SAFETY-CRITICAL POSITIONING
FOR AUTOMOTIVE APPLICATIONS: LESSONS FROM CIVIL AVIATION

Thursday, Nov 3, 2016
WELCOME TO
Safety-Critical Positioning for Automotive Applications:
Lessons from Civil Aviation

Co-Moderator: Lori Dearman, Sr. Webinar Producer

Chaminda Basnayake, Ph.D.
Principal Engineer
Renesas Electronics America

Mathieu Joerger
Assistant Professor
The University of Arizona

Jonathan Auld
Director
Safety Critical Systems
NovAtel
Who’s In the Audience?
A diverse audience of over 600 professionals registered from 42 countries, and provinces representing the following industries:

17% GNSS Equipment Manufacturer
14% Automaker/Automotive Tech Supplier
12% System Integrator
11% Product/Application Designer
7% Regulatory/Public Agency
7% Civil Aviation
32% Other
Welcome from Inside GNSS

Richard Fischer
Publisher
Inside GNSS and Inside Unmanned Systems
Safety-Critical Positioning for Automotive Applications: Lessons from Civil Aviation

Mark Petovello
Professor
Department of Geomatics Engineering
University of Calgary
Poll #1

When do you think fully autonomous cars will be mass produced? (Please select one)

- Before 2020
- 2020-2025
- After 2025
Evolution of Automotive Safety Technology
Path to Connected & Automated Vehicles

Chaminda Basnayake, Ph.D.
Principal Engineer
Renesas Electronics America
• Traditional safety features
  • Anti-Lock Braking Systems (ABS)
  • Airbags
  • Seatbelt pretensioning
  • Traction Control & Electronic Stability Control Systems

• Advance safety features (Function Specific Automation – Level 1)*
  • Adaptive Cruise Control (ACC)
  • Forward Collision Warning (FCW)
  • Lane keeping & Lane Departure Warning (LDW)
  • Brake Assist & Automatic Emergency Braking
  • Pedestrian detection
  • Backup Assist & Rear Cross Traffic Alert

• Next generation safety features (Combined Functions – Level 2)*
  • Tesla Auto Pilot
  • GM Super Cruise

• Autonomous driving (Limited to Full Self Driving - Level 3 & 4)*
  • Google, Uber,....

*Levels of vehicle automation definition by National Highway Traffic Safety Administration (NHTSA)
www.nhtsa.gov/staticfiles.rulemaking/pdf/Automated_Vehicles_Policy.pdf
• Connectivity based convenience & safety applications are becoming standard

• Current system are location-aware connectivity solutions
  • GNSS - Position & time
  • Cellular – Connectivity & time
  • Aided by other vehicle sensors
    • Wheel speed, gyro & accelerometer, steer/brake/transmission sensors

• Offer convenience & safety applications
  • Navigation
  • Emergency response
  • Diagnostic / prognostic /maintenance functions
  • Concierge services

• Customer expectations
  • Connectivity
  • Road level location awareness (~5 m)
  • Some outages are expected
    • Cellular coverage
    • GNSS & position availability / accuracy
Automotive System Architecture

Connectivity Device
- Gateway for all outside connectivity
- Standard cellular modem (i.e. 4G / 3G)
- May have direct connections to Telematics ECU and/or HMI (Human – Machine Interface)
- User device may be used as the Connectivity Device

Vehicle Antenna
- Typically contain multiple services: Cellular, GNSS, XM, other
- Typically a single enclosure antenna
- Styling considerations are important

Telematics System / Device / ECU
- Controls all telematics functions
- Retrieves vehicle data from CAN
- May be integrated with the Connectivity device
- May interface / control HMI / User Interface / Cluster

Sensors & Actuators
- Examples: Wheel Speed, Gyroscopes, Accelerometers

Control Area Network - CAN
- Communication medium between different ECUs, sensors and other modules
- Access may be controlled
- Messaging protocol may be unique to make, model & year

ECUs – Electronic Control Units
- May be directly or indirectly connected to CAN

Vehicle Antenna
- Typically contain multiple services: Cellular, GNSS, XM, other
- Typically a single enclosure antenna
- Styling considerations are important

