
Christian Guß
Application Engineer
The MathWorks GmbH
Agenda today

- Engineering challenges today
- Quality question
- Uniqueness of Polyspace
- How to comply with Safety Standards?
- Software Quality Objectives
High-Integrity Applications are complex

Software-based systems that are designed and maintained such that they have a high probability of carrying out their intended function

The Cost of Failure...

Ariane 5: Overflow Error

$7,500,000,000

Rocket & payload lost
The Cost of Failure…

Recall

Due to ECU software bug
The Cost of Failure…

Therac-25: Race Condition, Overflow

6 Casualties due to radiation overdose
Airworthiness Directives; The Boeing Company Airplanes
A Rule by the Federal Aviation Administration on 05/01/2015

DEPARTMENT OF TRANSPORTATION
Federal Aviation Administration
14 CFR Part 39
RIN 2120–AA64

Airworthiness Directives; The Boeing Company Airplanes

AGENCY: Federal Aviation Administration (FAA), DOT.

ACTION: Final rule; request for comments.

SUMMARY: We are adopting a new airworthiness directive (AD) for all The Boeing Company Model 787 airplanes. This AD requires a repetitive maintenance task for electrical power deactivation on Model 787 airplanes. This AD was prompted by the determination that a Model 787 airplane that has been powered continuously for 248 days can lose all alternating current (AC) electrical power due to the generator control units (GCUs) simultaneously going into failsafe mode.

This condition is caused by a software counter internal to the GCUs that will overflow after 248 days of continuous power.

We are issuing this AD to prevent loss of all AC electrical power, which could result in loss of control of the airplane.

DATES: This AD is effective May 1, 2015. The Director of the Federal Register approved the incorporation by reference of certain publications listed in this AD as of May 1, 2015.

We must receive comments on this AD by June 15, 2015.

https://www.federalregister.gov/articles/2015/05/01/2015-10066/airworthiness-directives-the-boeing-company-airplanes
How to avoid this? Engineering challenges today...

- Check MISRA
- Comply with ISO, IEC safety requirements
- Optimize Design and Architecture
- Deliver Bug-free software
- Measure Code Quality
- Reduce time and efforts for software testing
Typical Example… about the quality question

Final release… It’s done… Here is your software!

Great! Is it tested?

Engineer

OEM
Typical Example...about the quality question

Yes!
Everything is tested!
No errors!

Please prove it to me!
Typical Example...about the quality question

Please prove it to me!
Do You Know Which Quality Is Your Code Today?

Your source code

Testing

0% proven correct

0.000000...1% executions verified

0.000000...2% executions verified

0.000000...3% executions verified

Many executions for functional testing…
… do not prove code correctness
Problem: Tests aren’t exhaustive

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

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

More and more is proven correct

Difference of semantic analysis & testing
Typical Example...about the quality question

Please prove it to me!
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Initiation</th>
<th>Architecture</th>
<th>Design/Implementation</th>
<th>Unit Testing</th>
<th>Integration Testing</th>
</tr>
</thead>
</table>

**SYSTEMS**

- REQUIREMENTS
  - Architectural Design
    - Environment Models
    - Physical Components
    - Algorithms
  - System-Level Specification
  - Subsystem Design
  - Component Design
    - Test vectors and expected responses
    - Component tests in simulation
  - Code Verification and Validation
    - Run component tests on target
- Component Tests
  - Test vectors and expected outputs
  - System Tests
    - Run system tests on integrated controller
- User Acceptance Testing
- Complete Integration & Test
  - System-Level Integration & Test

**IMPLEMENTATION**

- C, C++
- VHDL, Verilog
- Structured Text
- MCU, DSP, FPGA, ASIC, PLC
- Subsystem Implementation
Examples of software safety requirements

Table 1 – Topics to be covered by modelling and coding guidelines

<table>
<thead>
<tr>
<th>Topics</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1a Enforcement of low complexity</td>
<td>++</td>
</tr>
<tr>
<td>1b Use of language subsets</td>
<td>++</td>
</tr>
<tr>
<td>1c Enforcement of strong typing</td>
<td>++</td>
</tr>
<tr>
<td>1d Use of defensive implementation techniques</td>
<td>o</td>
</tr>
<tr>
<td>1e Use of established design principles</td>
<td>+</td>
</tr>
<tr>
<td>1f Use of unambiguous graphical representation</td>
<td>+</td>
</tr>
<tr>
<td>1g Use of style guides</td>
<td>+</td>
</tr>
<tr>
<td>1h Use of naming conventions</td>
<td>++</td>
</tr>
</tbody>
</table>

