Mit Polyspace die Qualität des generierten und handgeschriebenen Codes effektiv verbessern

Christian Guß
Application Engineer
The MathWorks GmbH
What do all these systems have in common?

- Complex software developed to rigorous standards
- Extensively reviewed, analyzed and tested
- Yet still succumbed to costly failure
Examples: **Run-Time Errors** and **Programming Defects**

- Non-initialized data
- Out of bound array access
- Null pointer dereference
- Incorrect computation
- Concurrent access to shared data
- Illegal type conversion
- Unreachable states or code
- Overflows
- Non-terminating loops
- And lots more…

- Invalid use of = operator
- Invalid use of == operator
- Write without further read
- Uncalled function
- Missing null in string array
- Qualifier removed in conversion
- Race condition
- Invalid use of other standard library routine
- Memory leak
- And lots more…
Many executions for functional testing... ... do not prove code correctness

Which Quality Is Your Code Today?

Your source code

0% proven correct

Testing

0,000000...1% executions verified

0,000000...2% executions verified

0,000000...3% executions verified
Problem: Tests aren’t exhaustive

“Program testing can be used to show the presence of bugs, but never to show their absence” (Dijkstra [1])

“Given that we cannot really show there are no more errors in the program, when do we stop testing?” (Hailpern [2])

“Imagine how much time is used debugging and reviewing correct software” (C. Guss, today)

How is Polyspace code verification unique?

- Proves when code **will not fail** under any runtime conditions
- Finds **runtime errors**, **boundary conditions** and **unreachable code** without exhaustive testing
- Gives insight into runtime behavior and data ranges

Statically verifies all possible executions of your code (considering all possible inputs, paths, variable values)
Which Quality Is Your Code Today?

- **T0**
- **T0 + 3 months**
- **T0 + 6 months**

More and more is proven correct

Your source code

0% proven correct

Testing

Many executions for functional testing…
… do not prove code correctness

0,000000…1% executions verified

0,000000…2% executions verified

0,000000…3% executions verified
STATIC CODE ANALYSIS
Polyspace covers different approaches:

- Compiler Warnings
- Code Metrics, and Coding Rules
- Bug Findings (Fast, more categories)
- Formal Methods (full proven)
Polyspace product family for C/C++

- **Polyspace Bug Finder**
  - Quickly find bugs in embedded software
  - Identifies errors such as run-time, programming, dataflow, static and dynamic errors
  - Check code compliance for MISRA
  - Intended for every day use by software engineers

- **Polyspace Code Prover**
  - Proves code to be safe and dependable
  - Deep verification of software components
  - Perform QA signoff for production ready code
Polyspace support for code rules compliance

- **MISRA C Checker**
- **MISRA AC AGC** -- application of MISRA-C for generated code
- **MISRA C++ Checker**
- **JSF++ Checker**
- **Customization**
  - Turn rules off / warning / error
- **Custom Coding rules**
  - Define custom naming conventions
  - Mark violations as reviewed or indicate future action
Defects detected by Polyspace Bug Finder

Numerical
Zero divide, Overflow, Shift Integer and Float conversion Overflow Invalid use of std. library math routine, …

Static Memory
Array access out of bounds, Null pointer access, …

Dynamic Memory
Use of previously freed pointer, Unprotected dynamic memory allocation, …

Programming Defects
Invalid use of = or == operator, Declaration mismatch, …

Dataflow
Write without further read, Non-initialized variable, …

Other
Race Condition, …

For C and C++
## Applicability to Standards

ISO 26262-6 Software unit design and implementation

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th>Applicable Tools / Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Walk-through</td>
<td>+</td>
<td></td>
</tr>
<tr>
<td>1b Inspection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1c Semi-formal verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1d Formal verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1e Control flow analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1f Data flow analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1g Static code analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1h Semantic code analysis*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>++</td>
<td>+</td>
<td>o</td>
<td>o</td>
</tr>
<tr>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>o</td>
<td>o</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
</tbody>
</table>

✓ Polyspace Bug Finder
✓ Polyspace Code Prover

**Table 9 – Methods for the verification of the software unit design and implementation**

* … is used for mathematical analysis of source code by use of an abstract representation of possible values for the variables. For this it is not necessary to translate and execute the source code.

(ISO 26262-6, table 9, Method 1h)
Leverage an integrated tool chain
For Model-Based Design and automatic code generation and hand-written code

- Use traceability back to the model
- Use available context information for inputs and parameters

Polyspace verification on generated code
What does Polyspace help you with?

1. UNCOVER BUGS
   - Bug free code and efficient code reviews

2. SAVE TIME
   - Reduce the amount of robustness testing

3. CERTIFICATION DOCUMENTATION
   - Certification credits and automated reports