Day 2: Autonomous Vehicle Safety: How to Test, How to Ensure

Wednesday June 17, 2020
WELCOME TO
Day 2: Autonomous Vehicle Safety: How to Test, How to Ensure

Co-Moderator: Lori Dearman, Executive Webinar Producer
Housekeeping Tips

How to ask a question?
Who’s In the Audience?

A diverse audience of over 650 professionals registered from 50 countries, representing the following industries:

- **22%** Automotive
- **18%** Research
- **13%** University/Education
- **8%** Transportation/Logistics/ Asset Tracking
- **8%** Military and defense
- **4%** Machine control/mining/construction
- **3%** Precision Agriculture
- **24%** Other
Welcome from *Inside Unmanned Systems*

Richard Fischer  
Publisher  
*Inside GNSS*  
*Inside Unmanned Systems*
A word from the sponsor

Ajay Vemuru
Product Manager - PNT
Spirent Communications
Spirent

Your trusted PNT partner

visit spirent.com/pnt
Today’s Moderator

Alan Cameron
Editor in Chief
Inside GNSS
PNT Editor
Inside Unmanned Systems
WELCOME TO
Day 2: Autonomous Vehicle Safety: How to Test, How to Ensure

Co-Moderator: Lori Dearman, Executive Webinar Producer
What type of testing are you most familiar with?

Poll Results (single answer required):

- Live-sky: 34%
- Simulation: 43%
- Record and playback: 23%
Validating performance of Safety critical autonomous vehicle PNT systems

Ajay Vemuru
Product Manager - PNT
Spirent Communications
Hardware in the Loop (HIL) PNT Simulation

Simulated signals

Realtime processor
Vehicle model
ECM
Fault injection

Requirements Analysis
Architecture Partitioning
Algorithm Development
Model-Based Testing
System Integration
Code Generation

Early Validation of Requirements
Vehicle Integration & Testing
Spirent HIL setup
Realistic dynamics/trajectory
Who needs HIL

Automotive OEMs and Tier 1 suppliers
who want to test their PNT systems with driving simulators in a HIL environment

Teams working on Autonomy and Simulations
who want to test fusion systems with perception and path planning within their larger simulation environment

Source: google images
Enhanced HIL Setup

- In real time Spirent’s SimGEN can follow a given route, for instance from Google Maps, at a given real-time dynamic speed from a rolling road or any other source of motion.
Validating performance of safety critical autonomous vehicles PNT systems
## GNSS Test Methodologies

<table>
<thead>
<tr>
<th>Method / attribute</th>
<th>Live-sky</th>
<th>Simulation</th>
<th>Record &amp; playback system</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeatable</td>
<td>✗</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Controllable</td>
<td>✗</td>
<td>✓</td>
<td>Partial</td>
</tr>
<tr>
<td>Reference truth</td>
<td>✗</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>Realistic</td>
<td>✓</td>
<td>Representative*</td>
<td>✓</td>
</tr>
</tbody>
</table>

*and getting better and better!
AV Development Stages

Early Validation of Requirements

- Requirements Analysis
- Architecture Partitioning
- Algorithm Development

MiL
- Model-Based Testing

HiL
- System Integration

SysiL
- System Testing

SiL
- Code Generation

Vehicle Integration & Testing
Boundary Diagram concept

System Boundary / Device Under Test

Software Positioning Engine

**Inputs**
- Observation Data
- Navigation Data
- Configuration Data
- Weather
- IMU Data
- Corrections Data
- Many more inputs

**Outputs**
- Position Solution
- Velocity Solution
- Heading Solution
- Timing Solution
Level of Testing

BASIC

- Time to first fix
- Acquisition Sensitivity
- Tracking Sensitivity
- Static Position Accuracy
- Environmental Conditions
- Week Rollover (2019)

ADVANCED

COMPLIANCE

- ISO26262
- SOTIF
- Radio Equipment Directive (RED)
- GOST (Russia), eCall (EU)

Multipath
Jamming
Spoofing
Scintillation

Environmental Conditions
Simulator Key Performance Indicator

- Latest ICD Implemented
- Signal fidelity/Spectrum purity
- HUR/SIR and HIL (low latency)
- Scalability
- Automation
- Calibration (ISO 17025)
- Realism
Simulation Realism

- Atmospheric modelling
  - Ionosphere
  - Troposphere
  - Scintillation

Key parameters
Realistic error modelling (atmospheric and scintillation)
Remote interface for precise signal modification – support for user defined error models

- Environmental effect
  - Obscuration
  - Multipath
Record and Playback (RPS) system

