Unifying Model and Code Verification
Motivation

- Most controls applications are a combination of model-based generated code and hand code
- How do I efficiently verify this mix of hand code and generated code?
- MathWorks has tools for verifying models and tools for verifying code
- Is there a workflow for me to use these tools in a complementary, optimum way?
Case Study: Cruise Control Application

Objective: set cruise control target speed and pedal position based on driver & vehicle inputs

Cruise Control Application (C code)
- Hand code components
- Model-based Stateflow component
- Model-based S-function component

65 mph
Case Study: Cruise Control Architecture

System Inputs
- Cruise Power
- Brake
- Vehicle Speed
- Coast/Set
- Accel/Resume

Function Scheduler
- Read Inputs
- Fault Logging
- Target Speed Control Module
- Pedal Command Control Module
- Write Outputs

System Outputs
- Target Speed
- Engaged
- Pedal Position
Workflow for integrated Model-based and Hand Code Components
Workflow for integrated Model-based and Hand Code Components

Hand Code
- Software requirements
- Architectural design
- Unit design specification
- Unit design specification
- (Manual) implementation
- (Hand-written) C/C++ code

S-function Code
- Pedal Command Control Module
- Integrate as s-function

Cruise Control Application
- Read Inputs
- Fault Logging
- Write Outputs
- Compiled code
- Object code
- Compilation and linking

MBD Generated Code
- Software requirements
- Executable specification
- Model used for production code generation
- Generated C/C++ code

Target Speed Control Module
- Code generation
- Modeling
• Check MISRA compliance (Mdl Advisor)
Checking Model for MISRA compliance with Model Advisor
Checking Model for MISRA compliance with Model Advisor
Checking Model for MISRA compliance with Model Advisor

- Checks model design and code configuration settings
- Increases likelihood of generating MISRA C:2012 compliant code
Design Error Detection

- Check MISRA compliance (Mdl Advisor)
- Check model early for design errors
Floats to Integers: Checking the Model for Design Errors

- Simulink Design Verifier identifies design errors on the model
- These “dead logic” errors would prevent successful functional testing

Target Speed Control Module
Root Cause Analysis/Fix of Dead Logic

- Dead logic due to “uint8” operation on incdec/holdrate*10
- Fix change the order of operation 10*incdec/holdrate
Simulation and Test

- Functional testing (simulation)
Functional Testing Workflow

Requirements

Tests

Did we meet our requirements?

Review functional behavior

Did we completely test our model?

Structural coverage report

1. disabled (off) during start-up and not engaged (inactive)
2. not engaged (inactive) with enabling (on)
3. disengaged (not active) when disabled (off)
4. initial transition from disengaged (inactive) to engaged (active) only with "Set Speed" input after enabling (on)
Simulink Test™

- Authoring Tests
- Managing Tests
- Execution of Tests

- Key Features
  - Test harness
  - Test sequence block for running tests and assessments
  - Pass-fail criteria, including tolerances, limits, and temporal conditions
  - Baseline, equivalence, and back-to-back testing
  - Automatic report generation to document test outcomes
Functional Testing of Pedal Command (S-Function)

Coverage analysis for the model and the s-function code.

```c
25 {
  while((u >= X[index]) && (index < (mySize-1)))
26 { 
    index++; 
}
```

Uncovered Links:

**Metric**
- Decision (D1): 100% (2/2) decision outcomes
- Condition (C1): 75% (3/4) condition outcomes

**Conditions analyzed:**

<table>
<thead>
<tr>
<th>Description</th>
<th>True</th>
<th>False</th>
</tr>
</thead>
<tbody>
<tr>
<td>u &gt;= X[index]</td>
<td>105</td>
<td>21</td>
</tr>
<tr>
<td>index &lt; (mySize-1)</td>
<td>105</td>
<td>0</td>
</tr>
</tbody>
</table>
Back-to-Back Comparison Test (ISO 26262)

**Table 10 — Methods for software unit testing**

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Requirements-based test^a</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1b Interface test</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1c Fault injection test^b</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1d Resource usage test^c</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1e Back-to-back comparison test between model and code, if applicable^e</td>
<td>+</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td></td>
</tr>
</tbody>
</table>

^a The software requirements of the unit level are the basis for this requirements-based test.

^b This includes injection of arbitrary faults (e.g., by corrupting values of variables, by introducing code mutations, or by corrupting values of CPU registers).

