Susanne Graf, CNRS senior researcher at the Verimag laboratory (Grenoble), and Hassen Saidi (SRI International) were awarded the 2022 CAV award. CAV is a leading international conference on computer-aided verification, that is, theoretical and practical research on using computers to automatically verify that hardware or software behaves as intended. Computer-aided verification tools are for instance used when designing microprocessors, fly-by-wire aircraft control systems, or in other contexts where hardware or software malfunction may have costly, or even fatal, consequences.

Computer-aided verification is a hard problem. Indeed, theoretical work by Alan Turing and successors showed that there cannot be general algorithmic approaches to it, and even in restricted cases where an algorithmic approach is possible, the problems tend to be of high complexity. The computer-aided verification community has thus strived to design tractable approaches to safety proofs, for instance by safe over-approximation of the behaviors of the system.

The award is granted to Graf and Saidi for their pioneering work on predicate abstraction, which has proved to be very influential in the CAV community. In their paper “Construction of abstract state graphs with PVS”, published at CAV 1997, they proposed a method for the automatic construction of an abstract state graph of an arbitrary system using the PVS theorem prover. Given a parallel composition of sequential processes and a partition of the state space induced by a finite set of predicates on the program variables, the method constructs an abstract state graph, where the states are valuations over the predicates and the transitions are guaranteed to over-approximate the ones of the original system, allowing a conservative, abstract state space exploration for arbitrary programs. This technique has become known as “predicate abstraction” and has found countless applications, providing the fundamental building block for the well-known CEGAR (Counterexample-guided Abstraction Refinement) software model checking technique, as well as for popular software model checkers, such as SLAM and Blast.