

Formal Methods in Industrial Dependable Systems Design - The TTTech Example

Wilfried Steiner
TTTech

Abstract of Invited Talk

Over the last decades the field of dependable computer systems has gained tremendous significance in our modern society. We rely on the dependability of automobiles, railways, airplanes, medical devices, critical infrastructures, like the electrical grid or industrial production facilities, and many more. These dependable systems frequently implement non-trivial mechanisms, for example, to coordinate between redundant components, and a guarantee of correctness of these mechanisms is therefore crucial to avoid catastrophic incidents. Consequently, formal methods are frequently used in industrial dependable system design and in this talk I will discuss the various aspects in which formal methods are and have been deployed for specification, verification, and configuration at TTTech for critical networking products.