CityMobil

Certification Procedure

Jan van Dijke
Senior Project Manager
TNO Technical Sciences
Certification procedures

- Introduction
- Presentation of the TNO safety assessment method
Certification procedures

Status at the beginning of CityMobil

- Certification procedures exist for most products
- More and more often on European level
- Extensive range of European procedures in automotive world
- Limited range of European procedures in rail world
- Procedures for automated vehicles are almost non-existing
Certification procedures

Problems to be addressed:

- Levels of intelligence in transport systems are increasing
- Levels of complexity are increasing
- Traditional methods for test- and certification are not always sufficient anymore
- There is a need for a new approach:

A uniform method for safety assessment and certification of Intelligent Transport Systems
Certification procedures

Characterisation of traditional transport systems

- Driver is always in control (required by law)
- Straightforward relationships between input and output
- Technical and other requirements are laid down in (international) standards: EC; ECE; FMVSS
- Compliance with requirements can be established through standard (technical) tests
Certification procedures

Characterisation of Intelligent Transport Systems

Control is (partly) taken away from driver
- Complicated relationships between input and output
- Components are part of an “integrated system”
- Compliance cannot always be established through simple tests
- There are, as yet, no widely accepted certification standards
A method for safety assessment should be

- Uniform
- Suitable for the whole safety lifecycle
- Suited to become a certification standard
- Based on existing standards where possible
- At European level (world wide?)
Certification procedures

Certification of intelligent transport systems:
Proposed approach:

1. Establish an accepted safety level

2. Carry out a system safety analysis to show that the system is safe under varying (failure) conditions, using a standard system safety analysis method

3. Establish whether or not the system meets the accepted safety level

4. Check compliance with functional specifications through (existing) technical tests
Certification procedures

1. Establish an accepted safety level

How safe is “safe enough”?
Certification procedures

- Reference: Comparable road traffic
- Reference value: Fatalities in road traffic
- Basic assumption: AGV’s must be twice as safe as comparable traditional vehicles
### Certification procedures

Accepted (!?) safety level: Statistics

<table>
<thead>
<tr>
<th>Mode</th>
<th>Casualties / $10^9$ travellerkm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Car</td>
<td>5.9</td>
</tr>
<tr>
<td>Bus</td>
<td>0.4</td>
</tr>
<tr>
<td>Railways</td>
<td>4.2</td>
</tr>
</tbody>
</table>
Certification procedures

Statistics: reality

Europe 2004  
casualties / $10^9$ travellerkm

+ 5.9

+ 0.4

+ 4.2
Certification procedures

Establish an accepted safety level

- Practical example, Europe 2004:
  - 5.9 casualties per $10^9$ travellerkm

- Autonomous systems: assume that safety level should at least be 2 times better:
  - max 3 casualties per $10^9$ travelled km.
Certification procedures

2. Evaluate the design, using a standard system safety analysis method

Requirements:

- Method must enable assessment of the system as a whole as well as individual subsystems
- Method can be used in different stages of the design process (safety lifecycle)
- Link with IEC 61508 must be possible:
- Results must be objective and repeatable
Certification procedures

FMECA: Failure modes, effects and criticality analysis

- Suited for complete ITS systems and for subsystems
- Independent of type of subsystem
- Can be used as a design tool in different stages of the design process
- Link with IEC 61508 safety levels is possible
- However: Results depend on human assessments and ratings of failure modes and effects so repeatability and objectivity might be an issue
Certification procedures

System-safety Analysis process

Preparation
- Collect info
- Form a group of experts
- Establish safety criteria
- Define functional tests

System def & function analysis
- Divide in subsystems
- Define system boundaries
- Define inputs and outputs
- Define all system functions

FMECA
- Define failure modes
- Define causes
- Define effects
- Define safeguards
- Establish severity and likelihood
- Add recommendations
- Add comments

Conclusions & reporting
- Draw conclusions
- Make report
Certification procedures

Results of the analysis:

A combination of:
- Severity of the effect of a failure
- The likelihood that such an effect will occur as a result of that failure,
- The effect of built-in safeguards that mitigate the effects or the severity of such a failure
- The final result is a safety score for each failure mode/cause/effect combination in accordance with the following table
## Certification procedures

<table>
<thead>
<tr>
<th>Severity</th>
<th>LRes 1</th>
<th>Lres 2</th>
<th>Lres 3</th>
<th>Lres 4</th>
<th>Lres 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>S0 No injuries</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>S1 Moderate</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>S2 Serious</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>S3 Fatal</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>


Certification procedures

3. Establish whether or not the system meets the accepted safety level

- Accepted safety level:
  
  < 3 casualties per $10^9$ travellerkm

- assume average speed is 30 km/h
- $< 3 \times 30 / 10^9 = < 9 \times 10^{-8}$ casualties per hour
- $< 2.6$ per 10,000 years
## Certification procedures

<table>
<thead>
<tr>
<th>Severity</th>
<th>LRes</th>
<th>1/100000 years</th>
<th>1/10000 years</th>
<th>1/1000 years</th>
<th>1/100 years</th>
<th>1/10 years</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Lres 1</td>
<td>Lres 2</td>
<td>Lres 3</td>
<td>Lres 4</td>
<td>Lres 5</td>
</tr>
<tr>
<td>S0</td>
<td>No injuries</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>S1</td>
<td>Moderate</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>S2</td>
<td>Serious</td>
<td>5</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>S3</td>
<td>Fatal</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
</tr>
</tbody>
</table>
Certification procedures

4. Check compliance with technical requirements through existing technical tests

- Reduced number of test compared with present vehicles
- Tests to be carried out depend on type of component, vehicle or vehicle system
Certification procedures

- Procedure developed: 2002-2008 in the framework of European R&D projects
- Internal evaluations of TNO vehicles in 2003-2008
- Used for safety analysis of the Parkshuttle (Capelle a/d Ijssel, The Netherlands) in 2005/2006
- Used for certification of the CityMobil Rome demonstrator (Rome, Italy, 2009) and the Masdar PRT system.
Certification procedures

Conclusions:

- The method has proven valuable in evaluations of automated vehicles.
- The method is suited for autonomous vehicles, but also to evaluate the electronic systems of ADA vehicles.
- A vital next step is to convince certification authorities that the method is viable.
Certification procedures

Thank You