sponsored by Spirent — Promise. Assured. | InsideGNSS — GPS | GALILEO | GLONASS | BEIDOU | inside unmanned systems — INSIDE ENGINEERING, POLICY AND PRACTICE | HEXAGON | NovAtel

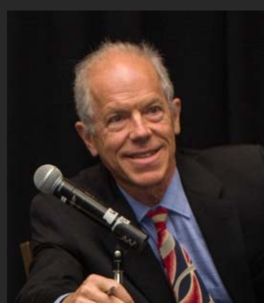
DAY 2

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



Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

Ajay Vemuru
Product Manager - PNT
Spirent Communications

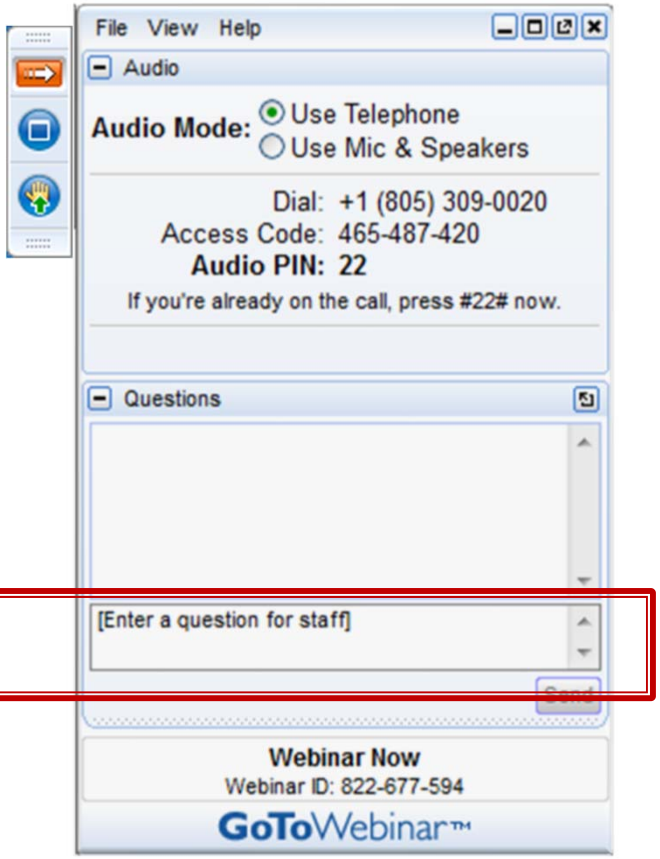
Ali Soliman
Business Development Manager, GNSS, PNT Technologies
Spirent Communications

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

Co-Moderator: Lori Dearman, Executive Webinar Producer

Housekeeping Tips

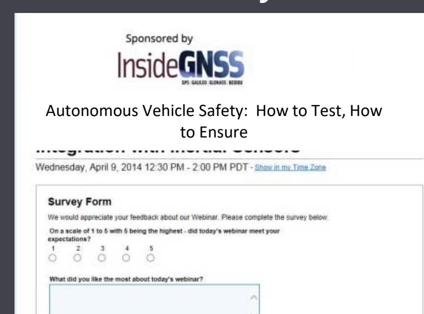
How to ask a question?



Recording

Poll

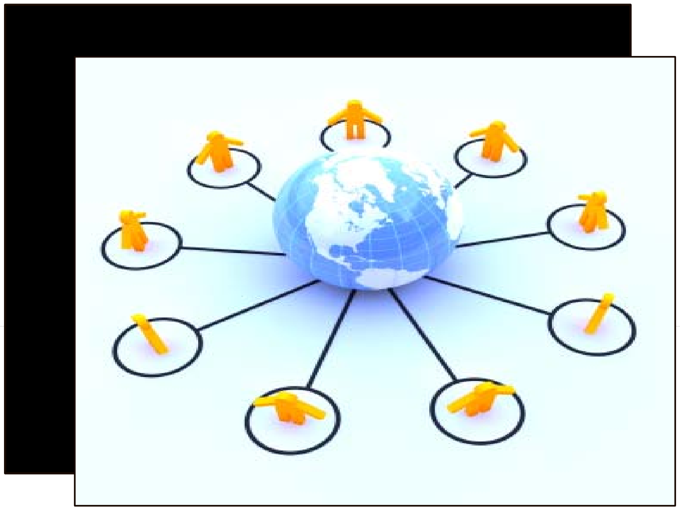
Post-webinar survey



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

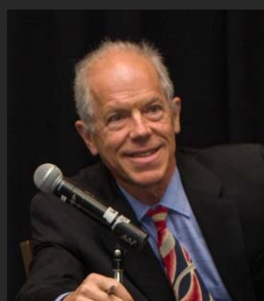

spirent™
Promise. Assured.
Your trusted PNT partner
visit spirent.com/pnt

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



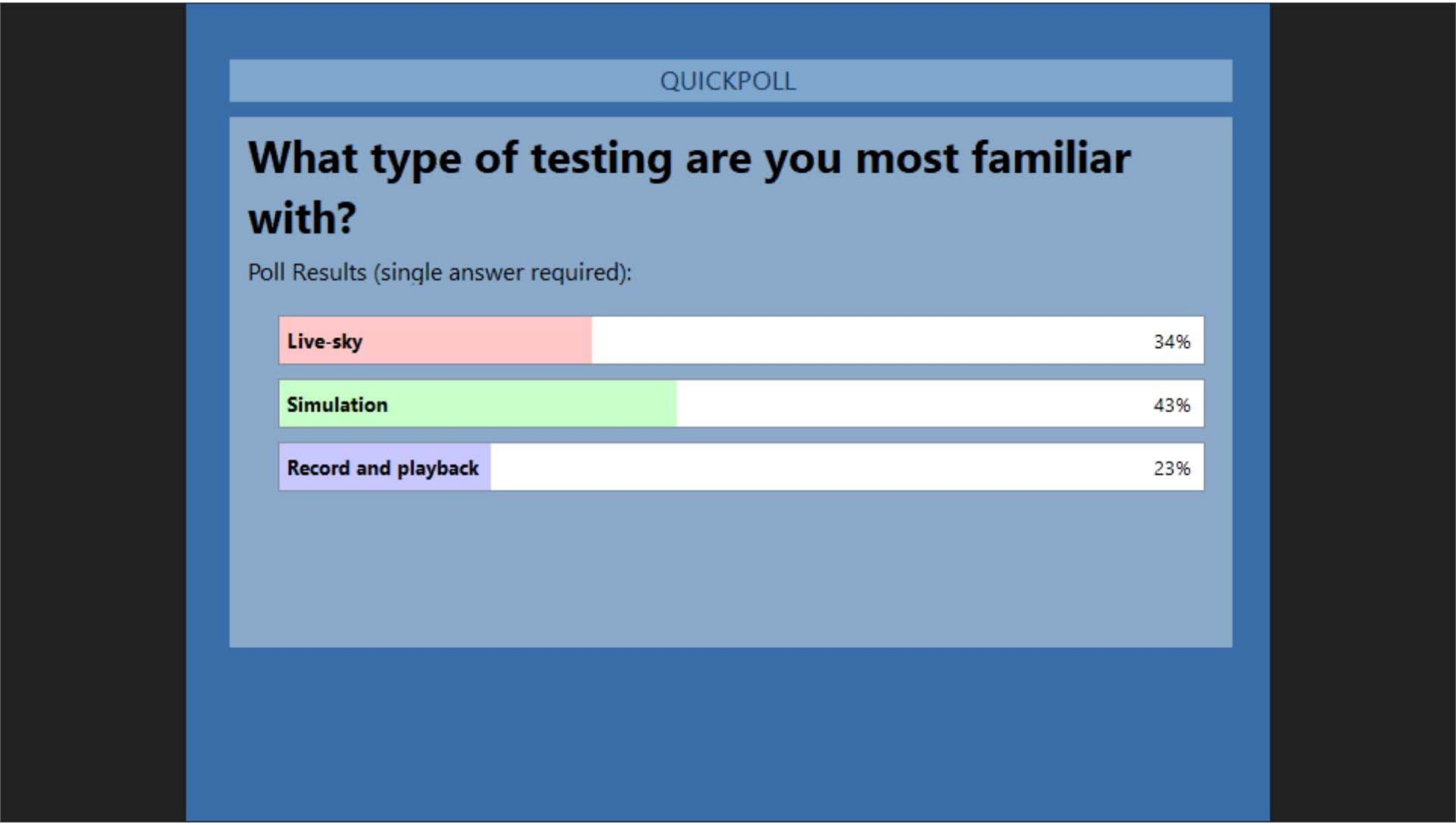
Alan Cameron
Editor in Chief
Inside GNSS
Inside Unmanned Systems

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

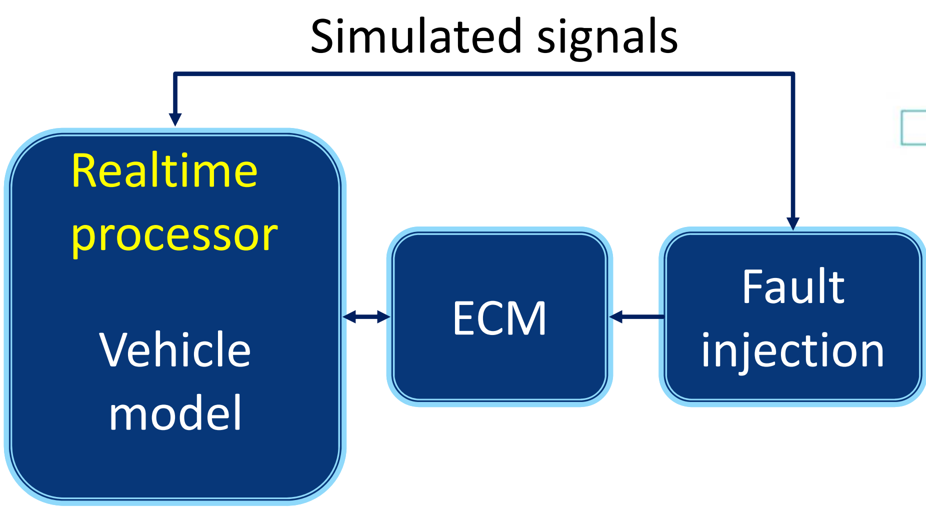
Co-Moderator: Lori Dearman, Executive Webinar Producer

