Lifting the Verification Level

Dr. Christian Ferdinand, AbsInt Angewandet Informatik GmbH

In safety-critical systems miscompilation is a serious problem since it can cause erroneous or erratic behavior including memory corruption and program crash, which may manifest sporadically and often is hard to identify and track down. Many verification activities are performed at the architecture, model, or source code level, but all properties demonstrated there may not be satisfied at the executable code level when miscompilation happens. This is not only true for source code review but also for formal, tool-assisted verification methods such as static analyzers, deductive verifiers, and model checkers. In consequence, many safety standards require additional, difficult and costly verification activities to show that the requirements already shown at higher levels are also satisfied at the executable object code level. CompCert is an optimizing compiler that is formally verified, using machine-assisted mathematical proofs, to be exempt from miscompilation. The executable code it produces is proved to behave exactly as specified by the semantics of the source C program. We give an overview of the design of CompCert and its proof concept and then focus on aspects relevant for industrial application. We summarize practical experience and give an overview of recent CompCert development aiming at industrial usage. CompCert's intended use is the compilation of life-critical and mission-critical software meeting high levels of assurance. In this context tool qualification is of paramount importance. We summarize the confidence argument of CompCert and give an overview of qualification strategies.