About the Company

- Verocel, Inc. founded in 1999
- Subsidiaries in UK, Germany and Poland
- Software verification services
  - Firm fixed price with a certification warranty
- Software verification tools, including
  - VeroTrace
  - VerOCode
- Standards used include DO-178C, IEC 61508, EN 50128
Why use software that was not developed to the relevant standards?

- Selling a product developed for a wider market into a safety-critical market, e.g. Wind River VxWorks
- Selling a product developed for one safety critical market in another, e.g. creating IEC 61508 certification evidence for Wind River VxWorks DO-178B
- Selling a product developed for one geographical market in another, e.g. needing to meet European standards
- Software developed for a different certification regime, e.g. software developed for a civil airliner reused on a military aircraft
- Legacy software developed prior to current standards, e.g. transitioning from EN 50128:2001 to EN 50128:2011
Verocel Experience of Reverse Engineering

- Wind River operating systems
  - VxWorks Cert
  - VxWorks 653
  - MILS
  - Hypervisor
- AdaCore GNAT Pro Safety-Critical certification package
- Eclipse 500 Electrical Power Management System
- Automatic Train Protection System (EN 50128 SIL 4)
- FAA-sponsored research on “Reverse Engineering Software and Digital Systems”
- ...etc.
Gap Analysis

• Identify gaps in the certification evidence
• Every project is different
  – Most projects do a reasonable job of software/hardware integration testing against a Software Requirements Specification
  – Design documentation often incomplete or out-of-date
  – Traceability often missing or incomplete
  – Software integration testing or component testing not always carried out
  – Test coverage not always measured
Importing Existing Documents
Importing Existing Requirements From DOORS
Creating Additional Requirements

Function Level Requirement

Ref. No: 28 - Version 1

State
- Incomplete
- Developed
- Ready For Review
- Failed
- Passed

Review State
- Incomplete
- Invaldated
- Ongoing
- Failed
- Passed

Development State
- Incomplete
- Complete

IA Required
- Yes
- No

Label
- SRD.2.1

Author
- Abramkiewicz, Krysztof

Function Name
- calcPwmValue

Viscosity
- Global
- Local

Properties
- Not A Requirement
- Not A Functional Requirement
- Derived
- Robustness
- Boundary
- Safety

Statement
This function shall calculate a value to be written to a PWM register based on a requested duty cycle.

Context
PWM register is 16 bits wide. The duty cycle value in the range [0; 100][%] is rescaled to the range [0; 65535], and the calculated value is then returned.
Developing Test Cases
Developing Test Procedures
Testing

- We test the integrated binary image running on the target computer
- Code under test is not changed
- Verocel Test Harness automates test execution
Test Coverage

- EN 50128 highly recommends
  - statement coverage for SIL 1 or SIL 2
  - branch and compound condition coverage for SIL 3 or SIL 4

Table A.21 – Test Coverage for Code

<table>
<thead>
<tr>
<th>Test coverage criterion</th>
<th>SIL 0</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement</td>
<td>D.50</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
</tr>
<tr>
<td>Branch</td>
<td>D.50</td>
<td>-</td>
<td>R</td>
<td>R</td>
<td>HR</td>
</tr>
<tr>
<td>Compound Condition</td>
<td>D.50</td>
<td>-</td>
<td>-</td>
<td>R</td>
<td>HR</td>
</tr>
<tr>
<td>Data flow</td>
<td>D.50</td>
<td>-</td>
<td>-</td>
<td>R</td>
<td>HR</td>
</tr>
<tr>
<td>Path</td>
<td>D.50</td>
<td>-</td>
<td>-</td>
<td>R</td>
<td>HR</td>
</tr>
</tbody>
</table>

**Requirements:**
1) For every SIL, a quantified measure of coverage shall be developed for the test undertaken. This can support the judgment on the confidence gained in testing and the necessity for additional techniques.
2) For SIL 3 or 4 test coverage at component level should be measured according to the following:
   - 2 and 3, or
   - 2 and 4, or
   - 5
   or test coverage at integration level should be measured according to one or more of 2, 3, 4 or 5.
3) Other test coverage criteria can be used, given that this can be justified. These criteria depend on the software architecture (see Table A.3) and the programming language (see Table A.10 and Table A.19).
4) Any code which it is not practicable to test shall be demonstrated to be correct using a suitable technique,
   e.g. static analysis from Table A.19.

**NOTE 1** Statement coverage is automatically achieved by Items 2 to 5.

**NOTE 2** The test coverage criteria in this table are used for structure-based (code-based, white box) testing. Test case measures for functional (specification-based, black box) testing are given in Table A.14.

**NOTE 3** A high percentage of coverage is usually difficult to achieve. The use of test case execution from boundary values (D.4) and equivalence classes and input partition testing (D.18) can enable a sufficient coverage to be achieved with a smaller number of tests.

**NOTE 4** The difference between 2 and 3 is dependent in practice on the level of the programming language and the use of compound conditions. When single conditions are used only, for example as a result of compilation, 2 and 3 are considered identical.
Test Coverage

• Provides evidence that all the code has been exercised
• Helps demonstrate absence of unintended functions
• Establishes the thoroughness of the requirements-based tests
VerOCode

- Suitable up to and including EN 50128 SIL 4
- Measures structural coverage without needing to instrument the source code
Rich Traceability
Presenting the Certification Evidence

- Delivered on a DVD
- ISA/regulator can browse the evidence using any web browser
- We offer a certification warranty
Presenting the Certification Evidence