^c Some aspects of the resource usage test can only be evaluated properly when the software unit tests are executed on the target hardware or if the simulator for the target processor supports resource usage tests.

^d This method requires a model that can simulate the functionality of the software units. Here, the model and code are stimulated in the same way and results compared with each other.

**Table 13 — Methods for software integration testing**

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1a Requirements-based test^a</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1b Interface test</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1c Fault injection test^b</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

^^ e This method requires a model that can simulate the functionality of the software components. Here, the model and code are stimulated in the same way and results compared with each other.
Check the Generated Code for Equivalent Model Behavior

- Integrated SIL mode support for model-to-code equivalence testing
- Coverage report for generated code for a detailed equivalence analysis
Optional: Automatic Code Reviews
Automatic Code Reviews

Model and code development

Simulink Code Inspector ®
Independent code inspection

- Static verification tool.
- Checks the generated code against model

Code Inspection Report
Traceability report
Functional testing (simulation)

• Code coverage (SIL)
SL Design Verifier created test cases to cover all possible “Decision/Condition” objectives in the model and s-function code.
Simulink Design Verifier – Test Generation for Modules

Overview

- **Input**
  - Model
  - Coverage metric
    - Decision coverage
    - Condition coverage
    - MC/DC
    - Custom Objectives (requirements-based)

- **Optional Input**
  - Modifiable parameter sets
  - Existing coverage data

- **Results**
  - Harness model
  - Input test signals
  - Unreachable objects
  - Detailed reports
Simulink Design Verifier – Property Proving

Overview

- Inputs
  - Model
  - Requirements
- Optional Inputs
  - Assumptions
- Property Proving
  - Proof satisfied or
  - Proof falsified
  - Counterexample
- Detailed reports
Simulink Design Verifier – Use Cases

Model Slicing

Test Generation

Design Error Detection

Property Proving
Issues Found on HIL Bench…

- The Cruise Control powered off during fault testing
- And, the Target Speed never exceeded 40 mph
Polyspace product family for C/C++

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

- Polyspace Bug Finder
  - Quickly find bugs in embedded software
  - Check code compliance for MISRA and JSF
  - Intended for every day use by software engineers

Ada language also supported for proving code
Customer Lookup Table: Checking the S-Function Code for Runtime Errors

```c
while((u >= X[index]) && (index < (mySize)))
{
    index++;
}
```

! **Pointer access out of bounds (Impact: High)**

Attempt to dereference pointer at index 11. Valid range: [0 .. 10]
Root Cause Analysis/Fix of S-Function Run-time Errors

```c
/* Definition for custom storage class: Global */

real32_T PedalCmdY[11] = { 0.0F, 0.5F, 1.0F, 1.5F, 2.0F, 2.5F,
                         3.0F, 3.5F, 4.0F, 4.5F, 5.0F } ;

int8_T SpeedDelX[11] = { -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 } ;

float Lookup1D_C(char u, char const X[], float const Y[])
{
    float y = 0.0f;
    unsigned char index = 0;
    float temp = 0.0f;

    unsigned char mySize = 11;

    if (engaged) {
        PedalPos = Lookup1D_C( (int8_T)rtb_Sum, (int8_T*)(&SpeedDelX[0]),
                               u, X[index], temp, index);
    } else {

        while((u >= X[index]) && (index < mySize)) {
            index++;
        }
    }

    else
    {
        while((u >= X[index]) && (index < (mySize-1))) {
            index++;
            if (index > 0)
```

Pedal Command Control Module
Configuring Polyspace from the Model
Launching Polyspace from the Model
Review Bug Finder MISRA results

MISRA AC AGC 8.10 (Obligatory)
All declarations and definitions of objects or functions at file scope shall have internal linkage unless external linkage is required.

Variable 'AccelResSw' should have internal linkage.

Polyspace Bug Finder - CruiseControl_PS C:\Demo\VnV\VnV_Wkshp

Results Summary

All results

Family | Information | File

MISRA AGC 18

1 Environment 4

8 Declarations and definitions 14

8.10 All declarations and definitions of objects or functions at file scope shall have internal linkage unless external linkage is required.