Detect and correct areas with high complexity

Polyspace Metrics
Examples of software safety requirements

Table 1 – Topics to be covered by modelling and coding guidelines

<table>
<thead>
<tr>
<th>Topics</th>
<th>ASIL</th>
<th>Verification</th>
<th>Coding Rules</th>
<th>Software Quality Objectives</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Confirmed</td>
<td>Justified</td>
<td>Quality Status</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Defects</td>
<td>Violations</td>
<td>Level</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Review Progress</td>
</tr>
<tr>
<td>Initiation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Design/Implementation</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unit Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integration Testing</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1a Enforcement of low complexity</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1b Use of language subsets</td>
<td>++++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1c Enforcement of strong typing</td>
<td>++++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1d Use of defensive implementation techniques</td>
<td>o++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1e Use of established design principles</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1f Use of unambiguous graphical representation</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lg Use of style guides</td>
<td>++</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>lh Use of naming conventions</td>
<td>++++</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Polyspace Metrics
Justify MISRA violations with Polyspace formal method

```c
float risk_of_floatdivisionbyzero(int p)
{
    float i;
    float j = 1.0;
    float tmp;

    tmp = j * p;
    if (tmp < 0.0) {
        i = -1.0;
    } else if (tmp > 1.9209290e-7F) {
        i = 1024.0 / tmp;
    } else {
        i = 0.0;
    }
    return i;
}
```

**MISRA Violation**

**Proven save (no Overflow)**

**A violation**
Justify MISRA violations with Polyspace formal method
Examples of software safety requirements

Initiation | Architecture | Design/Implementation | Unit Testing | Integration Testing

System validation/acceptance Tests

User Acceptance Testing
Complete Integration & Test
System-Level Integration & Test
Subsystem Integration & Test

Architectural Design
- Environment Models
- Physical Components
- Algorithms

System-Level Specification

Subsystem Design

Component Design
- Test vectors and expected responses

Component Tests
- Component tests in simulation

Code Verification and Validation
- Run component tests on target

IMPLEMENATION
- C, C++
- VHDL, Verilog
- Structured Text
- MCU, DSP, FPGA, ASIC, PLC

Component Tests
- Test vectors and expected outputs

System Tests
- System tests in simulation

Run system tests on integrated controller

System Tests
- Run system tests on integrated controller
Examples of software safety requirements

Minimize size in balance with other design considerations

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted size of software components</td>
<td>++</td>
</tr>
</tbody>
</table>

Initiation | Architecture | Design/Implementation | Unit Testing | Integration Testing
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Initiation</th>
<th>Architecture</th>
<th>Design/Implementation</th>
<th>Unit Testing</th>
<th>Integration Testing</th>
</tr>
</thead>
</table>

- **System validation/acceptance Tests**
  - User Acceptance Testing
  - Complete Integration & Test
  - System-Level Integration & Test
  - Subsystem Integration & Test
  - Subsystem Implementation

- **Component Tests**
  - Component Design
    - Test vectors and expected responses
  - Code Verification and Validation
    - Run component tests in simulation
  - Run component tests on target

- **System Tests**
  - System tests in simulation
  - Run system tests on integrated controller

- **Requirements**
  - System-Level Specification
    - Architectural Design
      - Environment Models
      - Physical Components
      - Algorithms
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>l1c Control flow analysis</td>
<td>++</td>
</tr>
</tbody>
</table>

Detect poor and potentially incorrect program structures

```c
int roll() {
    return(rand()%6+1);
}
void operation(int);
void main() {
    srand(time(NULL));
    int die = roll();
    if(die >= 1 && die <= 6)
        /*Unreachable code*/
        operation(die);
}```
Examples of software safety requirements

- **Initiation**
- **Architecture**
- **Design/Implementation**
- **Unit Testing**
- **Integration Testing**

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
</tr>
<tr>
<td>1c Control flow analysis</td>
<td>+</td>
</tr>
</tbody>
</table>

Detect poor and potentially incorrect program structures

