The Pentium processor bug, the failure of the AT&T switching system, the deaths related to overdosing from the Therac 25 irradiation machine, and reported software failures in Airbus aircraft provide evidence of the risks taken when we use advanced computer systems to control critical systems. When these critical systems are operational, financial resources, corporate reputations, industrial secrets, human lives, and the environment are all at risk. The complexity of these systems prohibits the use of conventional design and analysis techniques to provide high levels of confidence in the correct operation of these systems. The application of formal design and analysis to these critical systems is essential to provide this high level of confidence, and thus reduce the risks involved in the use of these systems.

The application of formal methods to the specification, design, verification and validation of advanced computer systems is part of the system engineering process in several trial projects throughout industry. The results of these trial projects and the development of industrial strength techniques are the focus of this minitrack. We present two papers that focus on the application of formal methods to industrially based systems. The reporting of the results and lessons learned will hopefully enable others to build on the successes and avoid the pitfalls and failures of others.

1. **Optimistic Simulation Protocol**


   This paper presents a formal view of the widely-used Time Warp protocol. It relies, as does Time Warp, heavily on Lamport's work on temporal reasoning in distributed systems. The authors use this protocol to present an interesting specification of a simulation system in the PVS specification and verification system. This provides and interesting application for formal specification in that the system is sufficiently complex yet is well explained enough for the reader to follow. To demonstrate the formal nature of this work, the authors describe the proof of the CC’s and of several invariants.

2. **Software Architecture for Embedded Systems**


   This paper uses presents an extension of Data Flow Networks as a process algebra for the industrial strength SPLICE software architecture. As such, it presents an approach to formalizing an existing industrial model which can then be used for rigorous formal validation of industrial systems. Although this work is still in the early stages, it demonstrates how formal methods can start to be integrated into industrial processes.