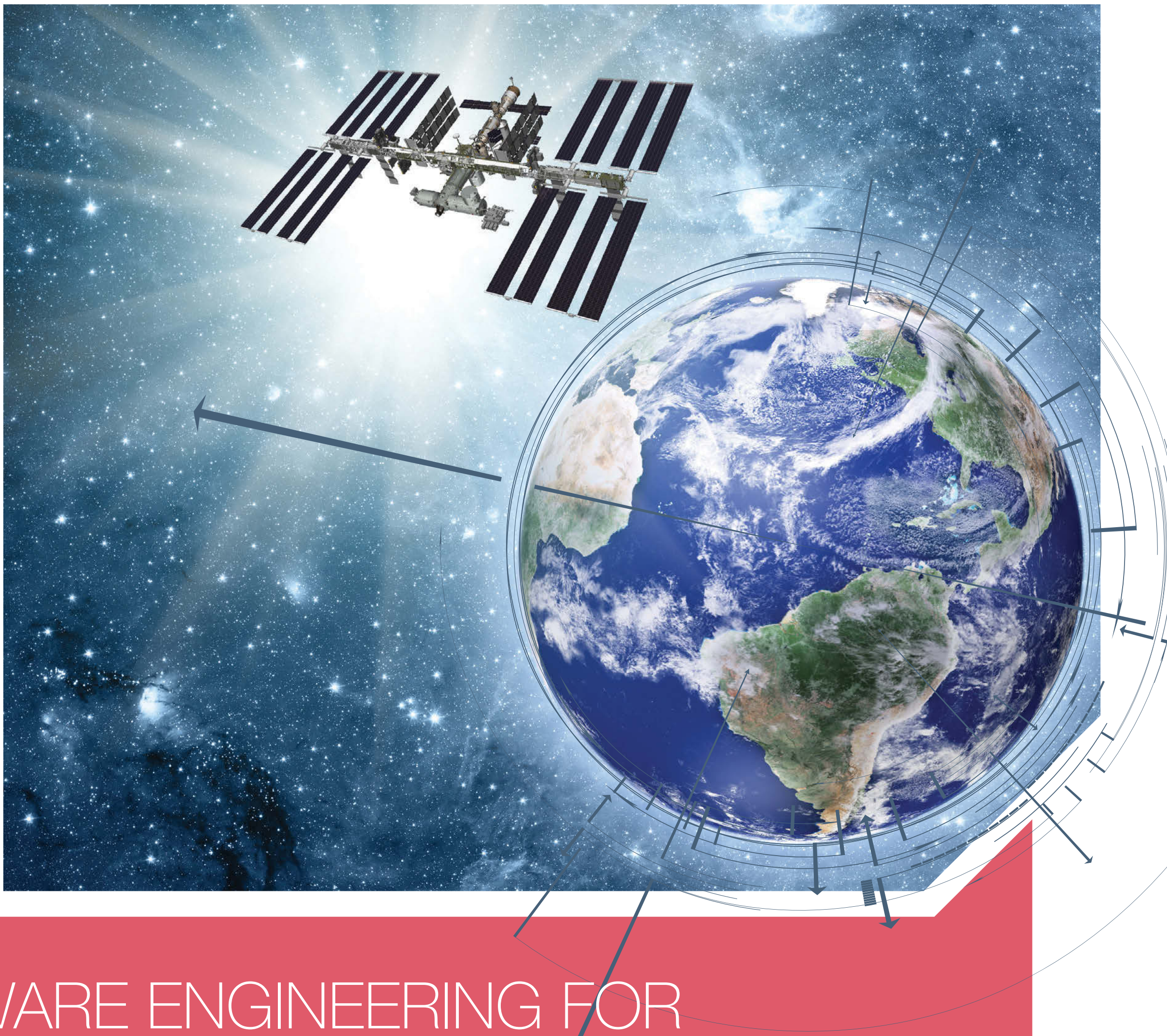

SOFTWARE ENGINEERING FOR THE EUROPEAN SPACE AGENCY

In the *Methods and Tools for On-Board Software Engineering* (*MTOBSE*) project Lero addresses several challenges associated with the development of on-board flight software for the European Space Agency (ESA).

The Space Avionics Open Interface Architecture (SAVOIR) initiative aims at improving efficiency and reducing development costs in space industry by common standards and interfaces such as a common reference architecture. Lero researchers Goetz Botterweck, Howell Jordan and Andreas Pleuss extended the reference architecture with concepts for variability using techniques from Software Product Lines. Their approach enables engineers to explicitly specify different variants or optional elements within the reference architecture together with dependencies between these variants. They provided tool support to 1) automatically extract a variability model from the reference architecture models, 2) enable engineers to visually configure the reference architecture for a concrete space mission based on the variability model, and 3) automatically generate the resulting mission-specific architecture models.

Lero researchers Andrew Butterfield and David Sanán explored the verification of separation/partitioning microkernels to support Integrated Modular Avionics, potentially allowing different payload packages to share on-board computing resources to save costs. They investigated formal verification techniques that might be employed in order to verify the correctness of such a kernel implementation according to a global standard for security products, and developed a reference specification for such a kernel. They also constructed a formal model of this kernel and explored ways to develop formal models of actual kernel code. They demonstrated that it would be feasible to formally specify and verify such a kernel to the level required for highest security standards currently in use.

Andrew Butterfield is currently retained by the European Space Agency as a formal methods expert, giving consultancy advice to a current activity looking at describing and piloting the process by which such a separation kernel would be qualified as suitable for spaceflight.

Mike Hinchey is the project leader for MTOBSE. The *MTOBSE* project is funded by the European Space Agency.