```c
int orderRegulate(void)
{
    int tmp, X;
    Increase_PowerLevel();
    SHR4_A = 22;
    tmp = PowerLevel SHR4_A;
    X = tmp;
    return X;
}
```
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data flow analysis</td>
<td>A</td>
</tr>
</tbody>
</table>

Detect poor and potentially incorrect program structures
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1d</td>
<td>A</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>B</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>C</td>
<td>+</td>
</tr>
<tr>
<td></td>
<td>D</td>
<td>+</td>
</tr>
<tr>
<td>Detection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Detect poor and potentially incorrect program structures

```c
static char reset_temperature(u8 in_v8) {
    int array[255-(64 * BIN_v8)];
    array[in_v8-255] = 0;
    return;
}
```

- **Green**: reliable, safe pointer access
- **Red**: faulty, out of bounds error
- **Gray**: dead, unreachable code
- **Orange**: unproven, may be unsafe for some conditions
- **Purple**: violation, MISRA-C/C++ or JSF++ code rules

Range data tool tip
Semantic Analysis Example

Read A INT;
A = A + 2 ;
...
If (A = 3) or (A = 7) or (A > 11) // improve robustness in regards of specification
then
B = C / (A - 8);
...
else
....
Endif ;

\[
A \in [\text{MinINT} + 2; 2] \cup \{4, 5, 6, 8, 9, 10, 11\}
\]

No test cases to write
No execution
No simulation
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Initiation</th>
<th>Architecture</th>
<th>Design/Implementation</th>
<th>Unit Testing</th>
<th>Integration Testing</th>
</tr>
</thead>
</table>

**Requirements**
- System-Level Specification
  - Subsystem Design
  - Architectural Design
    - Environment Models
    - Physical Components
    - Algorithms

**Implementation**
- Component Design
  - Test vectors and expected responses
- Integration Testing
  - Run system tests in simulation
- System Tests
  - Run system tests on integrated controller
- Component Tests
  - Run component tests on target

**Validation/Acceptance**
- Code Verification and Validation
  - Subsystem Integration & Test
  - System-Level Integration & Test
  - User Acceptance Testing
    - Complete Integration & Test
Examples of software safety requirements

- Use Polyspace to assist with analysis of equivalence classes
  - Analysis of interface data into the unit
  - Analysis of control modes within the unit

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>1b Generation and analysis of equivalence classes</td>
<td>++</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SW Unit 1</th>
<th>SW Unit 2</th>
<th>SW Unit 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

invalid valid invalid

A B C
Example: Equivalence class testing at unit level

