bowen and M.G. Hinchey, IEEE Software, **12**, No. 4 (1995) 34.