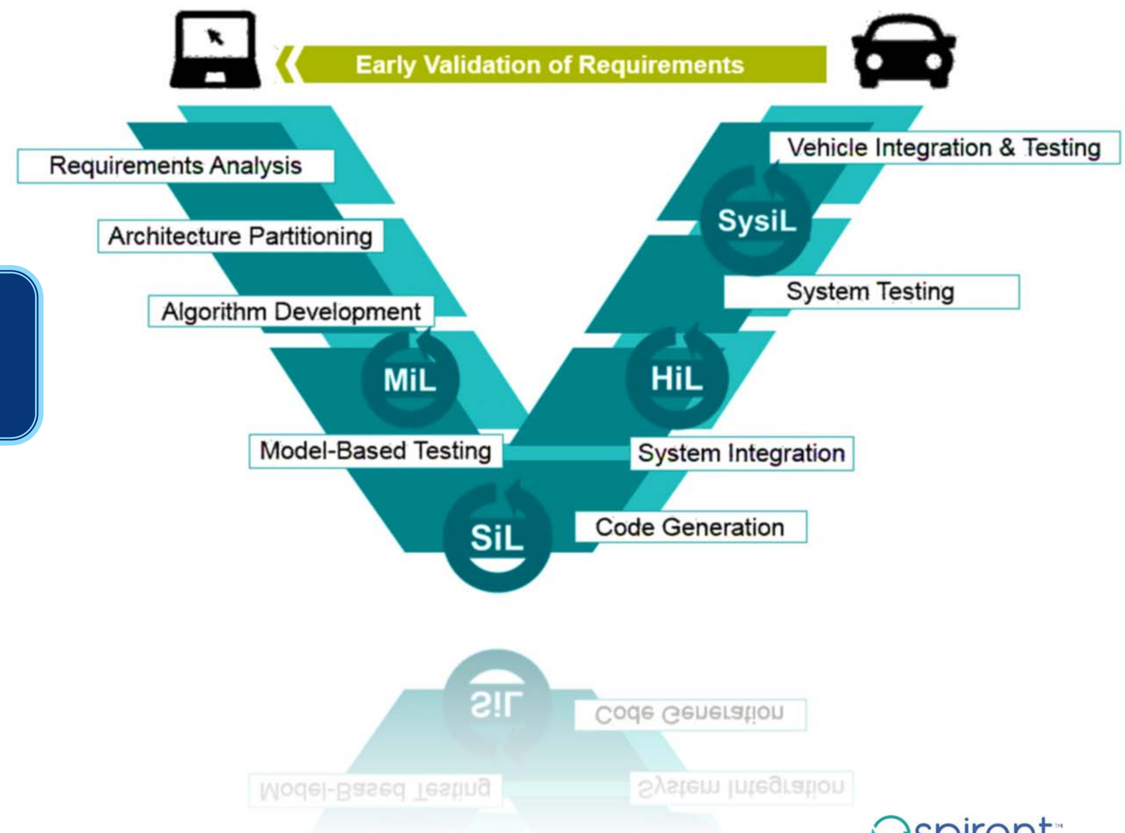

QUICKPOLL
What type of testing are you most familiar with?
Poll Results (single answer required):
Live-sky
34%
Simulation
43%
Record and playback
23%

Validating performance of Safety critical autonomous vehicle PNT systems

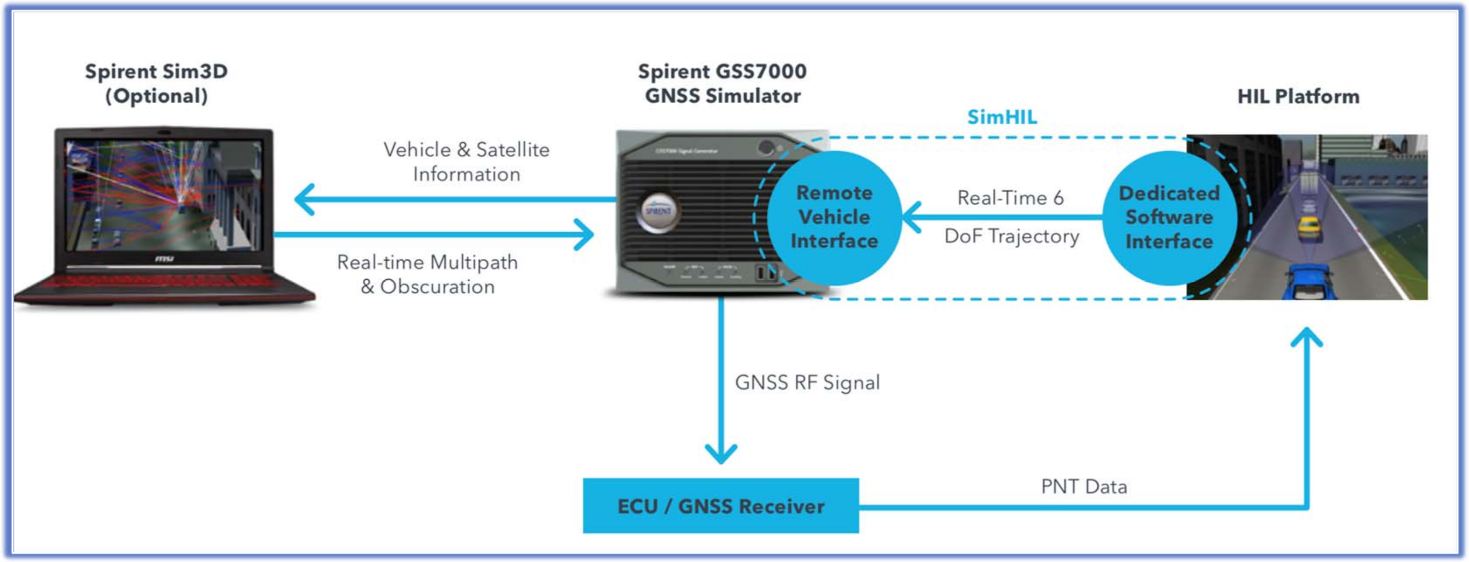
Ajay Vemuru
Product Manager - PNT
Spirent Communications

Hardware in the Loop (HIL) PNT Simulation





Spirent HIL setup
Realistic dynamics/trajectory



dSPACE IPG AUTOMOTIVE AVSIMULATION NATIONAL INSTRUMENTS CarSim Mechanical Simulation

Who needs HIL

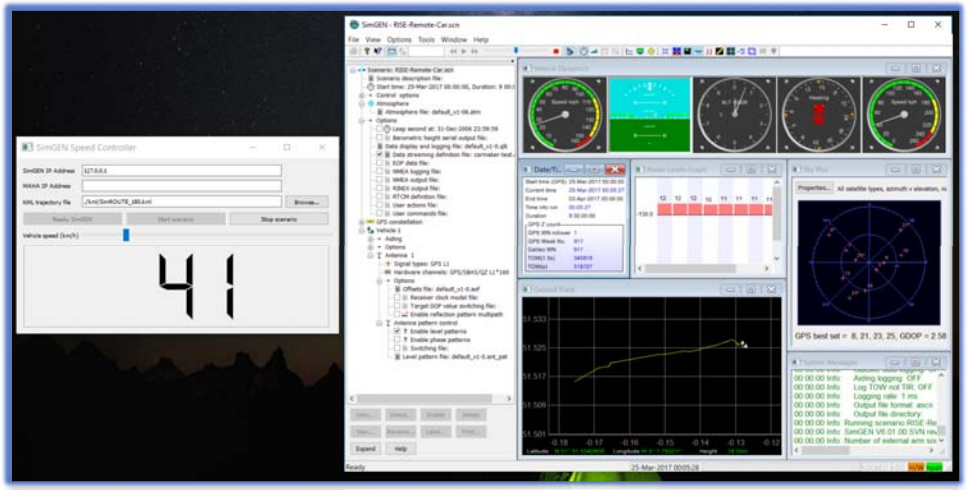
Automotive OEMs and Tier 1 suppliers
who want to test their PNT systems with driving simulators in a HIL environment

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

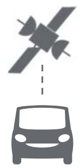
- In real time Spirent's SimGEN can follow a given route, for instance from Google Maps, at a given real-time dynamic speed from a rolling road or any other source of motion.



Validating performance of safety critical autonomous vehicles PNT systems

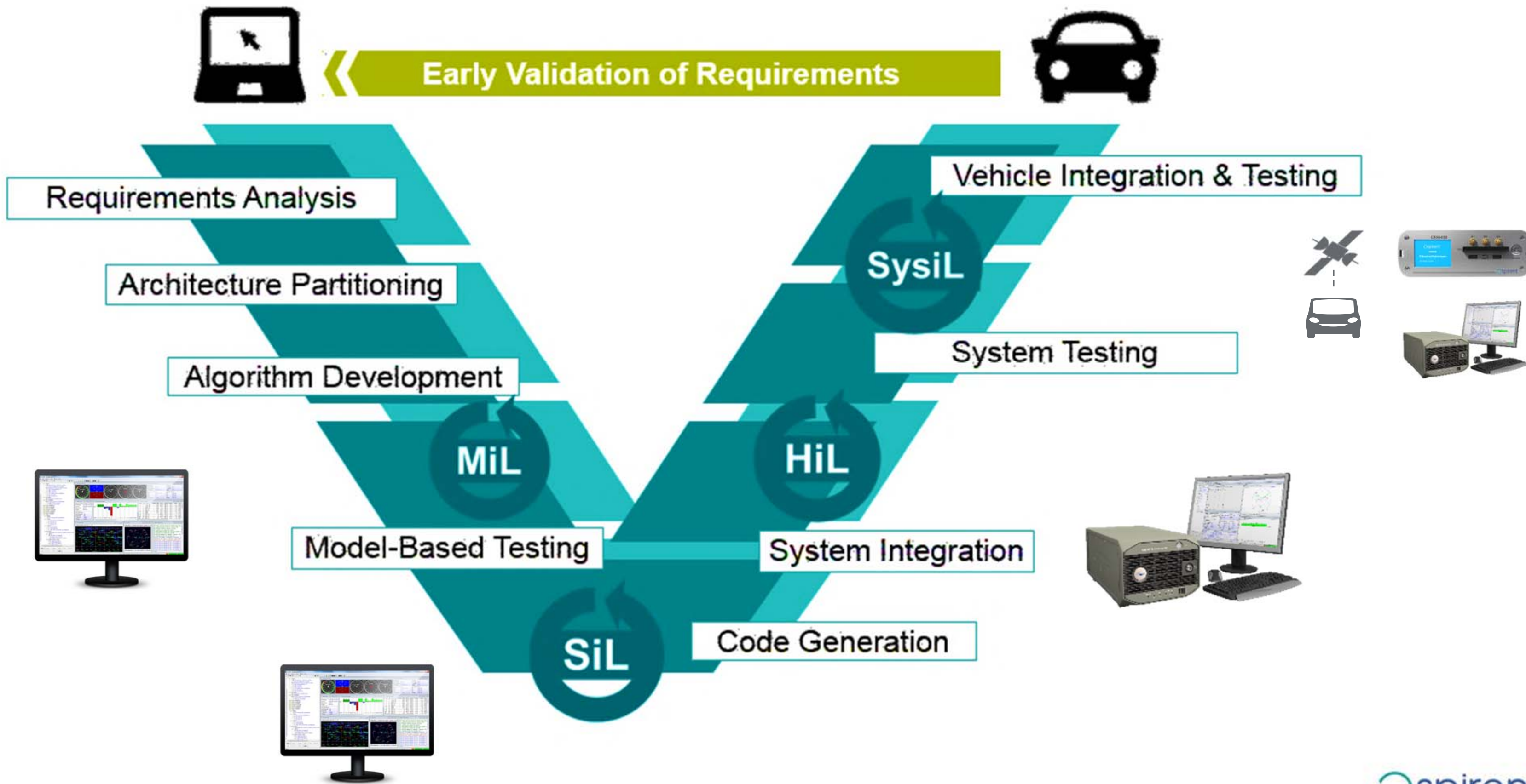
Ali Soliman
Business Development Manager, GNSS, PNT Technologies