Category: Obligatory

CruiseControl_PS.c

Global:

boolean_T AccelResSw;

boolean_T Brake;

boolean_T CoastSetSw;
Reduce MISRA violations with “Code Placement” setting

<table>
<thead>
<tr>
<th>Select:</th>
<th>Commonly Used Parameters</th>
<th>All Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>Solver</td>
<td>Global data placement (custom storage classes only)</td>
<td></td>
</tr>
<tr>
<td>Data Import/Export</td>
<td>Data definition:</td>
<td>Data defined in a single separate source file</td>
</tr>
<tr>
<td>Optimization</td>
<td>Data definition filename:</td>
<td>cruise_control_global.c</td>
</tr>
<tr>
<td>Diagnostics</td>
<td>Data declaration:</td>
<td>Data declared in a single separate header file</td>
</tr>
<tr>
<td>Hardware Implementation</td>
<td>Data declaration filename:</td>
<td>cruise_control_global.h</td>
</tr>
<tr>
<td>Model Referencing</td>
<td>#include file delimiter:</td>
<td>Auto</td>
</tr>
<tr>
<td>Simulation Target</td>
<td>Use owner from data object for data definition placement</td>
<td></td>
</tr>
<tr>
<td>Code Generation</td>
<td>Global data placement (MPT data objects only)</td>
<td></td>
</tr>
<tr>
<td>Report</td>
<td>Signal display level:</td>
<td>10</td>
</tr>
<tr>
<td>Comments</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Symbols</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom Code</td>
<td>Code Packaging</td>
<td>File packaging format: Modular</td>
</tr>
<tr>
<td>Interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Code Style</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Templates</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Target Speed Control Module
Justify other violations by adding annotation

Target Speed Control Module
What support is there for analyzing the integrated code?

- Check integrated code for run-time errors
  - Polyspace
Why code verification? Code verification is exhaustive!

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

Statically and semantically verifies all possible executions of your code (considering all possible inputs, paths, variable values)

```c
static void pointer_arithmetic(void) {
    int array[100];
    int *p = array;
    int i;

    for (i = 0; i < 100; i++) {
        *p = 0;
        p ++;
    }

    if (get_bus_status() > 0) {
        if (get_oil_pressure() > 0) {
            *p = 5;
        } else {
            i++;
        }
    }

    i = get_bus_status();
    if (i > 0) {
        if (i < 10) {
            p = 10;
        }
    }
}
```
Creating a Code Prover project to check the Integrated Code

- Read Inputs
- Write Outputs
- Scheduler
- Fault Logging

Target Speed Control Module
Pedal Command Control Module
Code Integration Check with Polyspace:
Non-terminating loop in Hand Code

SysTick_Handler.c  scheduler_executive.c  monitor_builtin_test_faults.c  fault_log.c

SysTick_Handler  scheduler_executive  monitor_builtin_test_faults  fault_log

Fault Logging

/* Store the current fault into circular buffer */
for (ix = 0; ix < 12u; ix++)
{
    FaultInfoElement[FaultRecIndexCntr + ix] = *pFIt;
    *pFIt = 0x00u;
pFIt++;
}

? Illegally dereferenced pointer ?
Warning: pointer may be outside its bounds
Dereference of local pointer 'pFIt' (pointer to unsigned int 32, size: 32 bits):
  Pointer is not null.
  Points to 4 bytes at offset multiple of 4 in [0 .. 40] in buffer of 40 bytes, so may be outside bounds.

Non-terminating loop ?
The loop is infinite or contains a run-time error.
loop may fail due to a run-time error (maximum number of iterations: 11)
void fault_log(FAULT_LOG_INFO_T *pFaultInfo)
{
    uint32_t ix;

    uint32_t *pFlt = (uint32_t *)pFaultInfo;

    /* Validate current fault index counter */
    if (FaultRecIndexCntr >= (MAX_FAULT_LOG_INFO_SIZE - 12u))
    {
        FaultRecIndexCntr = 0x00u;
    }

    /* Store the current fault into circular buffer */
    for (ix = 0; ix < 12u; ix++)
    {
        FaultInfoElement[FaultRecIndexCntr + ix] = *pFlt;
        *pFlt = 0x00u;
        pFlt++;
    }

    /* Update the circular buffer fault index counter */
    FaultRecIndexCntr += ix-1;
}
Code Integration Check with Polyspace: Dead Code Found in Generated Code

Vehicle speed signal propagated to “CruiseControl_PS.c” [0 … 40]

