Evaluation and Improvement of ETCS Test Cases for the Ceiling Speed Monitor

Jan Peleska, Cecile Braunstein, Wen-ling Huang, Felix Hübner, and Uwe Schulze
Background

- ERTMS/ETCS specification describes system test cases in SUBSET-076
- These test cases have the following objectives
  - Verify availability and correctness of essential functions
  - Verify conformance to the standard
Evaluation Technique

• Develop a test model for the CSM

• Formalise SUBSET-076 CSM tests so that they can be used for
  • test data generation and
  • test execution in RT-Tester model-based testing environment

• Develop a reference specification
Evaluation Technique

• Create mutants of the reference implementation

• **Test Suite A.** Run SUBSET-076 test suite against the mutants

• **Test Suite B.** Run extended SUBSET-076 test suite against the mutants, where sub-requirements have been considered

• **Test Suite C.** Run “standard” RT-Tester MBT tests against the mutants (transition coverage, MC/DC coverage …)

• **Test Suite D.** Run novel equivalence class strategy against the mutants

• Compare the **model coverage** and the **mutation score** achieved
Main Results – Requirements Coverage / Model Coverage

Table IX. Requirements Coverage and Model Coverage Overview.

<table>
<thead>
<tr>
<th>Requirement Coverage (ETCS specification)</th>
<th>Manually Defined Tests (A)</th>
<th>Extended Manual Tests (B)</th>
<th>Automatically Defined Tests (C)</th>
<th>Equivalence Class Testing (D)</th>
</tr>
</thead>
<tbody>
<tr>
<td>24 of 29 (82.76%)</td>
<td>29 of 29 (100%)</td>
<td>29 of 29 (100%)</td>
<td>29 of 29 (100%)</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test Cases</th>
<th>9</th>
<th>11</th>
<th>45</th>
<th>5524</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Coverage States</td>
<td>9 of 9 (100%)</td>
<td>9 of 9 (100%)</td>
<td>9 of 9 (100%)</td>
<td>9 of 9 (100%)</td>
</tr>
<tr>
<td>Model Coverage Transitions</td>
<td>10 of 10 (100%)</td>
<td>10 of 10 (100%)</td>
<td>10 of 10 (100%)</td>
<td>10 of 10 (90%)</td>
</tr>
<tr>
<td>Model Coverage MCDC</td>
<td>8 of 10 (80%)</td>
<td>8 of 10 (80%)</td>
<td>10 of 10 (100%)</td>
<td>10 of 10 (100%)</td>
</tr>
<tr>
<td>Model Coverage HITR</td>
<td>1 of 5 (20%)</td>
<td>3 of 5 (60%)</td>
<td>5 of 5 (100%)</td>
<td>5 of 5 (100%)</td>
</tr>
</tbody>
</table>
Main Results – Mutation Score

Table X. Mutation Score Overview.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of Test Cases</strong></td>
<td>9</td>
<td>11</td>
<td>45</td>
<td>5524</td>
</tr>
<tr>
<td><strong>Mutation Score</strong></td>
<td>108 of 186 (58 %)</td>
<td>116 of 186 (62 %)</td>
<td>126 of 186 (68 %)</td>
<td>186 of 186 (100 %)</td>
</tr>
</tbody>
</table>
Remarks

• Equivalence class testing method is complete with respect to a given fault domain

• Every correct behaviour of an SUT will be accepted (soundness)

• Every erroneous behaviour of the SUT will be rejected, provided that the true SUT behaviour is inside a (very large) set of pre-defined behavioural models (exhaustiveness)

• Experiments have shown that the equivalence class strategy also shows superior test strength for SUT behaviours outside the fault domain
Improvements for SUBSET-076

• We can easily improve the ETCS SUBSET-076 test suite by a (not too large) number of test cases:
  
  • Add test cases for case distinctions in the guard conditions concerning overspeeding
  