GNSS Test Methodologies

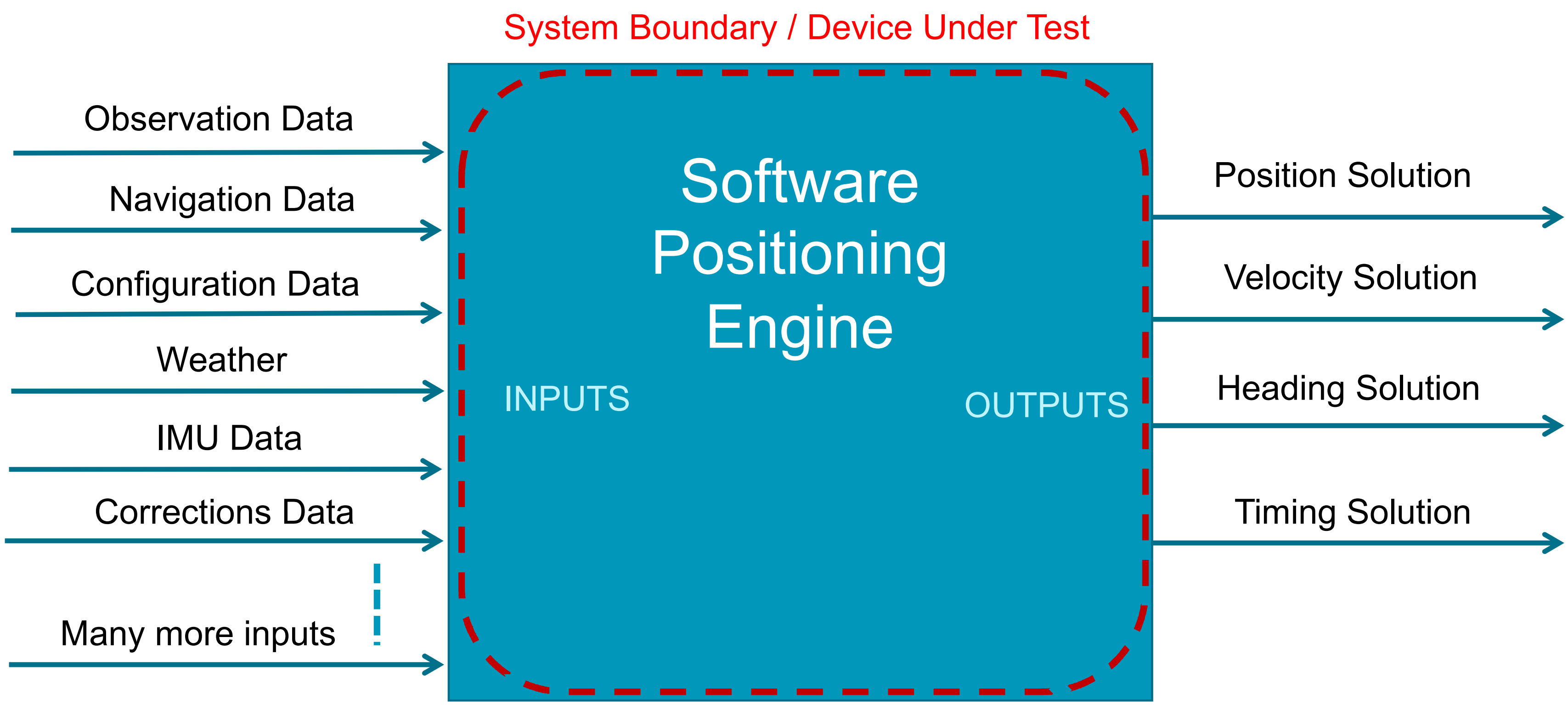
Method / attribute	 Live-sky	 Simulation	 Record & playback system
Repeatable	✗	✓	✓
Controllable	✗	✓	Partial
Reference truth	✗	✓	✗
Realistic	✓	Representative*	✓

*and getting better and better!

AV Development Stages



Boundary Diagram concept



Level of Testing

BASIC

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

ADVANCED

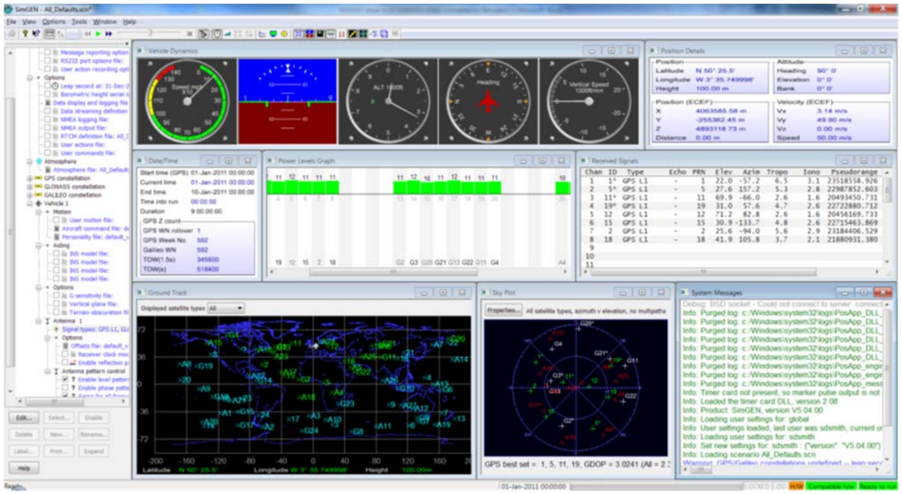
COMPLIANCE

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

- Multipath
- Jamming
- Spoofing
- Scintillation

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

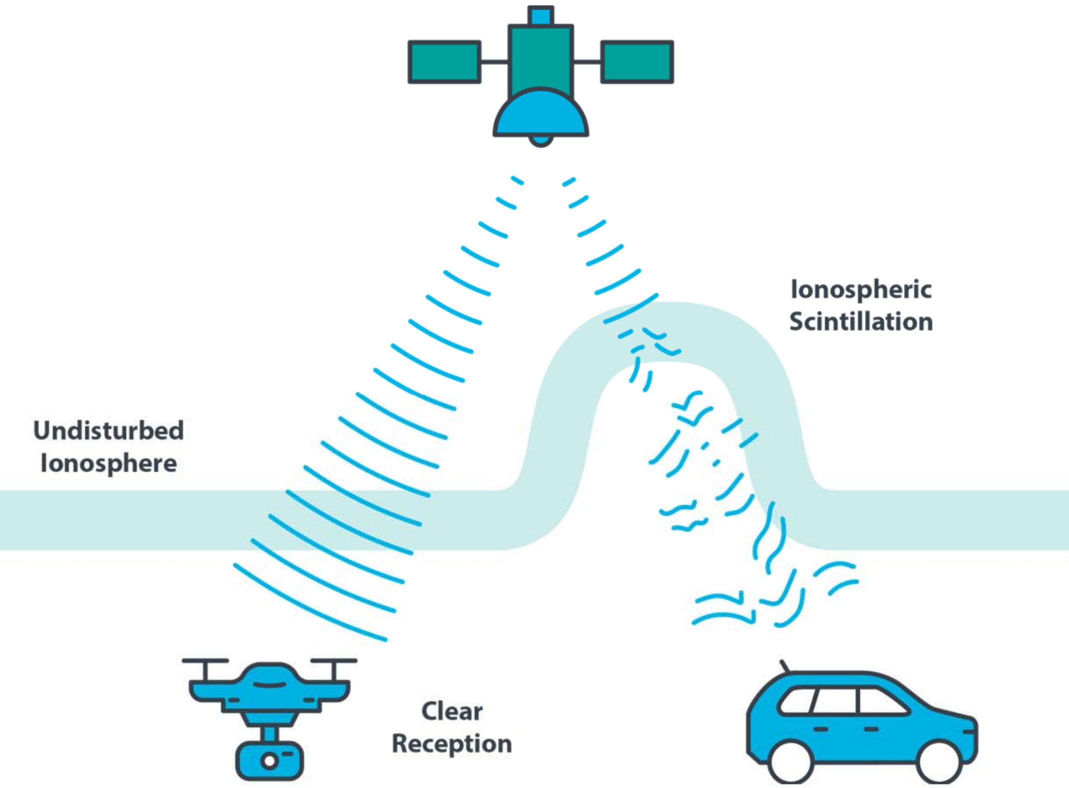
- Atmospheric modelling
  - Ionosphere
  - Troposphere
  - Scintillation

Key parameters

Realistic error modelling (atmospheric and scintillation)

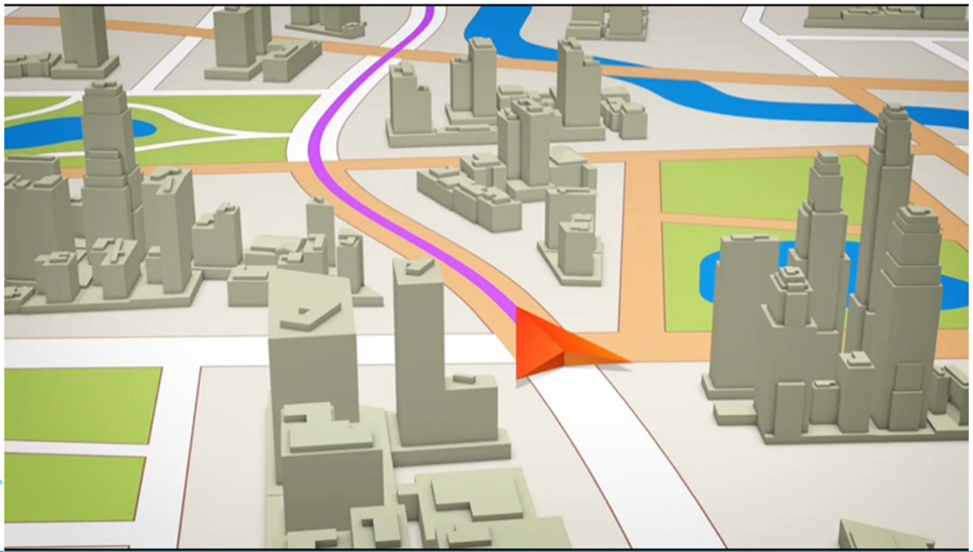
Remote interface for precise signal modification – support for user defined error models