Maximum target speed = 90

Unreachable/Dead code

```c
} else if (Speed > maxtspeed) {
    /* Transition: '<S1>:114' */
    /* Exit Internal 'ON': '<S1>:54' */
    DW.is_ON = CruiseControl_IN_NO_ACTIVE_CHILD;
    DW.is_CRUISE = CruiseControl_PS_IN_STANDBY;
    /* Entry 'STANDBY': '<S1>:52' */
    engaged = false;
```
Root Cause for Dead Code: Speed Sensor Input Hand Code

Changing analog-to-digital converter from 14 to 12-bit results in dead code

```
/* Conversion factors of speed */
#define NEW_ECU
#ifdef NEW_ECU
    #define SPEED_MASK 0xFFF
#else
    #define SPEED_MASK 0x3FFF /* Original design specification */
#endif

/* Scaling for conversion factor for translating sensor input to miles/hr */
#define CONV_FACTOR 0.01 /* FAILS */

#define MAX_AI_RAW_COUNTS_BUFFER_SIZE 10
AI_Speed.Speed = ((AI_Speed.Average & SPEED_MASK) * CONV_FACTOR);

/* Updated analog inputs */
MDB_Shared_Data.Speed = AI_Speed.Speed;
```
Workflow Summary: Complementary Model & Code Verification

- Functional testing (simulation)
- Check model early for design errors
- Check MISRA compliance (Mdl Advisor)
- Code coverage (SIL)
- SIL mode support
- Check integrated code for run-time errors
- Check s-function code for run-time errors
- Check MISRA compliance (Polyspace)

MBD Generated Code

Textual requirements → Executable specification → Model used for production code generation → Generated C/C++ code → Object code

Modeling → Code generation → Compilation and linking
ISO 26262 Structure

- ISO 26262-1: Vocabulary
- ISO 26262-2: Management of functional safety
- ISO 26262-3: Concept phase
- ISO 26262-4: Product development: system level
- ISO 26262-5: Product development: hardware level
- ISO 26262-6: Product development: software level
- ISO 26262-7: Production and operation
- ISO 26262-8: Supporting processes
- ISO 26262-9: ASIL-oriented and safety-oriented analyses
- ISO 26262-10: Guideline

ISO 26262-11: Model-Based Design
ISO 26262-12: Early verification and validation
ISO 26262-13: Code generation
ISO 26262-14: Tool classification and qualification
ISO 26262 Tool Qualification Approach - Details

I. Tool Classification

<table>
<thead>
<tr>
<th>Tool use cases</th>
<th>Tool impact</th>
<th>Tool error detection</th>
<th>Tool confidence level</th>
</tr>
</thead>
<tbody>
<tr>
<td>UC 1..n</td>
<td>T1 1</td>
<td>TD 1, High</td>
<td>TCL 1, not required</td>
</tr>
<tr>
<td></td>
<td>T1 2</td>
<td>TD 2, Medium</td>
<td>TCL 2</td>
</tr>
<tr>
<td></td>
<td>T1 3</td>
<td>TD 3, Increasing</td>
<td>TCL 3, Qualification methods for TCL3</td>
</tr>
</tbody>
</table>

II. Tool Qualification

- ASIL
- Qualification methods for TCL3
- Qualification methods for TCL2
- Qualification not required

Increasing qualification requirements
Qualification of MathWorks Tools

Tool qualification may involve multiple parties

- **Tool user**
  - Responsible for final tool qualification in the context of the application

- **Tool vendor**
  - Conducts generic pre-classification and pre-qualification based on reference use cases / reference workflow

- **3rd party assessor** (optional)
  - Provides independent assessment of reference workflow and pre-qualification artifacts

![MathWorks Pre-classification / qualification based on typical use cases (reference workflows)](TÜV SÜD Independent Assessment)

ISO 26262 Tool Qualification Kit

Tool User
Project-specific adaptation
Independent Assessment by TÜV SÜD

Example

Assessment Report

Report to the Certificate
Z10 11 01 67052 008
Software Tools for Safety Related Development
Simulink® Verification and Validation™
Simulink® Design Verifier™

Manufacturer:
The MathWorks, Inc.
3 Apple Hill Drive
Natick, MA 01760 USA

Report No.: MNB5534C
Revision 1.1 dated Jan. 26th 2011

5.2 Usage considerations for development processes which need to comply with IEC 61508, ISO 26262, EN 50128, or derivative standards