  • Add some boundary value test
CSM-Behaviour – Detailed Guard Conditions

\[ dV_{\text{warning}}(V_{MRSP}) = \begin{cases} \min \left\{ \frac{1}{3} + \frac{1}{30} \cdot V_{MRSP}, 5 \right\} & \text{if } V_{MRSP} > 110 \\ \frac{1}{4} & \text{if } V_{MRSP} \leq 110 \end{cases} \]  

\[ dV_{\text{sbi}}(V_{MRSP}) = \begin{cases} \min \left\{ 0.55 + 0.045 \cdot V_{MRSP}, 10 \right\} & \text{if } V_{MRSP} > 110 \\ 5.5 & \text{if } V_{MRSP} \leq 110 \end{cases} \]  

\[ dV_{\text{ebi}}(V_{MRSP}) = \begin{cases} \min \left\{ -0.75 + 0.075 \cdot V_{MRSP}, 15 \right\} & \text{if } V_{MRSP} > 110 \\ 7.5 & \text{if } V_{MRSP} \leq 110 \end{cases} \]
Admissible tolerance is constant in ranges $V_{\text{mrsp}}$ in $[0, 110]$, $[210, \text{max}]$ and increases with constant gradient in range $[110, 210]$

$$dV_{\text{ebi}}(V_{MRSP}) = \begin{cases} 
\min\{-0.75 + 0.075 \cdot V_{MRSP}, 15\} & \text{if } V_{MRSP} > 110 \\
7.5 & \text{if } V_{MRSP} \leq 110
\end{cases}$$

Test Case 1

Test Case 2

Test Case 3
Appendix II
The Ceiling Speed Monitoring Model
The CSM Model

• Three variants of speed monitoring are performed by the ETCS onboard computer (EVC European Vital Computer)

1. **Ceiling speed monitoring (CSM)** – supervise observance of maximal speed allowed according to speed profile

2. **Target speed monitoring** – enforce speed restrictions while train brakes to a target

3. **Release speed monitoring** – supervises speed while train approaches end of movement authority
The CSM Model – SysML

- **Model structure**
  - Top-down decomposition of blocks
  - First decomposition shows interface between test environment (TE) and system under test (SUT)
  - Last decomposition is associated with behaviour

- **Model behaviour** is represented by means of
  - Block operations
  - State machines
The CSM Model – TE-SUT Interface

Diagram showing the interaction between the System Under Test (SUT) and the Test Environment (TE). It includes interfaces for OdometryIn, SpeedRestrictionIn, NationalValuesIn, SnDMonitorIn, DMIOut, and TIOut. Additionally, there are enumeration types for DMICmd and V_est.
The CSM Model – TE-SUT Interface

V_{est}: estimated speed

V_{mrsp}: maximal speed allowed
The CSM Model – TE-SUT Interface

allowRevokeEB: release condition for emergency brake

SBAvailable: configuration switch for service brake
csmSwitch: activation switch for CSM functionality
The CSM Model – TE-SUT Interface

DMICmd: indications on driver-machine interface
The CSM Model – TE-SUT Interface

DMICmd: indications on driver-machine interface

NORMAL | OVERSPEED | WARNING | INTERVENTION
The CSM Model – TE-SUT Interface

**TICmd**: Train interface commands to service brake and emergency brake
The CSM Model – TE-SUT Interface

**TICmd**: Train interface commands to service brake and emergency brake

- NO_CMD
- SERVICE_BRAKE_CMD
- EMER_BRAKE_CMD
The CSM Model – CSM Block

composite structure SystemUnderTest

- FlowPort OdometryIn
- FlowPort SpeedRestrictionIn
- FlowPort NationalValuesIn
- FlowPort SnDMonitorIn
- FlowPort DMIOut
- FlowPort TIOut

«block,SUT»
SystemUnderTest

«block»
SystemUnderTest::CSM

- sbiCmd : int = SERVICE_BRAKE_CMD
  + calc_permitted_speed_to_driver() : void
  + calc_speed_onboard(int) : void
  + calc_speed_to_driver() : void
  + dV_ebi(float) : float
  + dV_sbi(float) : float
  + dV_warning(float) : float
CSM-Behaviour – Detailed
Guard Conditions

\[ dV_{\text{warning}}(V_{MRSP}) = \begin{cases} \min\left\{ \frac{1}{3} + \frac{1}{30} \cdot V_{MRSP}, 5 \right\} \quad \text{if } V_{MRSP} > 110 \\ 4 \quad \text{if } V_{MRSP} \leq 110 \end{cases} \] 

(1)

\[ dV_{\text{sbi}}(V_{MRSP}) = \begin{cases} \min\left\{ 0.55 + 0.045 \cdot V_{MRSP}, 10 \right\} \quad \text{if } V_{MRSP} > 110 \\ 5.5 \quad \text{if } V_{MRSP} \leq 110 \end{cases} \] 