- 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



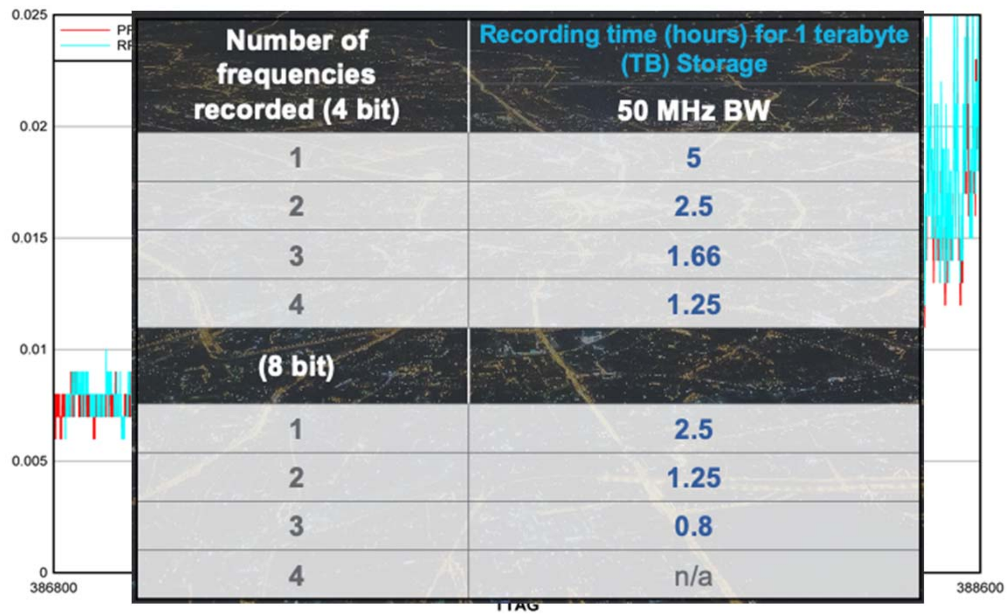
The RPS can be used to record GNSS signals along a drive route in urban areas. E.g. mounted in vehicle

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

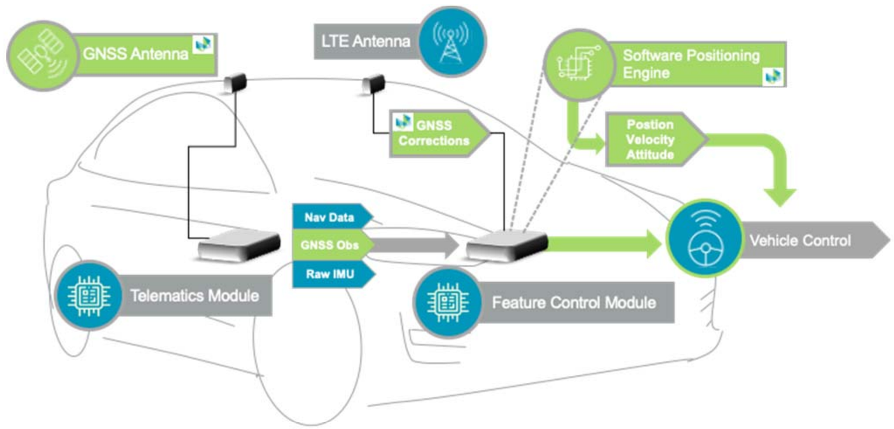
RPS Key Performance Indicator

- Quantization level
  - Signal fidelity
  - Dynamic range
- Clock stability and phase noise
- Large storage capacity
- GNSS + other signals



Number of frequencies recorded (4 bit)	Recording time (hours) for 1 terabyte (TB) Storage 50 MHz BW
1	5
2	2.5
3	1.66
4	1.25
(8 bit)	
1	2.5
2	1.25
3	0.8
4	n/a

RPS GNSS + Other Signals



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

Correction Data
PPP over NTRIP
RTK over serial bus

RECORD REPLAY

CAN/CAN-FD Data
Dead-reckoning

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

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

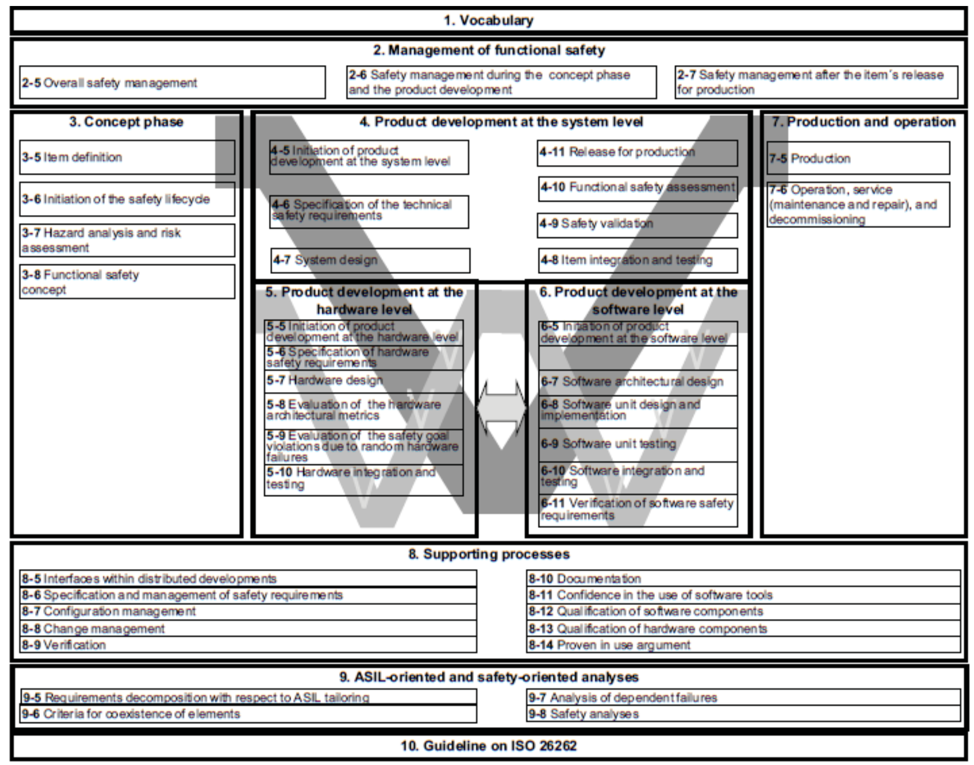
Specialization of IEC 61508 for series production passenger vehicles

- Up to 3,500 kg

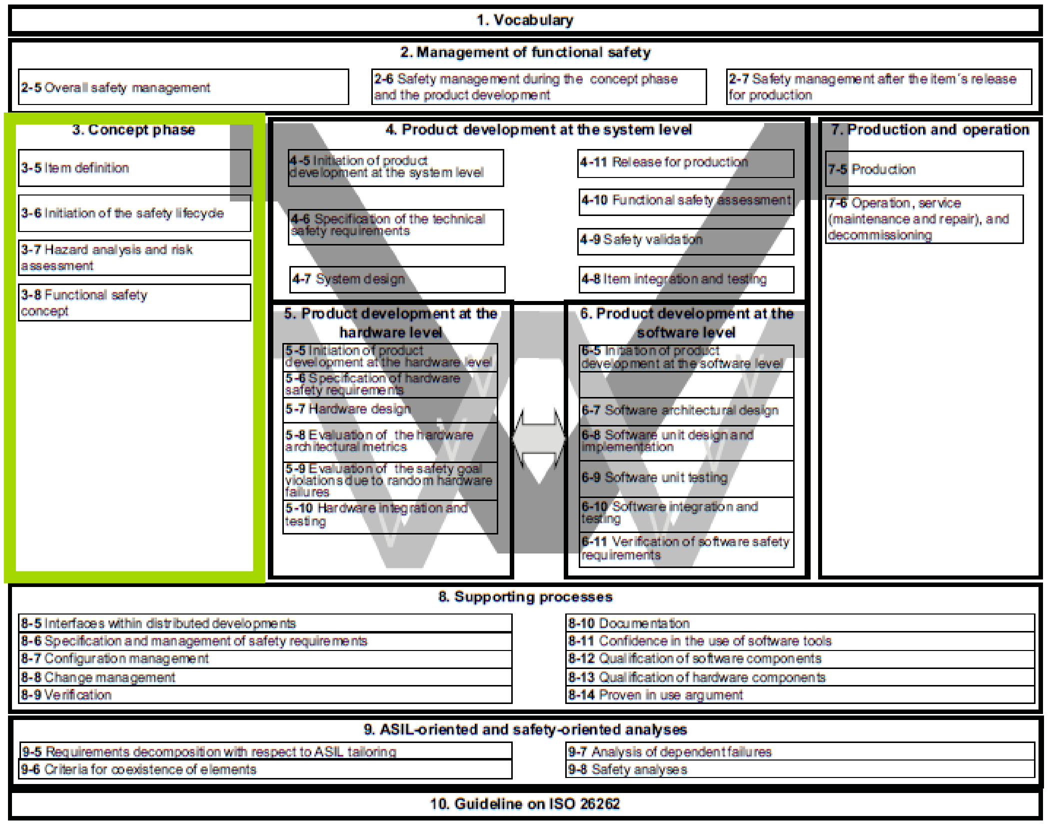
Addresses hazards caused by malfunction of the system

Defines processes and methods for:

- System, HW, and SW development
- Verification and validation
- Supporting processes



ISO 26262 – Concept Phase



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

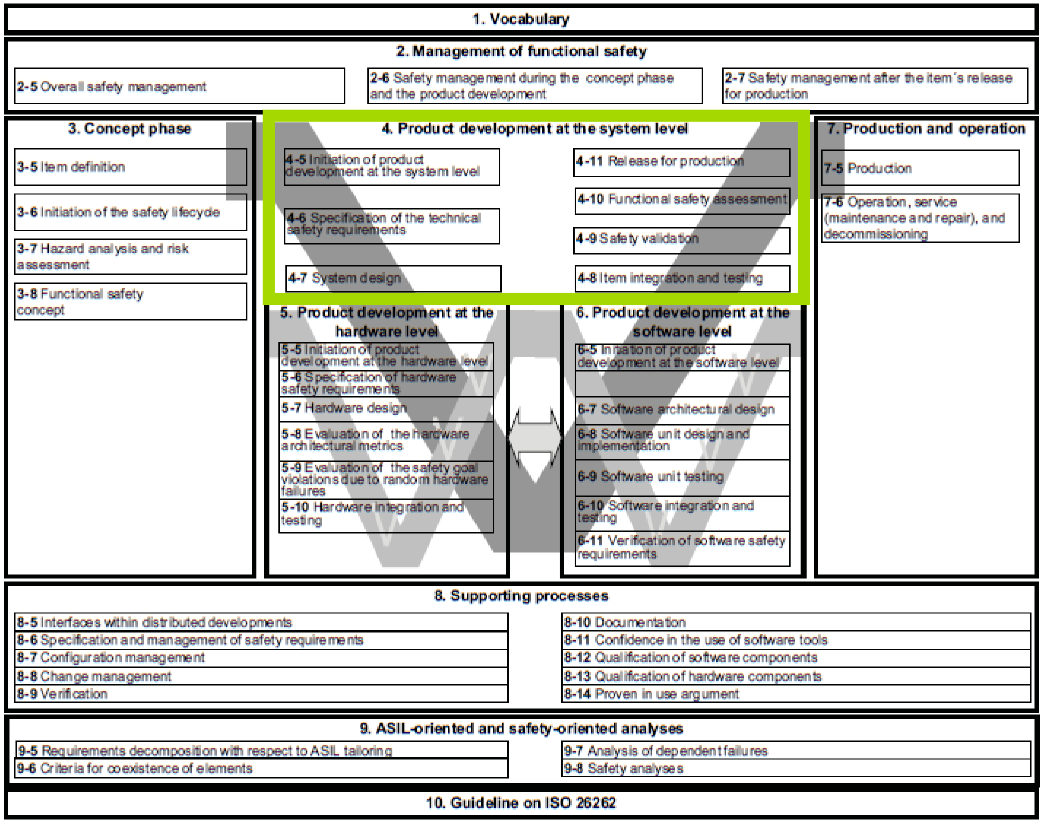
		C1	C2	C3
S1	E1	QM	QM	QM
	E2	QM	QM	QM
	E3	QM	QM	A
	E4	QM	A	B
S2	E1	QM	QM	QM
	E2	QM	QM	A
	E3	QM	A	B
	E4	A	B	C
S3	E1	QM	QM	A
	E2	QM	A	B
	E3	A	B	C
	E4	B	C	D