The capabilities of Simulink® Verification and Validation™ and Simulink® Design Verifier™ listed in sections 2.1.2 and 2.2.2 respectively are certified for use in development processes which need to comply with IEC 61508, ISO 26262, EN 50128, or derivative standards. The two verification tools allow the automation of core verification and validation activities for Simulink models and generated code.
A Complementary Model and Code Verification Process …

- Model and code checks before functional testing to minimize rework
- Perform functional, dynamic testing with model and code structural analysis with automation, and reuse of test assets
- Analyze the code to find issues resulting from the integration of
  - hand code
  - s-function code
  - model-based generated code
- Includes formal methods analysis to go beyond functional testing
- Enables more, early testing of the model and code
- Continual increase in design confidence
Thank You!
Process Compliance Demonstration

Annotated method tables with suggestions on how to use Model-Based Design processes and tools to apply the methods listed in ISO 26262-6

### Table 9 - Methods for Verification of Software Unit Design and Implementation

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th>Applicable Model-Based Design Tools and Processes</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Walkthrough</td>
<td>++ +</td>
<td>Simulink</td>
<td>Unit design walkthroughs can be based on a model, a generated Web View, or an SDD report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Simulink Report Generator – Web View, System Design Description (SDD) report</td>
<td>Code walkthroughs can be based on HTML code generation reports or code generation reports with an integrated Web View of the model.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Embedded Coder – Code generation report</td>
<td></td>
</tr>
<tr>
<td>Inspection</td>
<td>++ ++</td>
<td>Simulink</td>
<td>Unit design inspections can be based on a model, a generated Web View, or an SDD report.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Simulink Report Generator – Web View, System Design Description (SDD) report</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Simulink Verification and Validation – Model Advisor checks</td>
<td>Unit design inspections can be supported by ISO 26262.</td>
</tr>
</tbody>
</table>

### Table 10 - Methods for Software Unit Testing

<table>
<thead>
<tr>
<th>Methods</th>
<th>ASIL</th>
<th>Applicable Model-Based Design Tools and Processes</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>1a</td>
<td>++ ++</td>
<td>Simulink Verification and Validation – Requirements Management Interface (RMI)</td>
<td>RMI can be used to establish bidirectional links between textual requirements and models.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>IEC Certification Kit – Traceability matrix</td>
<td>Generated traceability matrices can be used to document and review existing links between textual requirements, models, and code.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Simulink – Signal Builder block</td>
<td>Generated test vector charts can be used to create open-loop model tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>StateFlow – Dynamic test vector charts</td>
<td>Dynamic test vector charts can be used to create closed-loop, reactive model tests.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Simulink Verification and Validation – Component testing capabilities</td>
<td>Component testing capabilities can be used to create model test harnesses. They also enable a requirements pane in the Signal Builder that can be used to link tests with textual requirements.</td>
</tr>
</tbody>
</table>
ISO 26262 – Walk-through and Inspection

“[..] unit specification design and implementation can be verified at the model level.”

ISO 26262 (2011)

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

\(^a\) In the case of model-based software development the software unit specification design and implementation can be verified at the model level.

\(^b\) Methods 1e and 1f can be applied at the source code level. These methods are applicable both to manual code development and to model-based development.

\(^c\) Methods 1e and 1f can be part of methods 1d, 1g or 1h.

\(^d\) Method 1h 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.

NOTE Table 9 lists only static verification techniques. Dynamic verification techniques (e.g. testing techniques) are covered in Tables 10, 11 and 12.
Qualification of Model-Based Design Tools

☑ pre-qualified for all ASILs according to ISO 26262
## Defects detected by Polyspace Bug Finder

### Numerical
- Integer division by zero
- Float division by zero
- Integer conversion overflow
- Unsigned integer conversion overflow
- Sign change integer conversion overflow
- Float conversion integer overflow
- Float conversion overflow
- Integer overflow
- Unsigned integer overflow
- Float overflow
- Invalid use of std. library integer routine
- Invalid use of std. library float routine
- Shift of a negative value
- Shift operation overflow

### Static memory
- Array access out of bounds
- Null pointer
- Pointer access out of bounds
- Uninitialized cast of function pointer
- Uninitialized cast of pointer
- Invalid use of std. library memory routine
- Invalid use of std. library string routine
- Arithmetic operation with NULL pointer
- Wrong allocated object size for cast
- Local address escape
- Buffer overflow from incorrect string format specifier