Connectivity Device
- Gateway for all outside connectivity
- Standard cellular modem (i.e. 4G / 3G)
- May have direct connections to Telematics ECU and/or HMI (Human – Machine Interface)
- User device may be used as the Connectivity Device

Vehicle Antenna
- Typically contain multiple services: Cellular, GNSS, XM, other
- Typically a single enclosure antenna
- Styling considerations are important

Telematics System / Device / ECU
- Controls all telematics functions
- Retrieves vehicle data from CAN
- May be integrated with the Connectivity device
- May interface / control HMI / User Interface / Cluster

Sensors & Actuators
- Examples: Wheel Speed, Gyroscopes, Accelerometers

Control Area Network - CAN
- Communication medium between different ECUs, sensors and other modules
- Access may be controlled
- Messaging protocol may be unique to make, model & year

ECUs – Electronic Control Units
- May be directly or indirectly connected to CAN
• New technologies are likely be added to existing systems
  • Industry may adapt V2X / Connected Vehicle technology as an add-on
  • In most cases integration may not involve a complete system redesign

• Some systems may need to do redesigned
  • Antenna design and placement
  • Dedicated sensors may be needed for some functions
    • Positioning & navigation: Existing sensors are integrated (typically loosely coupled) in current systems
  • No requirements around reliability, integrity and jamming

• Challenges unique to automotive
  • Design driven by styling, cost and complexity
  • Automotive design cycle is typically 3-4 years & design life is around 8 years*
  • Significant work is needed to widely utilize Over-the-Air (OTA) update capability

* www.consumerreports.org
Industry Expectations of GNSS

- Legacy
  - Road level positioning: Which road am I in?
  - May use existing sensors for aiding

- Today
  - Lane level positioning: Which lane am I in?
    - Lane guidance: GNSS with corrections & maps
    - V2X / Connected Vehicles
  - May use existing & new dedicated sensors for aiding
    - Camera, radar

- Beyond
  - Better than lane level positioning
    - Automation
    - Multiple sensors will have to be integrated

- GNSS still remains the only viable absolute positioning & timing source

- Industry expectation on GNSS needs to change
  - Accuracy: few meters > centimeters
  - Availability: most of the time > all the time
  - Reliability: System failure detection is critical
Why V2X / Connected Vehicles?

• Traditional sensors have their limitations
  • Occlusion of view
  • Sensor limitations: Rain, fog, lighting level/direction
  • Predicting driver and pedestrian intent / signal controls

• V2X / Connected Vehicles advantage
  • Enables real-time information sharing
  • Address most traditional sensor limitations

• Over a decade of R&D
  • FCC designated 5.9 GHz band in North America in 1999
  • Based on 802.11p Dedicated Short Range Communications (DSRC)
  • Established Over-the-Air (OTA) messaging protocols
  • USDOT funded over 10 years of R&D
    • [http://www.its.dot.gov/research.htm](http://www.its.dot.gov/research.htm)
  • Anticipated USDOT mandate starting around 2022
  • May be supplemented by cellular technology *

* End-to-end communication latency & throughput may need 5G technology to support all V2X use cases
Basics of V2X

• All road users exchange information
  • Vehicles broadcast Basic Safety Messages (BSM)
  • Pedestrian devices broadcast Pedestrian Safety Messages (PSM)
  • Traffic control devices also broadcast information
    • SPAT – Signal Phase & Timing
    • MAP – Intersection map
    • GPS – GPS / GNSS corrections

• Concept of Operation
  • Vehicles broadcast absolute position & time
  • Classify vehicles as:
    • Traveling in same direction, opposite or other
    • Same lane or adjacent lane
  • Identify threats & generate warnings

• Typical accuracy requirements
  • Road level: better than 5 m absolute
  • Lane level: better than 1.5 m absolute

  • Minimum performance requirements for V2X vehicle / onboard equipment (SAE 2945/1), On-Board System Requirements for V2V Safety Communications, http://standards.sae.org/j2945/1_201603/
  • Over-the-Air (OTA) message specification for V2X (SAE J2735), Dedicated Short Range Communications (DSRC) Message Set Dictionary, http://standards.sae.org/j2735_201603/
V2X Over-the-Air (OTA) Messaging