(2)

\[ dV_{\text{ebi}}(V_{MRSP}) = \begin{cases} \min\left\{ -0.75 + 0.075 \cdot V_{MRSP}, 15 \right\} \quad \text{if } V_{MRSP} > 110 \\ 7.5 \quad \text{if } V_{MRSP} \leq 110 \end{cases} \] 

(3)
Admissible tolerance is constant in ranges $V_{\text{mrsp}}$ in $[0,110]$, $[210,\text{max}]$ and increases with constant gradient in range $[110,210]$

$$dV_{\text{ebi}}(V_{\text{MRSP}}) = \begin{cases} 
\min\{-0.75 + 0.075 \cdot V_{\text{MRSP}}, 15\} & \text{if } V_{\text{MRSP}} > 110 \\
7.5 & \text{if } V_{\text{MRSP}} \leq 110 
\end{cases}$$
Appendix II
Complete Model-based Equivalence Class Partitioning Strategy
Complete Test Strategy

- System domain
  - Strategy is specified on semantic level: Reactive State Transition Systems (RSTS)
  - All concrete modelling formalisms whose semantics can be encoded as RSTS, inherit test strategy from RSTS
Complete Test Strategy

- **Reactive State Transition Systems (RSTS)**

\[ S = (S, s_0, R) \]

\[ S \subseteq V \rightarrow D \quad \text{Variable valuation functions} \]

\[ V = I \cup M \cup O \quad \text{Input, internal, output variable symbols} \]

\[ D = \text{Variable domains} \]

\[ R \subseteq S \times S \quad \text{transition relation} \]

- **Types of input variables may be infinite**
Complete Test Strategy

• Reactive State Transition Systems (RSTS)
  • Quiescent states: accept inputs, have quiescent or transient post states
  • Transient states: do not accept inputs, have quiescent post states
  • Livelock free
Complete Test Strategy

changes outputs and internal state, deterministic

only inputs change

Reactive State Transition Systems (RSTS)
Complete Test Strategy

- **I/O equivalence**

  Two states are I/O-equivalent if every input trace applied to these states lead to the same output trace observable in quiescent states.

  \[ s \sim s' \equiv \forall \tau = \vec{c}_1 \ldots \vec{c}_n \in D_I^* : (s/\tau)|_O = (s'/\tau)|_O \]
Complete Test Strategy

- **I/O equivalence**
  - Two states are I/O-equivalent if every input trace applied to these states lead to the same output trace observable in quiescent states.
  
  
  - Two systems are I/O-equivalent if their initial states are I/O equivalent.

\[
s \sim s' \equiv \forall \nu = \vec{c}_1 \ldots \vec{c}_n \in D^*_I, \quad (s/\nu)|_O = (s'/\nu)|_O
\]
Complete Test Strategy

- I/O equivalence

  - Two states are I/O-equivalent if every input trace applied to these states lead to the same output trace observable in quiescent states

  - Two systems are I/O-equivalent if their initial states are I/O equivalent

\[ s \sim s' \equiv \forall \tau = \tilde{c}_1 \ldots \tilde{c}_n \in D_I^*: (s/\tau)|_O = (s'/\tau)|_O \]

resulting quiescent state trace, restricted to outputs
Complete Test Strategy

- **Input Equivalence Class Partitioning (IECP)**

  - Factorise quiescent states into **I/O-equivalence classes** $q$
  
  - Factorise input space into **input equivalence classes (IEC)** $X$, such that
    
    - For all inputs $c$ of input equivalence class $X$
    
    - For all I/O-equivalence classes $q$
    
    - For all states $s$ in $q$
      
      - $s/c$ resides in the same target I/O-equivalence class $B(q,X)$
Complete Test Strategy

• Input Equivalence Class Partitioning (IECP)
  • Factorise quiescent states into I/O-equivalence classes $q$
  • Factorise input space into input equivalence classes (IEC) $X$, such that
    • For all inputs $c$ of input equivalence class $X$
    • For all I/O-equivalence classes $q$
    • For all states $s$ in $q$
      • $s/c$ resides in the same target I/O-equivalence class $B(q,X)$
Complete Test Strategy

