GOALS OF THE PROJECT

Verification of C programs used to control safety-critical systems e.g., as airplanes, subway lines, or power plants.

- Developing scalable interprocedural verification techniques for concurrent software
- Detecting memory management errors automatically
- Experimenting with real-life industrial scale programs written in C

METHODS

- Function summarization in Integer Arithmetic and Shape Graph domains
- Thread-local reasoning in Separation Logic for concurrent recursive data structures

RESULTS

New prototype tools for software verification:

- FLATA-C: integers, arrays, pointer arithmetic
- CELIA: lists with infinite data domains
- CHEAP: concurrent recursive data structures
- MThread: concurrent lock/value analysis

CONCLUSIONS AND FUTURE

- Compositionality is the key to scalability of program verification techniques and tools
- Need to extend compositional reasoning to richer theories e.g., abstract data containers, recursive data types, etc.

COORDINATEUR: Radu Iosif (VERIMAG)
PARTENAIRES: LIAFA, LSV, CEA, EdF, VERIMAG