- Defined in SAE J2735 DSRC Message Set
  - SAE – Society of Automotive Engineers
- Sent every 100 msec / 10 Hz
- Vehicle Position information
  - Time mark (GPS used as source)
  - Global coordinates
  - Accuracy estimate
- Motion / Heading / Acceleration
  - Others can predict future trajectory
- Control status
  - Others are made aware of intentions (i.e., lane change)
- Optional data can be added

Basic Safety Message (@ 10 Hz)

- Time
- Speed
- Brake
- Temp ID
- Latitude
- Heading
- Steering
- Message Type
- Longitude
- Acceleration
- Throttle
- Vehicle Type
- Elevation
- Exterior Lights
- Vehicle Size

Optional Messages (Variable Rate)
- Event Notifications
- Vehicle Trail
- Vehicle Path Prediction
- GNSS Measurement Data (RTCM*)

Proprietary Optional Messages (Variable Rate)

* Radio Technical Commission for Maritime Services (RTCM)
A Challenge for GNSS Industry....

- USDOT funded Connected Vehicle Pilots (CVP) starting in 2017
  - Includes sites in New York, Wyoming & Florida

- First exposure of V2X to deep urban canyons
  - Serious GNSS availability & multipath issues
  - Augmentations can help but performance, affordability, and complexity challenges remain
  - GNSS integrity, reliability and jamming/spoofing not in scope yet

Source:
Data courtesy of eTrans Systems
Maps: Google Earth & Maps

6th Avenue NY Skyview

GNSS Only Data from 6th Ave New York (Connected Vehicle Pilot Site)
Part I: Quantifying Navigation Safety of Autonomous Cars

Sensor Safety Metrics and Requirements for Autonomous Passenger Vehicles (APVs)

Mathieu Joerger
Assistant Professor
The University of Arizona
APVs Around the Corner... in 1958

1958

Electronic Age

1958

COLOR TELEVISION - 1958

HIGHWAY OF THE FUTURE

CONTROLLED HIGHWAY
 PLEASE SWITCH TO ELECTRONIC DRIVE
• Current approaches to APV safety
  - focus on Level 3 APVs: (Limited Self-Driving Automation)
    - driver expected to take over at any time
  - are mostly experimental:
    • e.g., Google: 2 million urban road miles; at fault in one (1) collision (02/16)
    • e.g., Tesla: 130 million highway miles driven by autopilot, one fatality (05/16)

• Human drivers in the U.S. achieve 1 fatality per 100 million mile driven

• A purely experimental approach is not sufficient
  - in response, leverage analytical methods used in aircraft navigation safety
  - In ‘Federal Automated Vehicles Policy’ (09/16), NHTSA mentions aviation safety
• It took decades of R&D to bring alert limit down to tens of meters [WAAS]

• Challenges in bringing aviation safety standards to APVs
  • GPS-alone is insufficient → multi-sensor system needed
  • not only peak in safety risk at landing → continuous risk monitoring
  • unpredictable meas. availability → prediction in dynamic APV environment

• **Accuracy**: typically a 95% requirement

• **Integrity**: measure of trust in sensor information
  - in aviation, up to $1 \times 10^{-9}$ per operation requirement
  - integrity risk = risk of unacceptably large pose error without a timely warning

• **Continuity**: about $1 \times 10^{-6}$ per operation requirement
  - continuity risk = risk of unscheduled interruption

• **Availability**: fraction of time where accuracy/integrity/continuity are met
• Evaluate safety risk contribution of **each system component**
Ask the Experts – Part 1

Chaminda Basnayake, Ph.D.  
Principal Engineer  
Renesas Electronics America

Mathieu Joerger  
Assistant Professor  
The University of Arizona

Jonathan Auld  
Director  
Safety Critical Systems  
NovAtel
Poll #2

In your opinion, what is the most important technology in an autonomous car? (Please select your top two)

- Cameras
- Lidar/Radar
- GNSS
- Inertial
- Map Matching
Part II: Quantifying Navigation Safety of Autonomous Cars