Uncontrollable (by driver)

Life threatening

High probability (of scenario)

ISO 26262 – System Design Phase

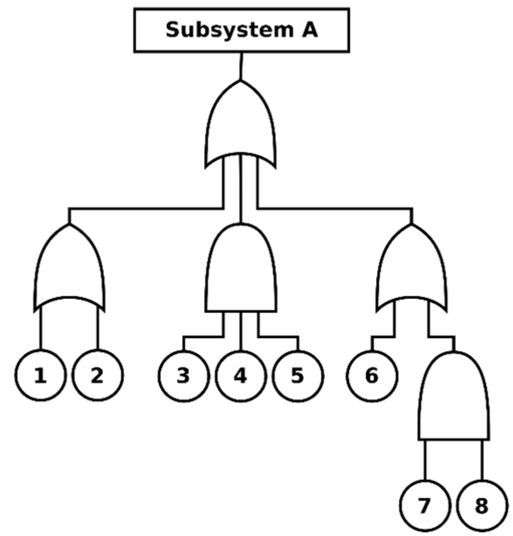


ISO 26262 – System Design Phase

Technical safety concept
- Allocate safety requirements to architecture

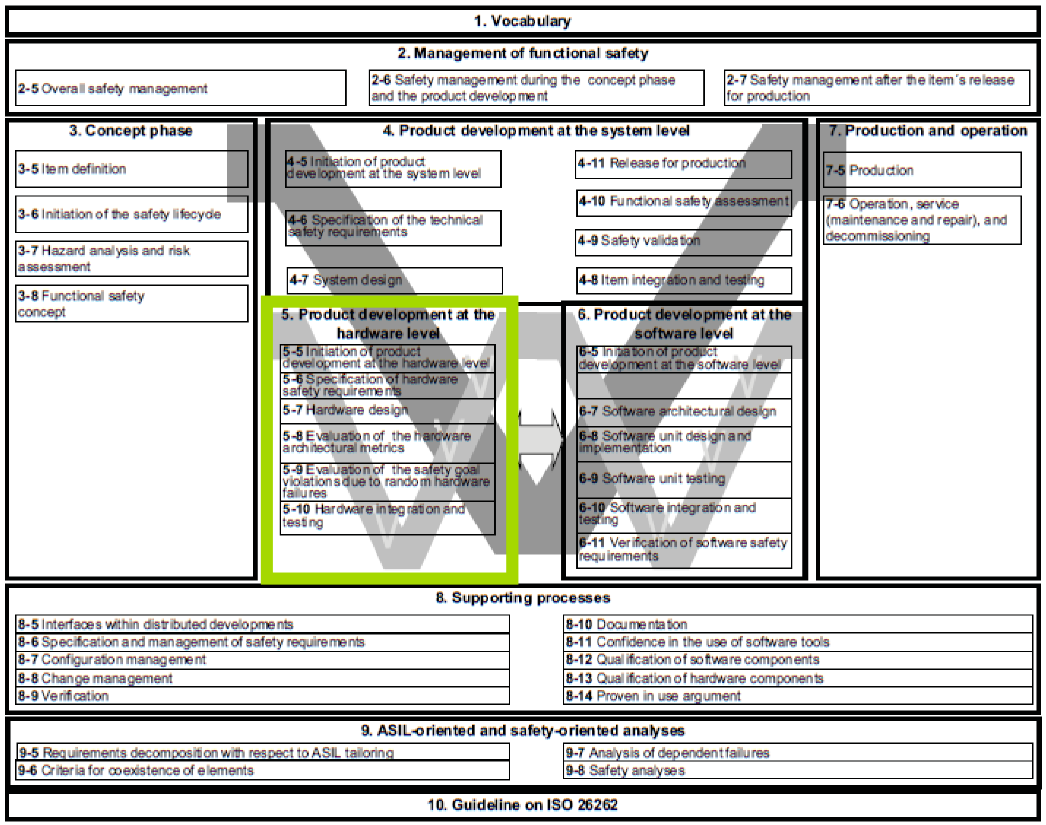
Safety requirements included in system design

Perform safety validation
- FMEA
- FTA
- DFA



O Proces FMEA				Deelnemers:	Afdeling:										(c) LL08
O Product FMEA				:	:										
F.M.E.A.Nummer:				:	:	Streef waarde = 36					Opsteller :				
Projectnummer :				:	:	Acceptabel <100					Opsteldatum :				
Gebruikte informatie bronnen:				:	:						Wijzigingsnummer : 0				
Failure Mode and Effect Analysis							VOOR ACTIE					NA ACTIE			
nr.	PRODUCT				K=kans op, O=ontdekkans, G=gevolg.		STATUS				Totaal=KxOxG	inschatting			
	PROCES	FUNCTIE	MOGELIJKE FOUT	OORZAAK	EFFECT	ONTDEKKINGSWIJZE	K	O	G	T	OPM/MAATREGEL	K	O	G	T
	Systeem / product														
1	onderdeel / proces stap	beschrijf functie	faal toestand	faal oorzaak	gevolg falen	hoe wordt falen ontdekt	5	5	5	125	bedenk oplossing	1	5	5	25

ISO 26262 – Hardware Design Phase



ISO 26262 – Hardware Design Phase

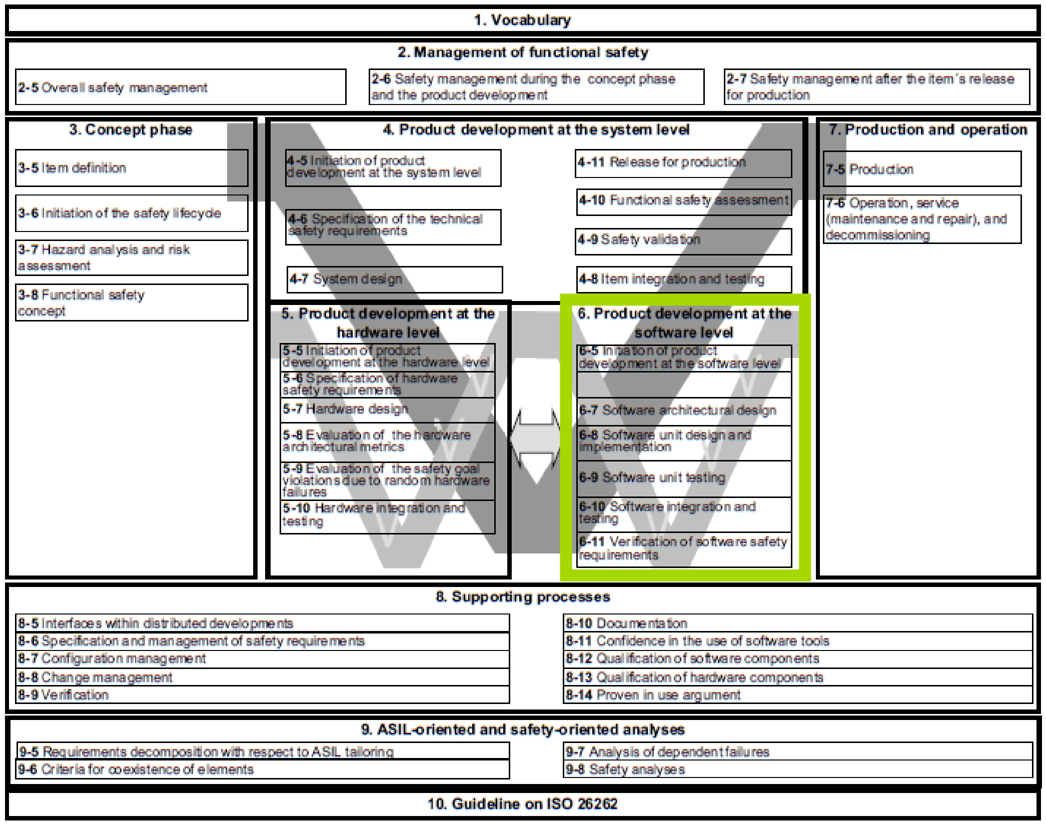
Define hardware safety requirements

Evaluate fault metrics - FMEDA

- Single Point Fault
- Dual Point Fault (ASIL C, D)
- Latent Fault
- FIT

ASIL	SPF	LF	FIT (1 FIT = 10^{-9}/h)
B	≥90%	≥60%	100
C	≥97%	≥80%	10
D	≥99%	≥90%	10

ISO 26262 – Software Design Phase



ISO 26262 – Software Design Phase

Define hardware safety requirements

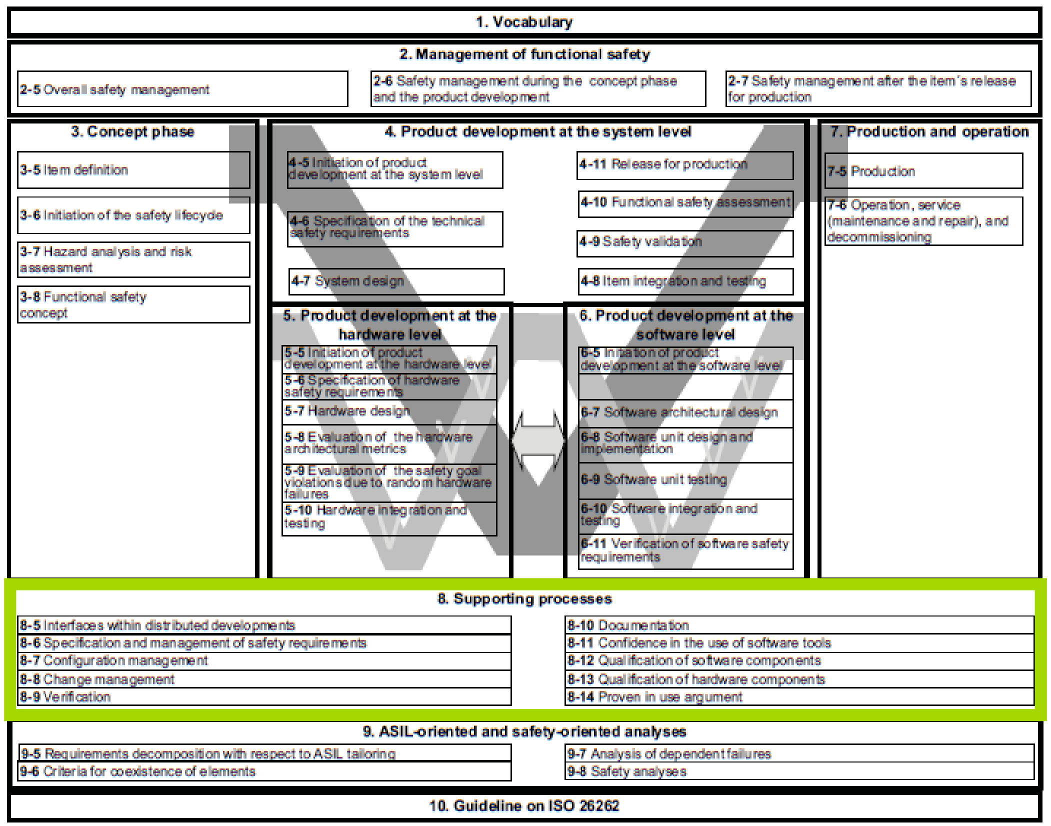
Apply appropriate design principles, e.g.
- Hierarchical structure
- Loose coupling
- Enforce low complexity

