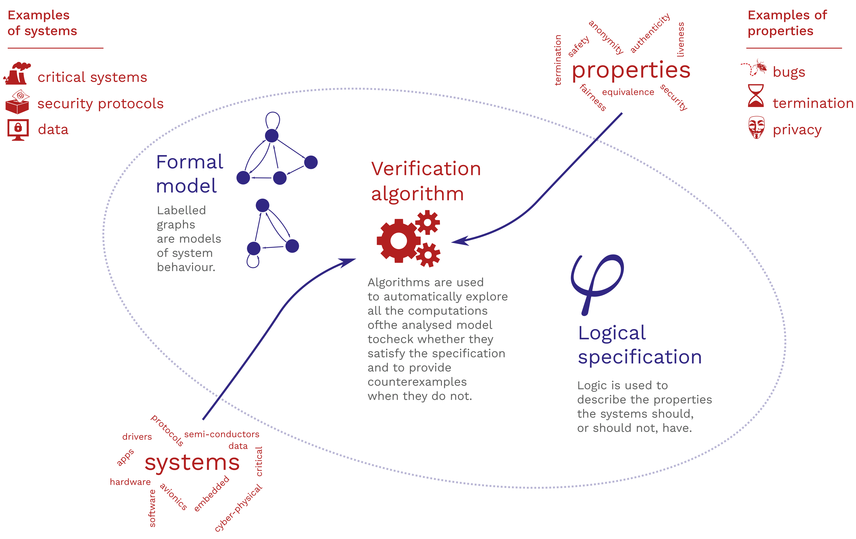
Model Checking

Proving system correctness, automatically

One of the goals of computing as a whole is to develop computing systems that perform the tasks they were designed to do in a reliable manner. Model checking is an area of research in Theoretical Computer Science that has had huge impact on achieving that difficult goal.

WHAT IS MODEL CHECKING?

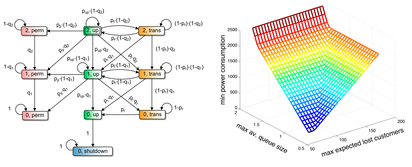


Edmund Melson Clarke (left), E. Allen Emerson (centre) and Joseph Sifakis (right) received the 2007 A.M. Turing Award "for their role in developing Model-Checking into a highly effective verification technology that is widely adopted in the hardware and software industries." Those scientists introduced Model Checking as an algorithmic system-verification technique in two path-breaking papers published in 1981 (Edmund M. Clarke, E. Allen Emerson) and 1982 (Jean-Pierre Queille; Joseph Sifakis).

WHAT DOES THE CHECKING?

Software tools carrying out this analysis are called model checkers and have been used to find and fix bugs in many mission-critical hardware and software systems, in program synthesis, and in optimal scheduling amongst many other applications. Examples of model checkers are Alloy Analyzer, BLAST, CADP, FDR2, HyTech, Java Pathfinder, mCRL2, NuSMV, Prism, SPIN, TLA+, and UPPAAL.

The pictures above describe the application of the model checker UPPAAL to the classic "train-gate example" where six trains want to cross a one-track bridge and to do so safely. Each train has a specified arrival rate and can be stopped before some time threshold. When a train is stopped, it can start again. Eventually trains cross the bridge and go back to their safe state. In the second picture, the tool is used to estimate the probability that Train 0 will cross the bridge in less than 100 units of time.



A discrete-time Markov Chain PRISM model of an embedded system comprising a processor which reads and processes data from two sensors (left) and a graph showing the power-versus-performance trade-off in power management policies for an IBM TravelStar VP disk-drive obtained using PRISM (right).