Sensor Safety Metrics and Requirements for Autonomous Passenger Vehicles (APVs)

Mathieu Joerger
Assistant Professor
The University of Arizona
• Evaluate safety risk contribution of each system component
• Each individual laser (radar) data point provides little information

• Feature extraction
  • find few distinguishable, and repeatedly identifiable landmarks

• Data association
  • from one time step to the next, find correct feature in stored map corresponding to extracted landmarks

[processed data from the KITTI dataset: http://www.cvlibs.net/datasets/kitti/]
Experimental Setup
True Versus Estimated Trajectory

Incorrect Association

- estimated landmark location
- range domain
- position domain
Multi-Sensor GPS/Laser System

Simulation Scenario: Vehicle Driving through Forest

Direct Simulation of SLAM

Vehicle and Landmarks Position Estimation

GPS Only

GPS and LASER

LASER Only

East (m)

North (m)

GPS Satellite Blockage due to the Forest

Simulated Laser Data, Extraction and Association

Laser Scanner Range Limit

Vehicle

Landmarks

Covariance Ellipses (x70)
Direct Simulation of SLAM

GPS Satellite Blockage due to the Forest

Vehicle and Landmarks Position Estimation

Simulated Laser Data, Extraction and Association
Direct Simulation of SLAM

Vehicle and Landmarks Position Estimation

Simulated Laser Data, Extraction and Association

GPS Satellite Blockage due to the Forest
Direct Simulation of SLAM

Time: 1 s

North (m)

East (m)

Inside GNSS
NovAtel
inside unmanned systems
• The integrity risk bound accounting for possibility of IA is much larger than risk derived from covariance only

  • Incorrect association occurs for landmark 6, which appears after being hidden behind 5
Key tradeoff: Fewer extracted features

- improve integrity by reducing risk of incorrect association,
- but reduce continuity
• Major challenges to analytical quantification APV navigation safety include
  • safety evaluation of laser, radar, and camera-based navigation
  • multi-sensor pose estimation, fault detection, and integrity monitoring
  • pose prediction in dynamic APV environment

• Analytical solution to APV navigation safety risk evaluation
  • could be used to set safety requirements on individual sensors
  • would provide design guidelines to accelerate development of APVs
  • would establish clear sensor-independent certification metrics
Safety Critical Development for High Precision GNSS in Autonomous Vehicles

Jonathan Auld
Director
Safety Critical Systems
NovAtel
Hexagon AB

Positioning Intelligence

Global Positioning Solutions and Services

Land  Air  Sea

High Accuracy and Reliability

» Head office located in Calgary, Canada
» More than 400 employees
» Part of the Hexagon Group
» 20+ Years in GNSS
» Market leader in our space with >50% market share.

NovAtel® Inc.
90s and early 2000s: Accuracy

- Positioning techniques
- DGPS, RTK
- Multipath mitigation

Now: Availability

- Multi-constellation: GPS, GLONASS, Galileo, Beidou
- Sensor Fusion
- Position + orientation

Future: Safety & Reliability

- Safety of Life applications
- Functional Safety and Integrity
- Protection from spoofing/jamming
Increasing Demand for Safety in Guidance

IEC EN 61508
DO-178C
DO-254
ISO 25119
EN 50126
EN 50128
EN 50129

ISO 26262
DO-178C
DO-254

How GNSS fits into automotive positioning

- GNSS will serve as the source of Absolute PVT to the autonomous driving challenge.

- An autonomous vehicle application will expect 100% availability in all conditions and locations
  - Urban, Rural, All Weather, All Visibility

- GNSS plays a critical role in this but cannot be the sole positioning source.

