Promises and pitfalls of formal methods: Are we in the right train ?

S. Parthasarathy[1]
drpartha@gmail.com

Keywords : automation, software, formal methods, railways, explication, domain engineering, safety, verification, validation, proof, abstraction.

EXTENDED ABSTRACT

The aim of this paper is to make an introspective study of some aspects of the use of formal methods in development and assessment of control systems for railways. The authors do not wish to enter into yet another polemical debate on the pros and cons of formal methods. Instead, the paper proposes a holistic approach to the subject.

The state of the art in formal methods is similar to the following scenario: a couple travelling in a modern hit-tech train, is confronted by the train´s conductor who is describing in great detail the precision and technology used in the particular train. Until the couple ask him: "Good....., but are we in the right train ?" The question is, "is formal methods" the right answer for implementing safety ?

"Formal methods" have been in existence since at least two decades now, and is still evolving. Its application in railways automation has been met with varying degrees of success. It does contribute to a relatively more organised and systematic approach to systems development, particularly in domains (such as the railways) which involve safety. However, it addresses only a subset of the problems faced by systems developers. The approach to safety-critical systems should treat the entire process integrally and in a seamless fashion. It should be evolutive and uniformly rigorous over the entire life cycle. Perhaps this is a tall order, which explains why no satisfactory solution exists till now.

[1]Permanent address : Algologic Research and Solutions, 78 Sancharpuri Colony, Bowenpally P.O., Secunderabad 500 011, India
e-mail: drpartha@gmail.com
WWW-URL: http://algolog.tripod.com/nupartha.htm

What is (are) formal methods ?

Paradoxically, a formal subject like "formal methods“ has no "formal" definition. Various interpretations are used in the literature. According to Wikipedia[2], the on-line encyclopedia, formal methods may be defined as :

> *In computer science, **formal methods** refers to mathematically based techniques for the specification, development and verification of software and hardware systems. The approach is especially important in high-integrity systems, for example where safety or security is important, to help ensure that errors are not introduced into the development process. Formal methods are particularly effective early in development at the requirements and specification levels, but can be used for a completely formal development of an implementation (e.g., a program).*

Formal methods is also a collective noun, like mathematics, physics, fluid dynamics etc.

Railways and safety

Ensuring safety in the railways is a big challenge due to the unusual conditions under which trains must operate:

1. Trains are often operated under unpredictable, or uncontrollable weather conditions. On application of the brakes, a moving train moves through a large distance before coming to a complete halt. This braking distance is a „safe braking distance“ if there is no obstacle on the track for all thsi distance. Usually, due to adverse weather conditions this safe braking distance is shorter than the visibility, leading to a potential accident.
2. Trains carry no steering devices. Manoevrability of locomotives is very limited. Thus when the driver sees an obstacle, he has no ways of avoiding the obstacle, except to apply the brakes.
3. There is a very large source and variety of possible intrusions on the tracks.

[2]http://en.wikipedia.org/wiki/Formal_methods

4. It is very difficult to justify investement in safety, because it is not easy to put a price on the accidents which would be avoided due to this investment.
5. Increasing automation and complexity of train control systems is not easy to assimilate by train operators.

Can formal methods help (is this the right train ?) ?

Without entering into a polemical debate on this issue, let us examine a few aspects of this question.

1. Proof is still an intellectual marathon
2. Formal methods is still an opinionated parochial subject. There is no universaly acceptable theory of formal methods. Every practitioner of FM swears by a specific formal method. There is no easy way to bridge two formal methods or find equivalences.
3. There is no easy way to choose the right formal method for a given situation.
4. Formal methods stop with the specifications or design, and marginally into program structures. Extending the same to cover the semantics of the programming language used or the underlying operating system is a formidable task.
5. It is difficult to capture the behaviour of programming related artefacts liek recursion or pointers.

References

1. Jim Woodcock, Martin Loomes, Software engineering mathematics -- Formal methods demystified, Pub.: Pitman (UK).
2. William A Wulf, Mary shaw, Paul Hilfinger, Lawrence Flon, Fundamental structures of computer science, Addison Wesley Pub. Co., Reading MA, USA.