How do you iterate design and test GNSS urban environment performance in the lab? E.g. Downtown Tokyo

The RPS can be used to record GNSS signals along a drive route in urban areas. E.g. mounted in vehicle

Other SOOP could also be recorded during the drive

These recordings can then be replayed in the lab, removing the need for repetitive live-sky testing
RPS Key Performance Indicator

- Quantization level
  - Signal fidelity
  - Dynamic range

- Clock stability and phase noise

- Large storage capacity

- GNSS + other signals

![Table showing recording time for different number of frequencies and storage capacities.](chart.png)
RPS GNSS + Other Signals

GNSS RF Signal
- Multi-Frequency
- Multi-Constellation
- Single or multiple antenna

Correction Data
- PPP over NTRIP
- RTK over serial bus

CAN/CAN-FD Data
- Dead-reckoning

Other Data
- IMU output (up to 8)
- Camera output (up to 4)

RECORD  REPLAY
Part I: Integrity for Precise Positioning in Automotive

Lance de Groot
Geomatics Lead, Safety
Critical Systems
Hexagon | NovAtel
Relevant Standards for GNSS in Automotive

01 ISO 26262
   - Road Vehicles – Functional Safety

02 ISO/PAS 21448
   - Road Vehicles – Safety of the Intended Function (SOTIF)

03 EN 16803
   - Use of GNSS-based positioning for road Intelligent Transport Systems

04 Others
   - IEC 61508, RTCM, NHTSA, 3GPP, …
ISO 26262 – Overview

Specialization of IEC 61508 for series production passenger vehicles
- Up to 3,500 kg

Addresses hazards caused by malfunction of the system

Defines processes and methods for:
- System, HW, and SW development
- Verification and validation
- Supporting processes
ISO 26262 – Concept Phase

<table>
<thead>
<tr>
<th>1. Vocabulary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Management of functional safety</td>
</tr>
<tr>
<td>3. Concept phase</td>
</tr>
<tr>
<td>4. Product development at the system level</td>
</tr>
<tr>
<td>5. Product development at the hardware level</td>
</tr>
<tr>
<td>6. Product development at the software level</td>
</tr>
</tbody>
</table>

5.1 Initiation of project development at the hardware level
5.2 Specification of hardware safety requirements
5.3 Configuration management
5.4 Verification

9. ASIL-oriented and safety-critical analyses
9.1 Requirements development with respect to ASIL tailoring
9.2 Analysis of dependent failures
9.3 Analysis of individual failures
9.4 Analysis of coherence of elements

10. Guideline on ISO 26262
ISO 26262 – Concept Phase

Hazard Analysis and Risk Assessment (HARA)
- Identify potential hazardous events
- Classified by severity, exposure, controllability – ASIL determination
- Define safety goals to address hazards

Functional Safety Concept
- How will we achieve the safety goals?
- Consider
  - Fault tolerant time interval
  - Degraded operation
  - Safe states

Example:
unintended steering at freeway speeds

- Uncontrollable (by driver)
- Life threatening
- High probability (of scenario)
ISO 26262 – System Design Phase

<table>
<thead>
<tr>
<th>1. Vocabulary</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Management of functional safety</td>
</tr>
<tr>
<td>3. Concept phase</td>
</tr>
<tr>
<td>4. Product development at the system level</td>
</tr>
<tr>
<td>5. Product development at the hardware level</td>
</tr>
<tr>
<td>6. Product development at the software level</td>
</tr>
<tr>
<td>7. Production and operation</td>
</tr>
<tr>
<td>8. Supporting processes</td>
</tr>
<tr>
<td>9. ASIL-oriented and safety-oriented analyses</td>
</tr>
<tr>
<td>10. Guideline on ISO 26262</td>
</tr>
</tbody>
</table>

| 2.1 Overall safety management | 2.6 Safety management during the concept phase and the product development | 2.7 Safety management after the item's release for production |

| 3.1 Term definition            | 3.2 Initiation of the safety lifecycle                                    |
| 3.3 Hazard analysis and risk assessment                                      | 3.4 Specification of the technical safety requirements                    |
| 3.5 System design                                                           |

| 4.1 Initiation of product development at the system level                    |
| 4.6 Functionality assessment                                                  |
| 4.7 System design                                                            |
| 4.8 Validation of the technical safety requirements                          |

| 5.1 Investigation of product development at the hardware level               |
| 5.2 Specification of hardware safety requirements                            |
| 5.3 Hardware design                                                          |
| 5.4 Evaluation of the hardware functionality                                |
| 5.5 Verification of the hardware safety requirements                         |
| 5.8 Software integration and testing                                        |
| 5.9 Verification of software safety requirements                            |

