Formal Specification and Analysis of AFDX Redundancy Management Algorithms

Jan Täubrich

Fa. Dipl.-Inform Jan Täubrich, Kiel, and Philips Medical Systems, Hamburg

Reliable communication among avionic applications is a crucial prerequisite for today's all-electronic fly-by-wire aircraft technology. The AFDX switched Ethernet has been developed as a calable, cost-effective network, based upon IEEE 803.2 Ethernet. It uses redundant links to increase the availability. Typical consensus strategies for the redundancy management task are not feasible, as they introduce too heavy delays. We formally investigate AFDX redundancy management algorithms, making use of Lamport's Temporal Logic of Actions (TLA). Furthermore, we present our experiences with the specification language TLA+ and the TLA+ model checker TLC.

This is joint work with Prof. Dr. Reinhard von Hanxleden, Christian-Albrechts-Universität zu Kiel, who performed part of it while with EADS Airbus, Toulouse.