- A fusion of multiple sensors will be required with GNSS playing a key role. Time alignment of sensors as well as positioning.
Today the primary use case is positioning for navigation.
Receivers are single frequency and support 1-2 constellations
Narrowband RF and Antennas
Accuracy - 2-5 meter level
Data rate outputs <=10Hz
Primarily pseudorange based positioning techniques, with some carrier phase assistance, in use.
No functional safety standards
No integrity data provided on the output solution
Built to automotive manufacturing standards
GNSS requirements for autonomous driving

• Lane level accuracy - <1 metre 3-sigma
  • Data rate outputs > 10 Hz
  • 3D Position and Velocity outputs
• Multi-frequency, Multi-constellation receiver and antenna
  • Improves overall accuracy
  • Required to assist in solution convergence time
  • Increases available measurements
• Supporting PPP correction service required over satellite and internet delivery.
• Initial focus is on Highway/Freeway with a transition to urban environments
• Functional Safety
  • ISO26262 Development
  • Integrity outputs to support protection levels
  • Authentication
Positioning Technology Options

- To allow for ubiquitous positioning at the **decimeter** level we believe a **PPP** level of service is required.
- RTK is certainly more accurate (cm level) but infrastructure costs are high and unnecessary.
- **PPP convergence times** continue to be too long for the automotive market but R&D is well underway to resolve this current limitation.
Defining Safety for a Navigation System

- **Integrity** = degree to which you can trust the information being provided by a navigation system.
- **Continuity** = ability of any navigation system to execute its function through a specified time period or operation.
- **Accuracy** = degree to which the estimated solution from a navigation system conforms to the true solution.
- **Availability** = percentage of the time that a system can be used for navigation purposes.
• Key challenge of making high precision GNSS applicable to autonomous vehicles is the safety requirements
• At the system level a safety case is developed and failure rates are allocated to sub systems
• Process and Development criteria for the Architecture, HW and SW needs to be compliant with industry standards and the applicable safety level.

### Approximate cross-domain mapping of ASIL

<table>
<thead>
<tr>
<th>Domain</th>
<th>Domain Specific Safety Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automotive (ISO 26262)</td>
<td>QM</td>
</tr>
<tr>
<td>General (IEC-61508)</td>
<td>(SIL-0)</td>
</tr>
<tr>
<td>Aviation (DO-178/254)</td>
<td>DAL-E</td>
</tr>
<tr>
<td>Railway (CENELEC 50126/128/129)</td>
<td>(SIL-0)</td>
</tr>
</tbody>
</table>

This comparison is from Wikipedia - http://en.wikipedia.org/wiki/Automotive_Safety_Integrity_Level
The GNSS PVT must now be both **Accurate and Safe**

- In all conditions (ex. poor multipath and/or low satellite count).
- Probability of misleading info at the level of $10^{-6}$ to $10^{-7}$/hr
- Balanced with Availability

**Integrity and Authentication** functions will be incorporated into PPP network.

Receiver burden will be higher than in aviation due to shorter time to alarm. RAIM techniques will need to be expanded to carrier phase positioning.
Summary of the Challenge

- Receiver and Antenna designed to hit automotive...
  - Safety and Quality requirements – ISO26262 and TS 16949
  - Cost and Volume – significantly different from current High Precision offerings
  - Styling – Antenna needs to fit the style requirements of the vehicle platform and still deliver the performance
  - PVT performance at the 1m 3-sigma level
  - A correction network delivering data over satellite and internet globally with safety considerations designed in...
    - Acceleration of PPP convergence times
    - Expansion of threat models and integrity analysis to the automotive use case

NovAtel’s Team is working to solve all of these challenges!
Visit www.insidegnss.com/webinars for:

- PDF of Presentations

Contact Info:

- Chaminda Basnayake, PhD
  chaminda.basnayake@renesas.com

- Mathieu Joerger
  joerger@email.arizona.edu

- Jonathan Auld
  Jonathan.Auld@novatel.com
Poll #3

In your opinion, what are the biggest challenges in autonomous cars (Please select your top two)

- Confidence that users will adopt
- Sensor technology
- Connectivity/Cyber security
- Certification
- Cost
Ask the Experts – Part 2

Chaminda Basnayake, Ph.D.
Principal Engineer
Renesas Electronics America

Mathieu Joerger
Assistant Professor
The University of Arizona

Jonathan Auld
Director
Safety Critical Systems
NovAtel

Inside GNSS @ www.insidegnss.com/
NovAtel @ www.novatel.com