# E-SPARK: Automated Generation of Verifiable Code from Formally Verified Designs

Rajiv Murali and Andrew Ireland

School of Mathematical and Computer Sciences,
Heriot-Watt University,
Edinburgh, EH14 4AS, UK.
{rm339, A.Ireland}@hw.ac.uk

The safety-critical sectors are faced with conflicting demands of achieving both high assurance as well increasing the productivity of their development process. Auto-coders have been effective in many areas, but the need for high levels of assurance has prevented its use in safety critical applications such as avionics. Standards for safety critical systems require a constant degree of verification, and most commercially available auto-coders do not satisfy this requirement.

We propose an approach where the auto-coder takes a formal model and generates code along with annotations, i.e. information flow analysis and proof assertions. In this way design invariants can be reused at the code level in order to support formal verification. Specifically, we have targeted Event-B and the SPARK Approach. At the design level, Event-B provides formal modeling supported by a strong and extensible toolset called Rodin. On the implementation level, the SPARK Approach includes a range of static analysis tools, from data flow analysis to formal verification. We have developed an eclipse based plug-in called E-SPARK for the Rodin platform that supports the automatic generation of provably correct code. At this stage, E-SPARK has been designed for the sequential subset of Event-B, and has been tested successfully on a range of arithmetic, searching and sorting examples of algorithmic design. Future development of E-SPARK could aim to target Event-B models of concurrent systems.