Experiences in Developing Model-Integrated Tools and Technologies for Large-Scale Fault Tolerant Real-Time Embedded Systems

Steven G. Nordstrom
Institute for Software Integrated Systems, Vanderbilt University
Nashville, TN, 37235
steve.nordstrom@vanderbilt.edu

Abstract. Conventional redundancy-based fault tolerance approaches are not appropriate for high energy physics experiments due to tremendous system cost (fault tolerance is limited to 10% overhead). A set of tools was developed at Vanderbilt University for specifying, simulating, and implementing a range of low overhead failure adaptation strategies within the context of a large scale embedded environment. The tools embrace a model-integrated approach that combines design specification, behavioral modeling, and code-generation to produce both simulations and system implementation. Experiments were conducted to evaluate the behavioral correctness, performance, and adaptability of the tools under a variety of failure scenarios.