Report on Verification/Validation of Implementation

D4.2.2

Jens Gerlach

Fraunhofer FOKUS

München, 14.1.2014

Overview

- What was investigated?
- Who did contribute?
- How was it investigated?
- What are the (intermediate) results?
- What are the next steps?

What was investigated?

- “BitWalker” is a small set of C routines for the manipulation of bit sequences
  - developed by Siemens (Stefan Gerken)
  - fairly low-level code with lots of bit manipulation
- BitWalker is used by other routines of Siemens’ treatment of Subset 026

Who did contribute?

- Siemens (providing source code and guidance)
- SQS (static analysis)
- Fraunhofer FOKUS (formal verification)
- CEA LIST (tool support)

How was it investigated?

- emphasis on static analysis/formal verification with open source tools
- SQS applied different static analysis tools
  - RSM, LocMetrics, Clang Static Analyzer, CPPcheck
  - emphasis on metrics but also coding guidelines (MISRA)
- Fraunhofer started with formal *functional* verification of BitWalker using CEA LIST's Frama-C toolset

Intermediate results

- SQS generated lots of tables with information about the source code quality of BitWalker
- Fraunhofer FOKUS
  - informal specification of BitWalker
  - derived formal specification of BitWalker in Frama-C’s specification language (ACSL)
  - formal verification still incomplete
    - see next slide

Next Steps

- Formal Verification still incomplete
  - informal specification must still be reviewed by Siemens
  - ACSL specification should be independently reviewed by knowledgeable persons (e.g. CEA LIST)
- Frama-C must improve on treatments of bit operations
  - Discussion between Fraunhofer and CEA LIST

Thank You!