### Dynamic memory
- Use of previously freed pointer
- Unprotected dynamic memory allocation
- Release of previously deallocated pointer
- Invalid free of pointer
- Memory leak

### Programming
- Invalid use of = operator
- Invalid use of == operator
- Declaration mismatch
- Invalid use of floating point operation
- Wrap-around on unsigned integer
- Assertion
- Invalid use of other standard lib. routine
- Missing null in string array
- Qualifier removed in conversion
- Wrong type used in sizeof
- Format string specifiers and arguments mismatch
- Writing to const qualified object

### Dataflow
- Write without further read
- Non-initialized variable
- Non-initialized pointer
- Variable shadowing
- Missing or invalid return statement
- Dead code
- Partially access array
- Uncalled function
- Pointer to non initialized value converted to const pointer
- Code deactivated by constant false condition
- Unreachable code
- Useless if

### Concurrency
- Race condition (atomic / non atomic)
- Missing lock/unlock
- Deadlock
- Double lock/unlock

### Resources management
- Use of previously closed resource
- Resource leak
- Writing to read-only resource

### Security / tainted data (38 checkers)
- chroot misuse
- Use of dangerous standard function
- Mismatch between data length and size
- Use of non-secure temporary file
- Sensitive heap not cleared
- Tainted array index
- Tainted external command
- Tainted integer division

### Object oriented (12 checkers)
- Object slicing
- Copy constructor not called
- Member not initialized in constructor
- …
Defects detected by Polyspace Bug Finder

Numerical
- Integer division by zero
- Float division by zero
- Integer conversion overflow
- Unsigned integer conversion overflow
- Sign change integer conversion overflow
- Float conversion overflow
- Integer overflow
- Unsigned integer overflow
- Float overflow
- Invalid use of std. library integer routine
- Invalid use of std. library float routine
- Shift of a negative value
- Shift operation overflow

Dynamic memory
- Use of previously freed pointer
- Unprotected dynamic memory allocation
- Release of previously deallocated pointer
- Invalid free of pointer
- Memory leak

Programming
- Invalid use of = operator
- Invalid use of == operator
- Declaration mismatch
- Invalid use of floating point operation
- Wrap-around on unsigned integer
- Assertion
- Invalid use of other standard lib. routine
- Missing null in string array
- Qualifier removed in conversion
- Wrong type used in sizeof
- Format string specifiers and arguments mismatch
- Writing to const qualified object

Dataflow
- Write without further read
- Mixed initialized variable
- Non-initialized pointer
- Variable shadowing
- Missing or invalid return statement
- Dead code
- Partially access array
- Uncalled function
- Pointer to non initialized value converted to const pointer
- Code deactivated by constant false condition
- Unreachable code
- Useless if

Security / tainted data (38 checkers)
- chroot misuse
- Use of dangerous standard function
- Mismatch between data length and size
- Use of non-secure temporary file
- Sensitive heap not cleared
- Tainted array index
- Tainted external command
- Tainted integer division

Object oriented (12 checkers)
- Object slicing
- Copy constructor not called
- Member not initialized in constructor
- ...

Static memory
- Array access out of bounds
- Null pointer
- Pointer access out of bounds
- Unreliable cast of function pointer
- Unreliable cast of pointer
- Invalid use of std. library memory routine
- Invalid use of standard library string routine
- Arithmetic operation with NULL pointer
- Wrong allocated object size for cast
- Local address escape
- Buffer overflow from incorrect string format specifier

Concurrency
- Race condition (atomic / non atomic)
- Missing lock/unlock
- Deadlock
- Double lock/unlock

Resources management
- Use of previously closed resource
- Resource leak
- Writing to read-only resource

Good practice
- Large pass-by-value argument
- More than one statement
- Delete of void pointer
- Hard-coded buffer size / loop boundary
- Unused parameter

Checkers inherited from Code Prover
Full list of run-time error checks in Polyspace Code Prover

C run-time checks
• Unreachable Code
• Out of Bounds Array Index
• Division by Zero
• Non-Initialized Variable
• Scalar and Float Overflow (left shift on signed variables, float underflow versus values near zero)
• Initialized Return Value
• Shift Operations (shift amount in 0..31/0..63, left operand of left shift is negative)
• Illegal Dereferenced Pointer (illegal pointer access to variable of structure field, pointer within bounds)
• Correctness Condition (array conversion must not extend range, function pointer does not point to a valid function)
• Non-Initialized Pointer
• User Assertion
• Non-Termination of Call (non-termination of calls and loops, arithmetic expressions)
• Known Non-Termination of Call
• Non-Termination of Loop
• Standard Library Function Call
• Absolute Address
• Inspection Points