Use suitable coding standards
- E.g. MISRA C, MISRA C++

Unit and integration test
- Requirements coverage
- Structural coverage

ASIL	A	B	C	D
Statement Coverage	✓	✓		
Branch Coverage		✓	✓	✓
MC/DC				✓

ISO 26262 – Verification



ISO 26262 – Verification

Occurs throughout the process

Focus on robust testing methods

1d	Analysis of boundary values
1e	Error guessing based on knowledge or experience
1f	Analysis of functional dependencies

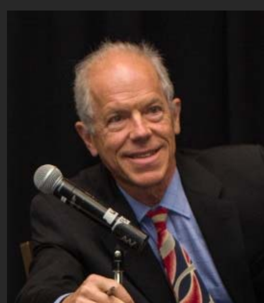
1a	Requirements-based test[a]
1b	Interface test
1c	Fault injection test[b]
1d	Resource usage test[c]

Requires confidence in tools

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

		Tool error detection		
		TD1	**TD2**	**TD3**
Tool impact	TI1	TCL1	TCL1	TCL1
	TI2	TCL1	TCL2	TCL3

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

QUICKPOLL

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

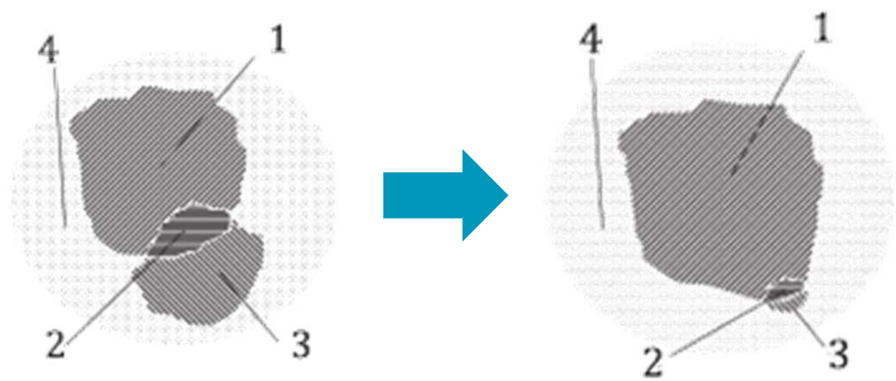
ISO 26262 focuses on hazards from failures in the E/E systems

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?



HEXAGON

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

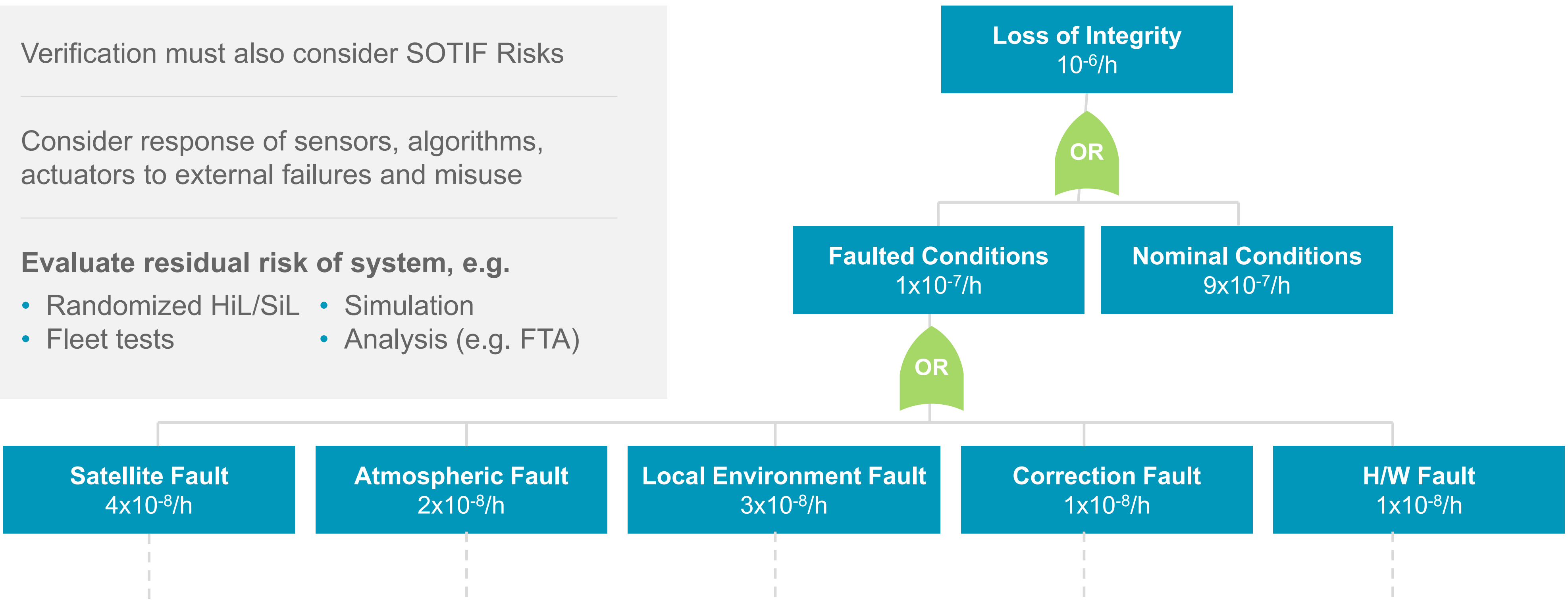
SOTIF – Verification and Validation

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
- Simulation
- Fleet tests
- Analysis (e.g. FTA)



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

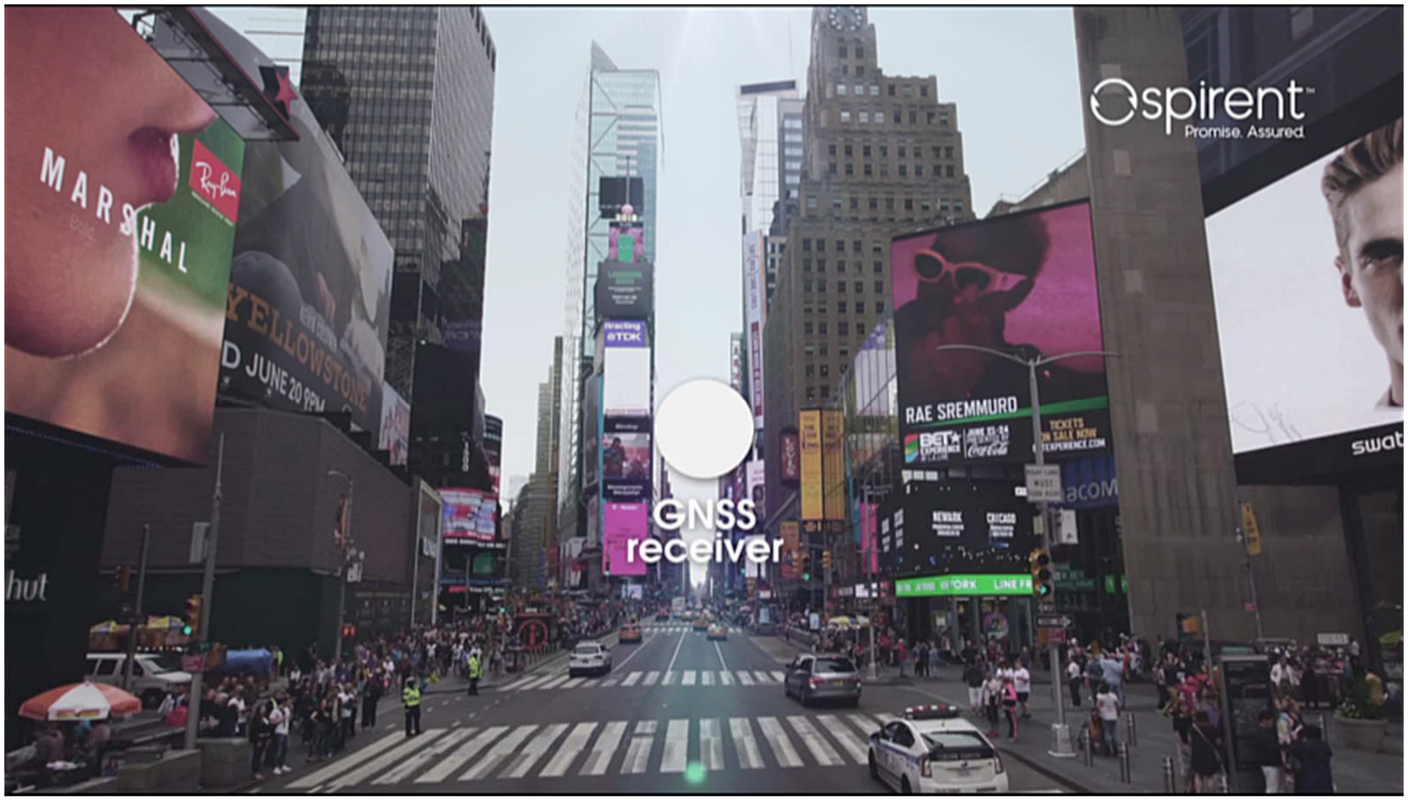
EN 16803-3
will define requirements and classifications for security performance

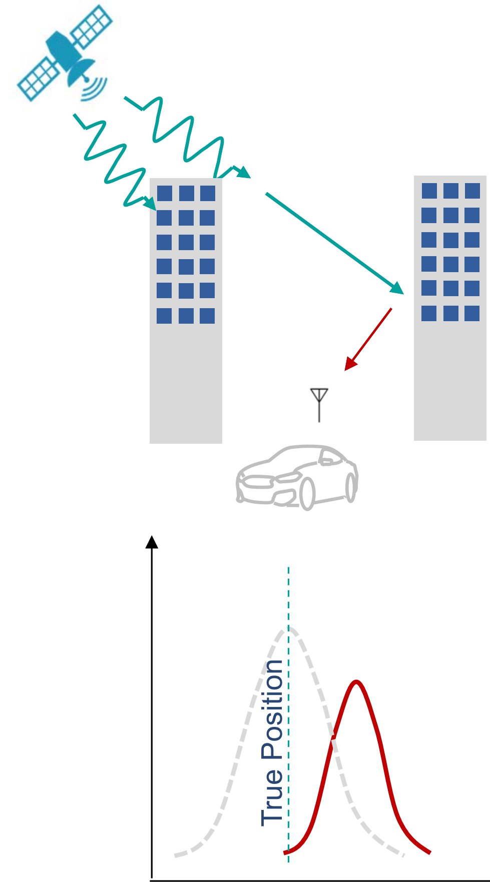
EN 16803-4
will define methods for verification of GBPT