| 6.1 Integration of product development at the software level                  |
| 6.2 Software architecture design                                            |
| 6.3 Software unit design and implementation                                 |
| 6.4 Software unit testing                                                    |
| 6.5 Verification of software safety requirements                            |

| 8.1 Manuals and documentation                                               |
| 8.2 Configuration management                                                |
| 8.3 Change management                                                        |
| 8.4 Verification                                                             |

| 9.1 ASIL-orientation and safety-orientation analysis                         |
| 9.2 Safety evaluation                                                        |
| 9.3 Analysis of dependent failures                                           |

| 10.1 Guideline on ISO 26262                                                  |
ISO 26262 – System Design Phase

**Technical safety concept**
- Allocate safety requirements to architecture

**Safety requirements included in system design**

**Perform safety validation**
- FMEA
- FTA
- DFA

### Failure Mode and Effect Analysis

<table>
<thead>
<tr>
<th>Processor</th>
<th>Function</th>
<th>Possible Error</th>
<th>Cause</th>
<th>Detection Difficulty</th>
<th>Requirement</th>
<th>Status</th>
<th>Total Rx DoG</th>
<th>Preparation/Measure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Process 1</td>
<td>descrip func 1</td>
<td>fail cond 1</td>
<td>fail cause 1</td>
<td>result 1</td>
<td>3</td>
<td>5</td>
<td>bedenk oplossing 1</td>
</tr>
</tbody>
</table>
ISO 26262 – Hardware Design Phase

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>2-5 Overall safety management</td>
<td>2-6 Safety management during the concept phase and the product development</td>
<td>3-5 System definition</td>
<td>4-10 Release for production</td>
<td>5-6-7-8-9-10 Evaluation of the hardware functionality due to exceed hardware failures</td>
<td>6-7-8-9-10 Verification of software safety requirements</td>
<td>7-6 Production</td>
</tr>
<tr>
<td>3-6 Initiation of the safety lifecycle</td>
<td>3-7 Hazard analysis and risk assessment</td>
<td>3-8 Functional safety concept</td>
<td>4-10 Functional safety assessment</td>
<td>5-10 Software architectural design</td>
<td>6-7 Software unit design and implementation</td>
<td>7-6 Operation, service maintenance and repair, and decommissioning</td>
</tr>
<tr>
<td>3-9 System design</td>
<td></td>
<td></td>
<td>4-9 Safety validation</td>
<td>5-11 Software unit testing</td>
<td>6-8 Software integration and testing</td>
<td></td>
</tr>
<tr>
<td>3-10 Hazard analysis</td>
<td></td>
<td></td>
<td>4-8 System integration and testing</td>
<td>5-11 Verification of software safety requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4-11 Release for production</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-10 Documentation</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5-11 Use of software tools</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-12 Qualification of software components</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-13 Qualification of hardware components</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6-14 Use in use argument</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. Supporting processes

6. Supporting processes

9. ASIL-oriented and safety-oriented analyses

a. Requirement decomposition with respect to ASIL tailoring
b. Analysis of dependent failures
c. Other aspects for consistence of elements

d. Safety analysis

10. Guideline on ISO 26262
ISO 26262 – Hardware Design Phase

Define hardware safety requirements

Evaluate fault metrics - FMEDA
- Single Point Fault
- Dual Point Fault (ASIL C, D)
- Latent Fault
- FIT

<table>
<thead>
<tr>
<th>ASIL</th>
<th>SPF</th>
<th>LF</th>
<th>FIT  (1 FIT = 10⁻⁹/h)</th>
</tr>
</thead>
<tbody>
<tr>
<td>B</td>
<td>≥90%</td>
<td>≥60%</td>
<td>100</td>
</tr>
<tr>
<td>C</td>
<td>≥97%</td>
<td>≥80%</td>
<td>10</td>
</tr>
<tr>
<td>D</td>
<td>≥99%</td>
<td>≥90%</td>
<td>10</td>
</tr>
</tbody>
</table>
ISO 26262 – Software Design Phase
ISO 26262 – Software Design Phase

- Define hardware safety requirements
- Apply appropriate design principles, e.g.
  - Hierarchical structure
  - Loose coupling
  - Enforce low complexity
- Use suitable coding standards
  - E.g. MISRA C, MISRA C++
- Unit and integration test
  - Requirements coverage
  - Structural coverage

