Formal Methods Assurance for TTP

John Rushby
Computer Science Laboratory
SRI International
Menlo Park CA 94025 USA

Email: Rushby@csl.sri.com
WWW: http://www.csl.sri.com/˜rushby
Phone: +1 (650) 859-5456 Fax: +1 (650) 859-2844

TTP/C is used to support safety-critical applications, so its own correctness requires a very high degree of assurance. That assurance has been provided by the extensive testing and fault-injection performed by TTTech and the Technical University of Vienna, and by experience in the field.

"Formal methods" is a branch of computer science that can provide a complementary approach to assurance based on mathematical logic. This approach uses model checking and automated theorem proving to examine the behaviors of the algorithms employed in TTP/C under all possible circumstances. The two approaches are complementary because traditional testing examines *some* of the behaviors of the *actual system*, while formal methods examine *all* the behaviors of a *mathematical model* of the system.

SRI is a leader in the field of formal methods. We are participating in a NASA-sponsored project that is developing and using formal methods for assurance of TTP/C applications in commercial aviation. I will outline the methods used and progress achieved, and will describe the potential benefits to users of TTP/C and the opportunities for wider exploitation of this technology.