Validating performance of safety critical autonomous vehicles PNT systems

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

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

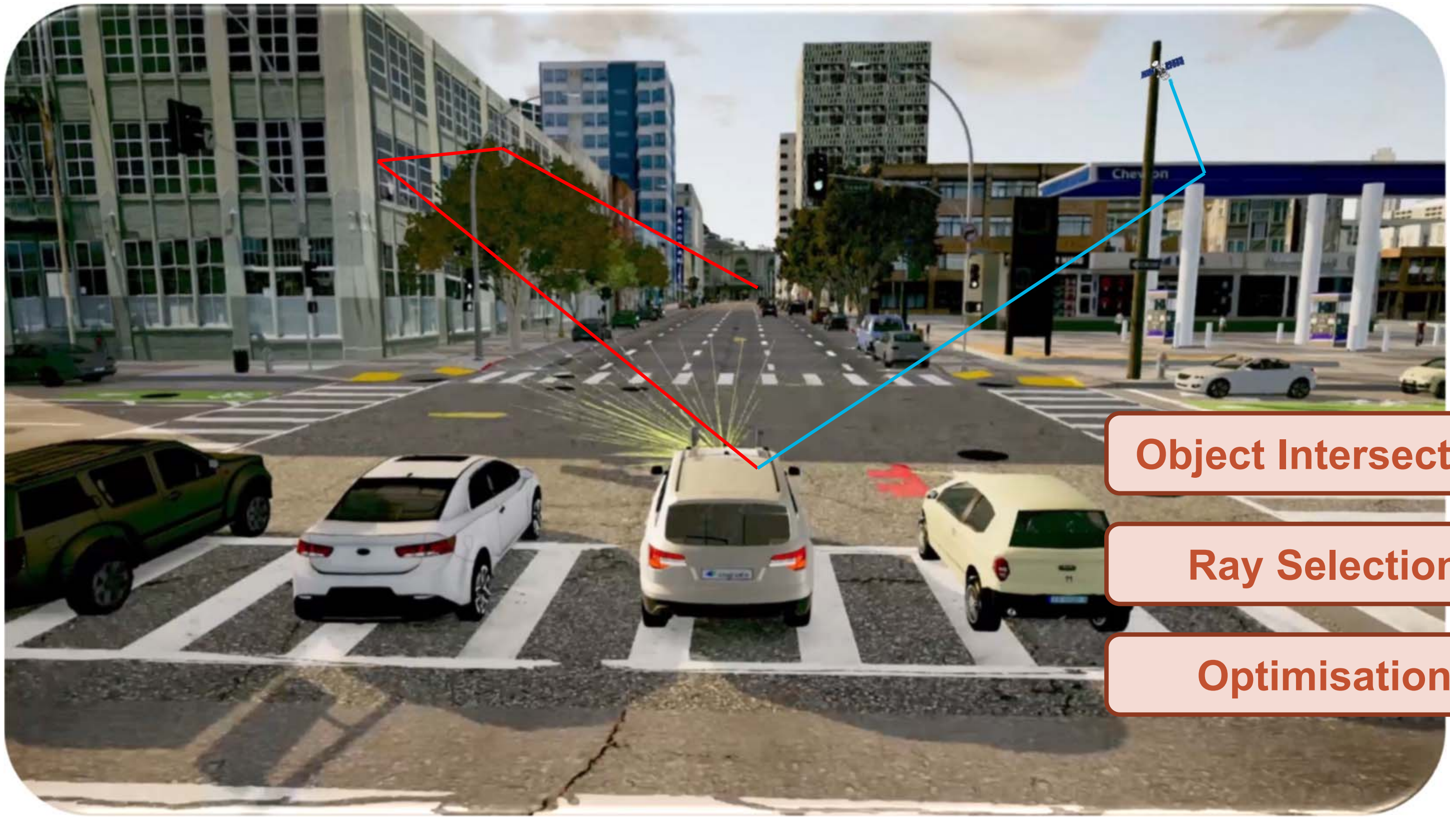
GNSS Prop. Model

Bringing the Real World to the Lab

Environment

Physics

Solver
(Ray-Tracing)



Object Intersection

Ray Selection

Optimisation

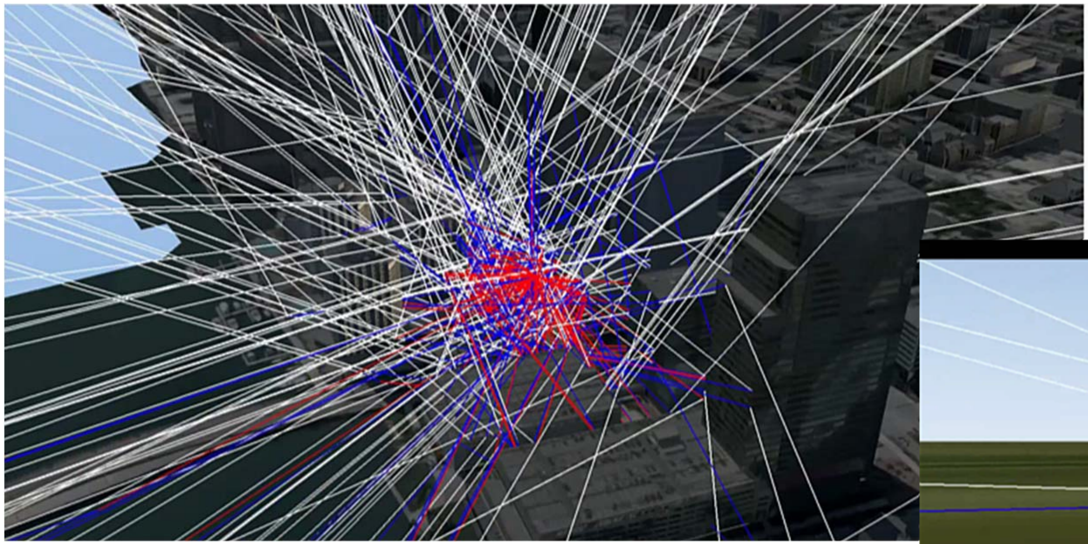
Bringing the Real World to the Lab

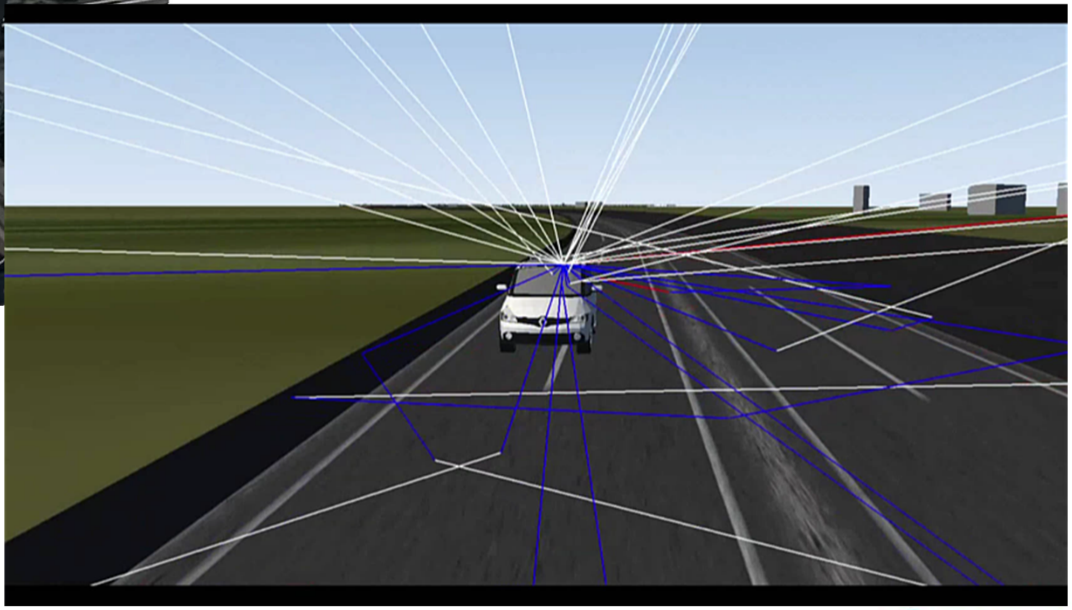
Environ

Physics

Solver
(Ray-Tracing)