```c
#include <Add1_file.h>

int16 Add1(int16 u1, int16 u2)
{
    return u1+u2;
}
```

Testing

```c
int test_add( int a, int b )
{
    int c = Add1(a, b);
    if ( a >= 0 && b >= 0 && c < 0 )
        fprintf ( stderr, "Overflow!\n" );
    if ( a < 0 && b < 0 && c >= 0 )
        fprintf ( stderr, "Underflow!\n" );
    return c;
}
```
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Initiation</th>
<th>Architecture</th>
<th>Design/Implementation</th>
<th>Unit Testing</th>
<th>Integration Testing</th>
</tr>
</thead>
</table>

**System validation/acceptance Tests**

**User Acceptance Testing**

**Integration Testing**

**System Tests**

**Component Tests**

<table>
<thead>
<tr>
<th>REQUIREMENTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Architectural Design</td>
</tr>
<tr>
<td>Environment Models</td>
</tr>
<tr>
<td>Physical Components</td>
</tr>
<tr>
<td>Algorithms</td>
</tr>
</tbody>
</table>

**Implementation**

<table>
<thead>
<tr>
<th>IMPLEMENTATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>C, C++</td>
</tr>
<tr>
<td>VHDL, Verilog</td>
</tr>
<tr>
<td>Structured Text</td>
</tr>
<tr>
<td>MCU, DSP, FPGA, ASIC, PLC</td>
</tr>
</tbody>
</table>

**Code Verification and Validation**
Examples of software safety requirements

Use Polyspace to help with identification and analysis of boundaries

- Identification of Zero divisor
- Range analysis of boundaries

Testing at the edge of equivalence partition
Example: Optimize Design and Architecture decision

Non Robust Module

External code

Potential Runtime Error inside!!!
Example: Optimize Design and Architecture Decisions

Non Robust Module

Additional Range-Limiting Code

Free from Runtime Errors
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
Resume: Scope of the metrics - Key Categories

- Quality Plan
- Detailed Design Description
- Code Metrics
- MISRA-2004 Rules
- Un-reachable Branches
- Non-terminating Constructs
- Run-time Errors
- Dataflow Analysis

SQO

Software Quality Objectives
A quality model called SQO

- **Key Categories**
  - List of suggested quality objectives
  - Thresholds to reach quality requirements
  - Built on metrics from HIS*

*) Hersteller Initiative Software (HIS)

Example of Software Quality Requirement defined in SQO:

3.7. **Systematic runtime errors**

SQR-200 The supplier shall demonstrate that for all files within a module a review of systematic runtime errors has been performed and that errors which have not been corrected are justified, for the following categories:

- Out-of-bounds array access
- Division by zero
- Read access to non-initialized data
Introducing the Software Quality Objectives (SQO) project

- ISO-26262 doesn’t detail how to set up OEM/suppliers interface

- OEM and suppliers have to agree on:
  - A quality model and a process guide
  - Compliant to ISO-26262

- One example is “SQO”:
  - OEM and suppliers created a working group*
  - They published a document named “Software Quality Objectives for Source Code”

The SQO group started in 2007 with OEMs, and extended to suppliers

* MathWorks acted as a facilitator in the group
Software Quality Objectives: Incremental Quality

- **SQO Step 1**: Quality Plan & Detailed Design, Code Metrics, 1st MISRA-2004 rules subset
- **SQO Step 2**: Systematic run-time errors, Non terminating constructs
- **SQO Step 3**: Unreachable branches
- **SQO Step 4**: 1st subset of potential run-time errors, 2nd MISRA-2004 rules subset, 2nd subset of potential run-time errors
- **SQO Step 5**: 3rd subset of potential run-time errors, Dataflow Analysis
- **SQO Step 6**: Start of Production

Start → Design → Prototyping → Testing → Start of Production
SQO is compliant with ISO 26262

IEC certification process requires to define a quality model and its application.

<table>
<thead>
<tr>
<th>ISO 26262 objective</th>
<th>SQO level required</th>
<th>No/Partial/ Full coverage</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Enforcement of low complexity</td>
<td>SQO-1</td>
<td>Full</td>
<td></td>
</tr>
<tr>
<td>1b Use of languages subsets</td>
<td>SQO-5</td>
<td>Full</td>
<td></td>
</tr>
<tr>
<td>1c Enforcement of strong typing</td>
<td>SQO-5</td>
<td>Full</td>
<td></td>
</tr>
<tr>
<td>1d Use of defensive implementation techniques</td>
<td>SQO-5</td>
<td>Partial</td>
<td>MISRA rules about if and switch statements</td>
</tr>
<tr>
<td>1e Use of established design principles</td>
<td>SQO-5</td>
<td>Partial</td>
<td>Some design guidelines are checked at the code level with MISRA</td>
</tr>
<tr>
<td>1f Use of unambiguous graphical representation</td>
<td>N/A</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1g Use of style guides</td>
<td>N/A</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>1h Use of naming conventions</td>
<td>SQO-5</td>
<td>Partial</td>
<td>Naming of Global Variables</td>
</tr>
</tbody>
</table>

It’s not an additional task of the certification process.
Using tools to implement SQO
Example SQR-150: Code complexity
Coverage: Full

Tools exist!

• To create reports and automate ISO 26262 AND SQO activities
• PASS/FAIL status for each objective
• Progress monitoring over time
• Clear list remaining items to be reviewed/fixed
• Pre-qualified for all ISO 26262 ASIL
Summary: Typical engineering challenges …

- Check MISRA
- Optimize Design and Architecture
- Measure Code Quality
- Comply with ISO, IEC safety requirements
- Deliver Bug free software
- Reduce time and efforts for software testing
Thanks!

Interested to reduce your ISO/IEC compliance effort?