C++ run-time checks
• Unreachable Code
• Out of Bounds Array Index
• Division by Zero
• Non-Initialized Variable
• Scalar and Float Overflow
• Shift Operations
• Pointer of function Not Null
• Function Returns a Value
• Illegal Dereferenced Pointer
• Correctness Condition
• Non-Initialized Pointer
• Exception Handling (calls to throws, destructor or delete throws, main/tasks/C_lib_func throws, exception raised is not specified in the throw list, throw during catch parameter construction, continue execution in __except)
• User Assertion
• Object Oriented Programming (invalid pointer to member, call of pure virtual function, incorrect type for this-pointer)
• Non-Termination of Call
• Non Termination of Loop
• Absolute Address
• Potential Call
• C++ Specific Checks (positive array size, incorrect typeid argument, incorrect dynamic_cast on reference)
Examples of software safety requirements

<table>
<thead>
<tr>
<th>Topics</th>
<th>ASIL A</th>
<th>ASIL B</th>
<th>ASIL C</th>
<th>ASIL D</th>
</tr>
</thead>
<tbody>
<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>0</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>1g Use of style guides</td>
<td>+</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
<tr>
<td>1h Use of naming conventions</td>
<td>++</td>
<td>++</td>
<td>++</td>
<td>++</td>
</tr>
</tbody>
</table>

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

Detect and correct areas with high complexity

Polyspace Metrics
Examples of software safety requirements

Enforcement of coding guidelines

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

Polyspace Metrics
Reference Workflow

Model-Based Design for ISO 26262

Modeling standards checking (Simulink V&V)

Simulation / model testing (Simulink, Simulink Test)
Model coverage Req. Mgmt. Int. (Simulink V&V)

Module and integration testing at the model level

Review and static analysis at the model level

PIL test (Embedded Coder)

Traceability matrix analysis (IEC Certification Kit) or model vs. code coverage (Simulink V&V)

Equivalence testing

Prevention of unintended functionality

Textual requirements

Executable specification

Model used for production code generation

Generated C code

Object code

Modeling

Simulink/Stateflow

Code generation

Embedded Coder

Compilation and linking

Third-party tool
**Advanced Reference Workflow**

**Additional Best Practices**

- Modeling standards checking (Simulink V&V)
- Property Proving, Design Error Detection (Simulink Design Verifier)
- Simulation / model testing (Simulink, Simulink Test)
- Model coverage Req. Mgmt. Int. (Simulink V&V)
- Module and integration testing at the model level
- Review and static analysis at the model level
- PIL test (Embedded Coder)
- Test generation (Simulink Design Verifier)
- Run-time error detection (Polyspace products)
- Traceability matrix analysis (IEC Certification Kit) or model vs. code coverage (Simulink V&V)
- MISRA-C checking (Polyspace products)
- Prevention of unintended functionality
- Equivalence testing

---

Textual requirements → Executable specification → ...

Model used for production code generation → Generated C code → Object code

Simulink/Stateflow → Embedded Coder

Simulation / model testing

Modeling

Code generation → Compilation and linking

Third-party tool
Workflow Summary:
Complementary Model & Code Verification

- Check s-function code for run-time errors
- Check integrated code for run-time errors
- Check MISRA compliance (Polyspace)
Model-Based Design
Verification and Validation

Requirements Traceability
• Navigation and Reports

Modeling Standards Checking
• Automatic Review

Testing and Test Automation
• Test Authoring
• Coverage Analysis
• Automatic Test Case Generation

Property Proving
• Quickly find incorrect behavior
• Prove correctness of behavior

Static Analysis on Model and Code
• Identify defects
• Prove absence of runtime errors
• Compliance to coding standards

Compliance to ISO 26262
• Workflow and tool qualification
Verification on Code Level – Polyspace

- Finds bugs
- Checks coding rule conformance (MISRA/JSF/Custom)
- Provides metrics (Cyclomatic complexity etc.)
- Proves the existence and absence of errors
- Indicates when you’ve reached the desired quality level