- **Fault model**
  - Reference model
  - Conformance relation
  - Fault domain

\[ \mathcal{F} = (\mathcal{S}, \sim, \mathcal{D}(\mathcal{S}, m, \mathcal{I}_2)) \]
Complete Test Strategy

CSM model as RSTS – semantic representation of SysML model

\[ \mathcal{F} = (\mathcal{S}, \sim, \mathcal{D}(\mathcal{S}, m, \mathcal{I}_2)) \]
Complete Test Strategy

$I/O$-equivalence as conformance relation

\[ \mathcal{F} = (S, \sim, D(S, m, I_2)) \]
Complete Test Strategy

Maximal number of I/O-equivalence classes for each member of the fault domain

\[ \mathcal{F} = (S, \sim, D(S, m, I_2)) \]
Complete Test Strategy

A refined IECP – satisfying

\[ \forall X \in \mathcal{I}, X' \in \mathcal{I}' : \\
    (X \cap X' \neq \emptyset \Rightarrow \\
    \exists X_2 \in \mathcal{I}_2 : X_2 \subseteq X \cap X') \]

\[ \mathcal{F} = (\mathcal{S}, \sim, \mathcal{D}(\mathcal{S}, m; \mathcal{I}_2)) \]
Complete Test Strategy

A refined IECP – satisfying

\[ \forall X \in \mathcal{I}, X' \in \mathcal{I}' : (X \cap X' \neq \emptyset \Rightarrow \exists X_2 \in \mathcal{I}_2 : X_2 \subseteq X \cap X') \]

\[ \mathcal{F} = (\mathcal{S}, \sim, \mathcal{D}(\mathcal{S}, m; \mathcal{I}_2)) \]
Complete Test Strategy

A refined IECP – satisfying

\[ \forall X \in \mathcal{I}, X' \in \mathcal{I}': (X \cap X' \neq \emptyset \Rightarrow \exists X_2 \in \mathcal{I}_2 : X_2 \subseteq X \cap X') \]

\[ \mathcal{F} = (\mathcal{S}, \sim, \mathcal{D}(\mathcal{S}, m; \mathcal{I}_2)) \]

IECP of fault domain member
Complete Test Strategy

A refined IECP – satisfying

\[ \forall X \in \mathcal{I}, X' \in \mathcal{I}' : (X \cap X' \neq \emptyset \Rightarrow \exists X_2 \in \mathcal{I}_2 : X_2 \subseteq X \cap X') \]

\[ \mathcal{F} = (\mathcal{S}, \sim, \mathcal{D}(\mathcal{S}, m; \mathcal{I}_2)) \]
If $X$ triggers behaviour in some CSM state $s$, and $X'$ triggers non-conforming behaviour of RSTS representing SUT behaviour, then there exists $X_2$ in intersection of $X$, $X'$, and a member of $X_2$ will be used in the test.

$$\forall X \in \mathcal{I}, X' \in \mathcal{I}': (X \cap X' \neq \emptyset \Rightarrow \exists X_2 \in \mathcal{I}_2, X_2 \subseteq X \cap X')$$

$$\mathcal{F} = (S, \sim, \mathcal{D}(S, m, \mathcal{I}_2))$$
Complete Test Strategy

**Theorem.** Given any IECP, create input alphabet $A$ by selecting one input candidate $c$ from each IEC $X$.

For arbitrary input trace $\mathfrak{i}$, there exists another input trace $\tau$ in $A^*$, such that $\mathfrak{i}$ and $\tau$ produce the same outputs, when applied to any start state $s$.

\[
\forall \mathfrak{i} \in D_I^* : \exists \tau \in A^* : \forall s \in S : \# \mathfrak{i} = \# \tau \land (s/\mathfrak{i})|_O = (\tau/\mathfrak{i})|_O
\]
Complete Test Strategy

- I/O-equivalence class factorisation and IECP induce complete DFSM abstraction of test model

- Extract input DFSM alphabet \( A \) from refined IECP \( I_2 \)

- Apply complete DFSM strategy for DFSM fault model with maximal number of states \( m \) and conformance relation DFSM-equivalence – Complete DFSM strategies are, e.g., W-Method or Wp-Method