<table>
<thead>
<tr>
<th>ASIL</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement Coverage</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Branch Coverage</td>
<td></td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>MC/DC</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
</tbody>
</table>
ISO 26262 – Verification

1. Vocabulary

2. Management of functional safety
   2.1 Overall safety management
   2.2 Safety management during the concept phase and the product development
   2.3 Safety management after the item’s release for production

3. Concept phase
   3.1 Core-definition
   3.2 Initiation of the safety lifecycle
   3.3 Hazard analysis and risk assessment
   3.4 Functional safety concept

4. Product development at the system level
   4.1 Initiation of product development at the system level
   4.2 Specification of the technical safety requirements
   4.3 System design

5. Product development at the hardware level
   5.1 Initiation of product development at the hardware level
   5.2 Specification of hardware safety requirements
   5.3 Hardware design
   5.4 Evaluation of the inherent and residual fault-tolerance
   5.5 Realization of the safety case position due to modified hardware failures
   5.6 Hardware integration and testing
   5.7 Verification of software safety requirements

6. Product development at the software level
   6.1 Initiation of product development at the software level
   6.2 Software architectural design
   6.3 Software unit design and implementation
   6.4 Software unit testing
   6.5 Software integration and testing
   6.6 Verification of software safety requirements

7. Production and operation
   7.1 Production
   7.2 Operation, service maintenance and repair, and decommissioning

8. Supporting processes
   8.1 Interfaces within distributed developments
   8.2 Specification and management of safety requirements
   8.3 Configuration management
   8.4 Change management
   8.5 Verification
   8.6 Documentation
   8.7 Confidence in the use of software tools
   8.8 Qualification of software components
   8.9 Qualification of hardware components
   8.10 Proof of use argument
   8.11 Analysis of dependent failures
   8.12 Analysis of occurrence of failures

9. ASIL-oriented and safety-oriented analyses
   9.1 Requirements decomposition with respect to ASIL mapping
   9.2 Code for occurrence of elements
   9.3 Safety analyses
   9.4 Guideline on ISO 26262
ISO 26262 – Verification

- Occurs throughout the process

Focus on robust testing methods

- Analysis of boundary values
- Error guessing based on knowledge or experience
- Analysis of functional dependencies

1a Requirements-based test
1b Interface test
1c Fault injection test
1d Resource usage test

Requires confidence in tools

- Analogous to HARA
- Based the impact and detectability of tool errors

<table>
<thead>
<tr>
<th>Tool impact</th>
<th>TD1</th>
<th>TD2</th>
<th>TD3</th>
</tr>
</thead>
<tbody>
<tr>
<td>TI1</td>
<td>TCL1</td>
<td>TCL1</td>
<td>TCL1</td>
</tr>
<tr>
<td>TI2</td>
<td>TCL1</td>
<td>TCL2</td>
<td>TCL3</td>
</tr>
</tbody>
</table>
Ask the Experts

Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Ajay Vemuru
Product Manager - PNT
Spirent Communications

Ali Soliman
Business Development Manager, GNSS, PNT Technologies
Spirent Communications

Lance de Groot
Geomatics Lead, Safety Critical Systems
Hexagon | NovAtel
Experimentally validating the performance of safety-critical autonomous vehicle PNT system will require: (select one)

Poll Results (single answer required):

- A month’s worth of data: 7%
- A year’s worth of data: 28%
- 10 years’ worth of data: 29%
- Can all be done in simulation: 37%
Part II: Integrity for Precise Positioning in Automotive

Lance de Groot
Geomatics Lead, Safety Critical Systems
Hexagon | NovAtel
SOTIF – Overview

**Supplement to ISO 26262**

ISO 26262 focuses on hazards from failures in the E/E systems

**SOTIF** focuses on hazards that can occur even when the system itself is fault free

**Considerations:**
- Limitations in the function (e.g. image feature classification)
- Errors in external inputs (e.g. GNSS errors)

**ISO 26262 is safety of execution**
- Did we build it safely?

**SOTIF is safety of performance**
- Will it actually work safely?
SOTIF – Design Analysis

Hazard analysis

Similar to ISO 26262

Consider different triggering events
• Environmental conditions
• Known limitations of the system components
• Foreseeable misuse

Assess events by severity and controllability
SOTIF – Design Update

Modify design to avoid or mitigate unavoidable risks by:

- Improving performance
- Restricting operating environment
- Adding monitoring or fallback
- Improving testability
SOTIF – Verification and Validation

Verification must also consider SOTIF Risks

Consider response of sensors, algorithms, actuators to external failures and misuse

