Formal Methods at Scale

Ray Richards, DARPA

Formal methods at scale in the defense industry would align with the DoD's Digital Engineering Strategy, facilitating the design and implementation of systems of ever-increasing complexity. The ability to analyze and explore the design space, the early identification and remediation of flaws, the removal of issues being identified during system integration resulting in costly delays and rework, and removing much of the uncertainty and risk of system (and System of System) integration ought to be the expectation of the benefits of formal methods.

In order to reap the benefits of formal methods in the development of military systems one must understand the impediments to adoption of these technologies. In any industry, the adoption of new design technologies must provide an appropriate return on investment. In order to make the business decision to adopt a design technology the benefit must be clearly measurable. To date the areas where formal methods have made successful inroads in the defense industry are niche areas where formal methods can improve the efficiency of a specific task in the design process, often the benefits are localized to that task. An example of which is automated test case generation. Formal methods have been used to generate test cases from design specifications, meeting stringent test coverage criteria. The benefits established are localized, but measurable in terms of labor hours saved in test generation. While these sort of uses of formal methods are promising, they are limited in the benefits that formal methods can provide.

The defense industry does not operate with the advantages of economies of scale. Instead of amortizing the development costs of military systems over the lifespan of the system, the government pays for the development of such systems and then allows the manufacturer to sell items to the military at a reasonable profit. Consequently, the return on investment of new design technologies only accrues over the development process; it does not accumulate over the life of the system. The benefit to the use of formal methods must be measurable and greater than the opportunity cost. The costs involved in industrial scale use of formal methods includes the acquisition of tooling, support contracts for the tools, overhauling engineering processes to maximize the benefits of formal methods, and training the engineering workforce on the new process and tools. The return on this investment needs to be greater than other investments that could have been made with those resources, such as R&D into a new capability. Furthermore, overhauling engineering processes may be seen as exceedingly risky. Defense companies compete on their ability to engineer the necessary military systems. Hence, their engineering processes are viewed as valuable intellectual property, providing their comparative advantage in the marketplace.

It is difficult to calculate the return on investment when the envisioned benefit is the avoidance or reduction of a future cost, when the avoided cost cannot be known. It is well known that the cost of addressing a design flaw goes up dramatically over the course of the design process. With a flaw in a fielded system being 300-1000 times as costly as finding it at the earliest point in the design cycle. However, when a flaw is identified and remediated early through the application of formal methods, it is impossible to know that the cost of identifying and remediating the flaw using traditional methods. It could be immense, or it could be negligible.

In order for the government to attain the benefits of formal methods at scale, it needs to create conditions that are conducive to their adoption. Activities to this end include but are not limited to funding research in formal methods enabled digital engineering processes, engage in pilot programs that apply formal methods at scale, revision of certification criteria to recognize and accommodate evidence generated by formal analysis, and continued investment in underlying formal methods capabilities.