- **Theorem.**
  
  DFSM(reference model) DFSM-equivalent to DFSM(implementation) if and only if
  
  RSTS(reference model) I/O-equivalent to RSTS(implementation)
Normal or Overspeed

Warning

Service Brake Intervention

Emergency Brake Intervention

\( \bar{c}_3, \bar{c}_4/(3, 0) \)

\( \bar{c}_5/(4, 2 - sb_0) \)

\( \bar{c}_6/(4, 2) \)

\( \bar{c}_1, \bar{c}_3, \bar{c}_4, \bar{c}_5, \bar{c}_6/(4, 2) \)

\( \bar{c}_4/(3, 0) \)

\( \bar{c}_1, \bar{c}_2/(0, 0) \)

\( \bar{c}_5/(4, 2 - sb_0) \)

\( \bar{c}_3, \bar{c}_4, \bar{c}_5/(4, 2 - sb_0) \)

\( \bar{c}_6/(4, 2) \)

\( \bar{c}_2/(0, 0) \)

\( \bar{c}_1, \bar{c}_2/(0, 0) \)

\( \bar{c}_3/(2, 0) \)
# Test suites resulting from W-Method application

<table>
<thead>
<tr>
<th>$\tilde{c}_i$</th>
<th>$V_{est}$</th>
<th>$V_{MRSP}$</th>
<th>allowRevokeEB</th>
<th>$X_i$</th>
<th>specified by</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\tilde{c}_1$</td>
<td>60</td>
<td>90</td>
<td>0</td>
<td>$X_1$</td>
<td>$0 &lt; V_{est} \leq V_{MRSP} \land$ allowRevokeEB = 0</td>
</tr>
<tr>
<td>$\tilde{c}_2$</td>
<td>60</td>
<td>90</td>
<td>1</td>
<td>$X_2$</td>
<td>$V_{est} = 0 \lor (V_{est} \leq V_{MRSP} \land$ allowRevokeEB = 1)</td>
</tr>
<tr>
<td>$\tilde{c}_3$</td>
<td>152</td>
<td>150</td>
<td>0</td>
<td>$X_3$</td>
<td>$V_{MRSP} &lt; V_{est} \leq V_{MRSP} + dV_{\text{warning}}(V_{MRSP})$</td>
</tr>
<tr>
<td>$\tilde{c}_4$</td>
<td>125</td>
<td>120</td>
<td>1</td>
<td>$X_4$</td>
<td>$V_{MRSP} + dV_{\text{warning}}(V_{MRSP}) &lt; V_{est} \leq V_{MRSP} + dV_{\text{sbi}}(V_{MRSP})$</td>
</tr>
<tr>
<td>$\tilde{c}_5$</td>
<td>66</td>
<td>60</td>
<td>0</td>
<td>$X_5$</td>
<td>$V_{MRSP} + dV_{\text{sbi}}(V_{MRSP}) &lt; V_{est} \leq V_{MRSP} + dV_{\text{ebi}}(V_{MRSP})$</td>
</tr>
<tr>
<td>$\tilde{c}_6$</td>
<td>260</td>
<td>230</td>
<td>0</td>
<td>$X_6$</td>
<td>$V_{MRSP} + dV_{\text{ebi}}(V_{MRSP}) &lt; V_{est}$</td>
</tr>
</tbody>
</table>

Coarsest IECP

\[ \text{TEST\_SUITE}_{sb_0=1} = \{ \tilde{c}_i \cdot \tilde{c}_j \cdot \tilde{c}_k \cdot \tilde{c}_3 \mid i, j, k = 1, \ldots, 6 \} \cup \{ \tilde{c}_j \cdot \tilde{c}_i \cdot \tilde{c}_k \cdot \tilde{c}_h \cdot \tilde{c}_3 \mid h, i, k = 1, \ldots, 6, \ j = 4, \ldots, 6 \} \]

\[ \text{TEST\_SUITE}_{sb_0=0} = \{ \tilde{c}_i \cdot \tilde{c}_j \cdot \tilde{c}_h \cdot \tilde{c}_g \mid h, i, j = 1, \ldots, 6, \ g = 1, 3 \} \cup \{ \tilde{c}_j \cdot \tilde{c}_i \cdot \tilde{c}_k \cdot \tilde{c}_h \cdot \tilde{c}_g \mid h, i, k = 1, \ldots, 6, \ j = 4, \ldots, 6, \ g = 1, 3 \} \]