Evaluate residual risk of system, e.g.
- Randomized HiL/SiL
- Fleet tests
- Simulation
- Analysis (e.g. FTA)

Loss of Integrity
$10^{-6}$/h

OR

Faulted Conditions
$1\times10^{-7}$/h

Nominal Conditions
$9\times10^{-7}$/h

Satellite Fault
$4\times10^{-8}$/h

Atmospheric Fault
$2\times10^{-8}$/h

Local Environment Fault
$3\times10^{-8}$/h

Correction Fault
$1\times10^{-8}$/h

H/W Fault
$1\times10^{-8}$/h
EN 16803

European standard under development

Covers assessment of GNSS Based Positioning Technology in Intelligent Transportation Systems (ITS)

EN 16803-1
defines metrics for characterizing GBPT

EN 16803-2
will define requirements and classifications for basic performance

EN 16803-3
will define requirements and classifications for security performance

EN 16803-4
will define methods for verification of GBPT
Multipath and Obscuration
Bringing the Real World to the Lab

Environment

Physics Engine

Solver (Ray-Tracing)

Geometry / 3D

Material Properties

Moving Objects
Bringing the Real World to the Lab

- Environment
- Physics
- Solver (Ray-Tracing)
  - Signal Properties
  - Env. Interaction
  - GNSS Prop. Model
Bringing the Real World to the Lab

Environment

Physics

Solver (Ray-Tracing)

Object Intersection

Ray Selection

Optimisation
Bringing the Real World to the Lab

Environment

Physics

Solver (Ray-Tracing)
Sim3D
GNSS Antenna

- GNSS Antenna is an important input to the system.

- Simulation tool should provide the necessary parameters to ensure testing is representative of the real antenna performance.

- Some parameter that is supported in conducted simulation:
  - Antenna pattern (Gain/Phase)
  - Antenna polarization
  - Antenna placement relative to the vehicle
Zoned Chamber approach
Spoofing

- False location and time readings can have severe impacts on automated and autonomous devices
- Anti-spoofing will play an ever-increasing role in safety-critical applications – compliance with regulations and standards will soon be mandatory across multiple industries

**Key parameters**

- Signal fidelity
- Dedicated tools for testing anti-spoofing techniques
- Expertise in anti-spoofing test scenario design
Spirent Spoofing Capabilities

- The ‘multi-copy constellation’ feature
  - Allows up to 12 copies of a constellation to be simulated
  - Each with full manipulation of parameters (orbital, signal properties, additional errors etc.)

- The ‘n-vehicle to 1RF’ feature allows multiple spoofer trajectories to be simulated with one RF output.

- SimSAFE™ is Spirent's dedicated testing and monitoring tool for spoofing attacks
  - Different types spoofing: signal, data, nulling, or meaconing
  - Spoofing signal can synchronize to GNSS live-sky
Interference

GNSS signals are very weak and can be easily overshadowed by intentional or unintentional interference:

- Intentional
  - State-sponsored jamming
  - ‘Personal privacy devices’ fitted to company vehicles to prevent tracking of movement. The illegal use of PPDs is increasing.

- Unintentional
  - Harmonics
  - Adjacent band interference etc

Key parameters

Multiple interference sources – static or dynamic with precise phase alignment

Realistic propagation modelling
Spirent Interference Capabilities

- Embedded Interference
  - Simulate simultaneously GNSS and interference signal
  - In-band interference with realistic power modelling and precise phase alignment
  - Different interference types i.e. CW, PSK narrowband/ broadband, CW pulse, AWGN, FM, AM, PM

- GSS7765 - Interference Simulation System
  - Comprises one or more high quality commercial signal generators plus an Interference Combination Unit (ICU).
  - Output power of up to +10dBm
  - Broad range of interfering signal options for both in-band and out-band interference
**What are you most interested in testing for?**

Poll Results (single answer required):

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic system performance: sensitivity, accuracy, TTFF, etc.</td>
<td>20%</td>
</tr>
<tr>
<td>Performance under spoofing and/or jamming conditions</td>
<td>24%</td>
</tr>
<tr>
<td>Standards compliance: ISO 26262, SOTIF, etc.</td>
<td>11%</td>
</tr>
<tr>
<td>All of the above are equally important</td>
<td>45%</td>
</tr>
</tbody>
</table>
Ask the Experts

Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Ajay Vemuru
Product Manager - PNT
Spirent Communications

Ali Soliman
Business Development Manager, GNSS, PNT Technologies
Spirent Communications

Lance de Groot
Geomatics Lead, Safety Critical Systems
Hexagon | NovAtel