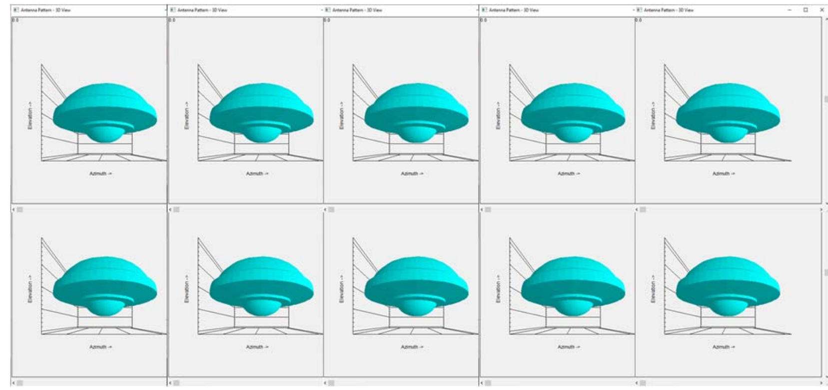
Sim3D

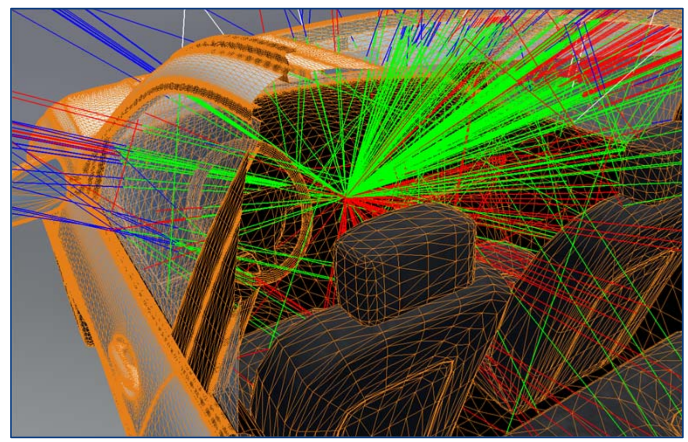




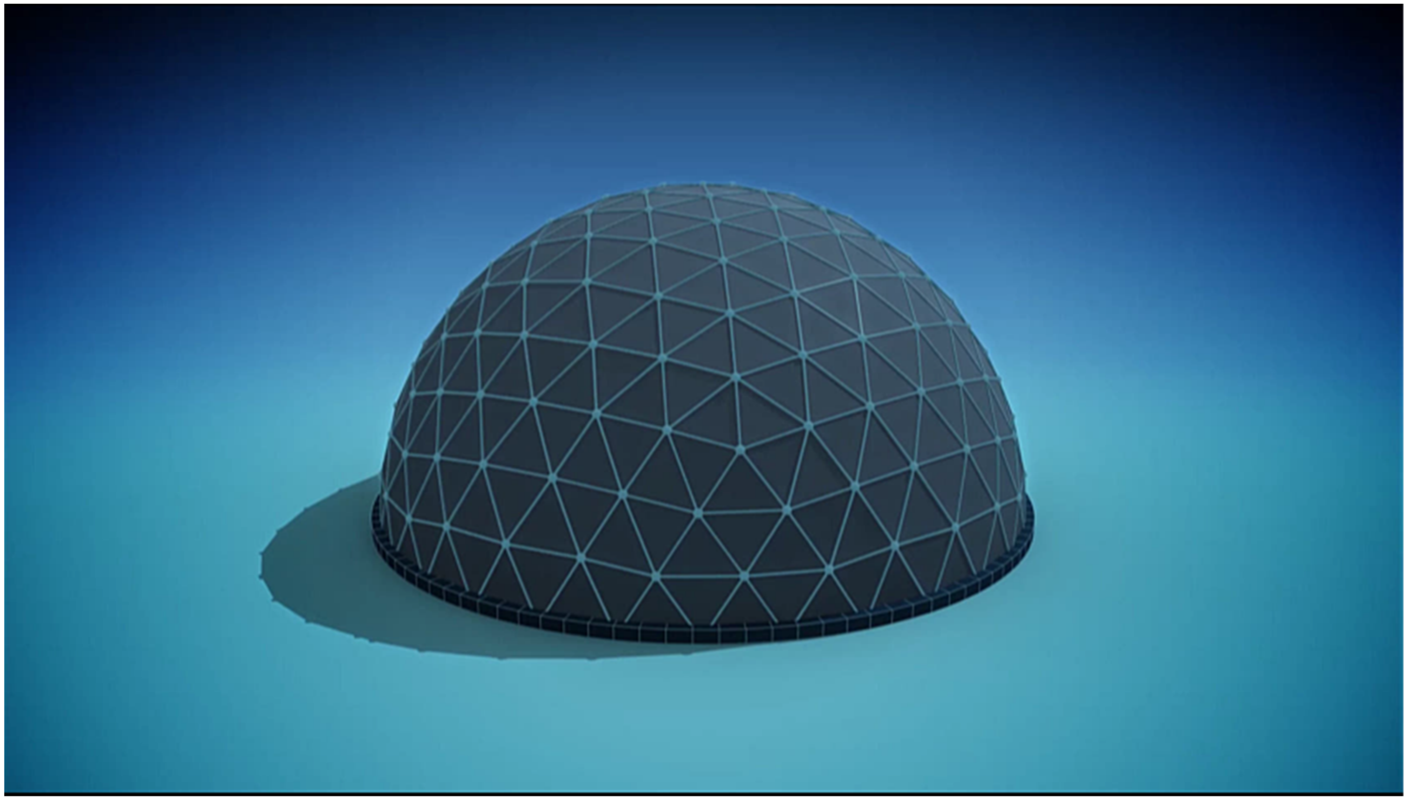
GNSS Antenna

- 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

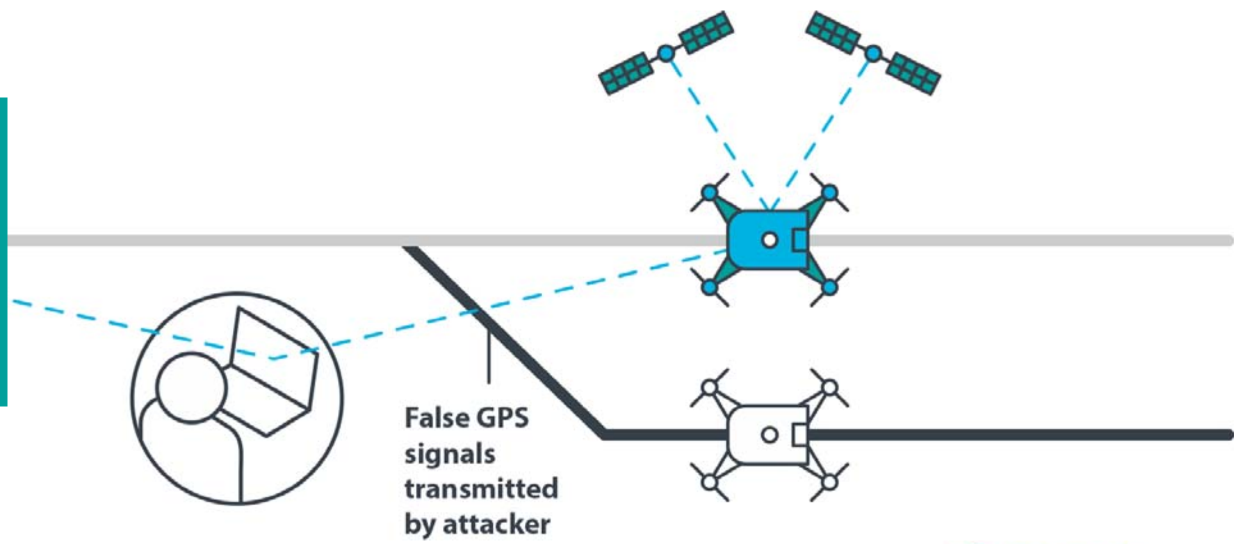
- False location and time readings can have severe impacts on automated and autonomous devices
- Anti-spoofing will play an ever-increasing role in safety-critical applications – compliance with regulations and standards will soon be mandatory across multiple industries

Key parameters

Signal fidelity

Dedicated tools for testing anti-spoofing techniques

Expertise in anti-spoofing test scenario design

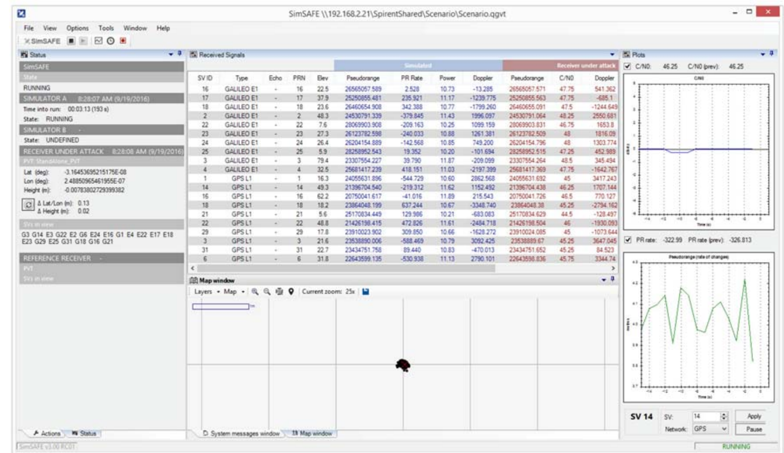


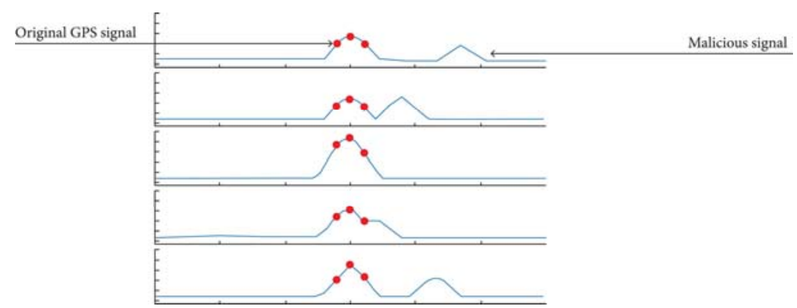
Spirent Spoofing Capabilities

- 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

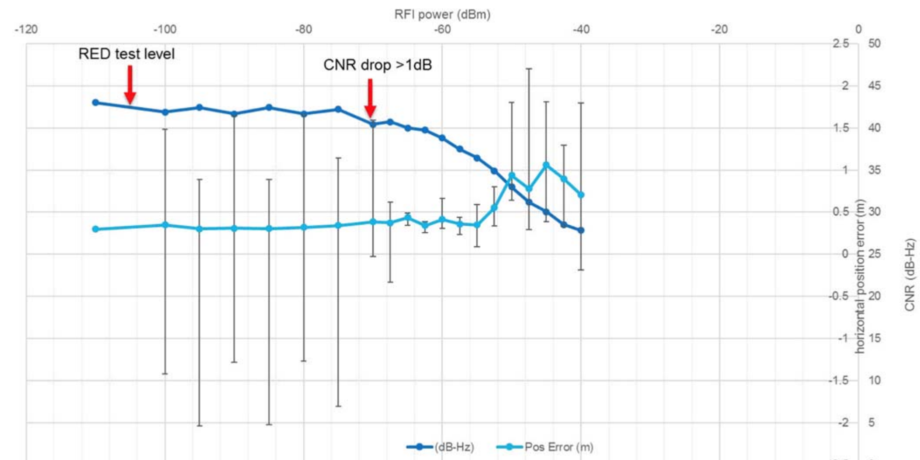
Key parameters

Multiple interference sources – static or dynamic with precise phase alignment

Realistic propagation modelling

Figure 1: Reports of GPS interference made by pilots to the NASA Aviation Safety Reporting System

Source: https://asrs.arc.nasa.gov/index.html

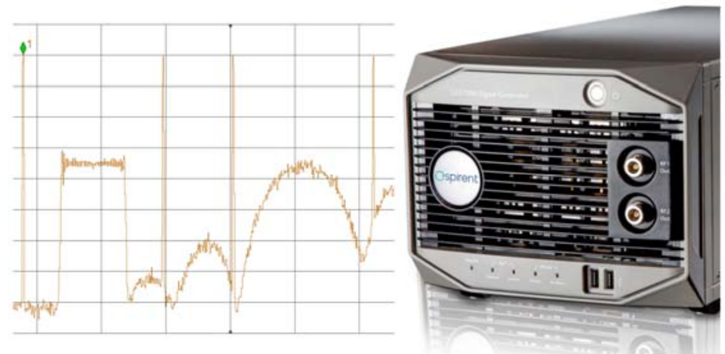


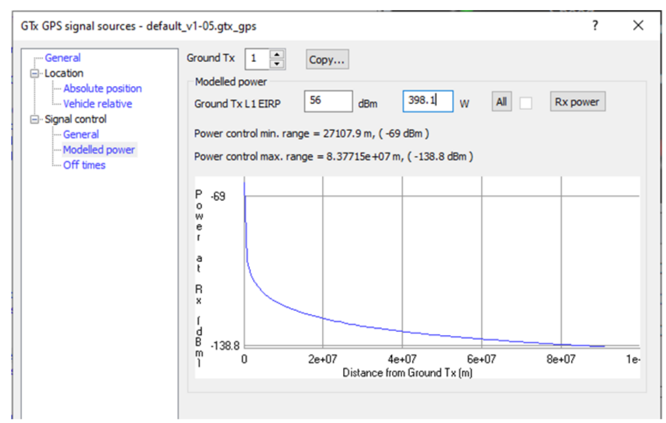
RFI Power and Horizontal position error at 1554MHz with measurement range (HPE) added - Receiver A

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





QUICKPOLL

What are you most interested in testing for?

Poll Results (single answer required):

Basic system performance: sensitivity, accuracy, TTFF, etc.	20%
Performance under spoofing and/or jamming conditions	24%
Standards compliance: ISO 26262, SOTIF, etc.	11%
All of the above are equally important	45%

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