PNT Assurance Standards for GNSS Receivers Used in Critical Applications

Brent Disselkoen, Dr. Gary A. McGraw
Rockwell Collins

ICG-8 2013
Dubai, UAE
9-14 Nov, 2013
Overview

• The lack of hardware and software Position, Navigation, and Time (PNT) Assurance Standards for Global Navigation Satellite System (GNSS) receivers increases operational risks in critical applications

• Critical applications include
  – First responders
  – Law enforcement
  – Critical infrastructure
  – Autonomous vehicle navigation

• Key risk areas include
  – Susceptibility to spoofing and interference
  – Cyber threats
  – Long-term product support and availability

PNT Assurance Standards will help ensure performance and availability for critical applications
Standards Adoption

• Historically the commercial aircraft industry has been the most proactive in developing standards for using open service GPS for flight critical applications
  – DO-229 RAIM FDE(Receiver Autonomous Integrity Monitoring, Fault Detection and Exclusion)
  – RTCA/DO-254 Hardware Design Assurance
  – RTCA/DO-178B Software Design Assurance

• This presentation proposes adopting PNT Assurance Standards for a Robust Open Service (ROS) GNSS receiver
  – Leveraging commercial aircraft industry standards and practices
  – Addressing commercial receiver technology and applications
GNSS Environment

• Multi-Constellation GNSS promises
  – Improved accuracy
    • Multiple frequencies provide ionospheric delay compensation and redundancy
    • More satellites provide better solution geometry
  – Integrity
    • More satellites provide redundancy
    • Improved control segment monitoring and communications
  – Interference immunity
    • More robust signal structures
• These promises are at risk in critical applications if
  – Signal susceptibilities are not mitigated
  – Cyber protection is not in place
  – No protection against design faults is provided

Critical applications need PNT Assurance Standards to maximize benefit of multi-constellation GNSS
# Open Service GNSS Receiver Classes

## Open Service Receiver Classes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Consumer</th>
<th>Aviation GPS</th>
<th>High-grade COTS GNSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design Assurance</td>
<td>✗</td>
<td>☑</td>
<td>✗</td>
</tr>
<tr>
<td>Security (Anti-Spoofing)</td>
<td>✗</td>
<td>Not presently required</td>
<td>☑ Signal Checks</td>
</tr>
<tr>
<td>Integrity Monitoring</td>
<td>✗</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Interference Mitigation</td>
<td>☑ DSP</td>
<td>Not presently required</td>
<td>☑ DSP</td>
</tr>
<tr>
<td>Rugged</td>
<td>☑</td>
<td>☑ Avionics Environment</td>
<td>☑</td>
</tr>
<tr>
<td>Accuracy</td>
<td>☑ L1/SBAS, L1OF</td>
<td>☑ L1/SBAS, migrating to L1/L5 GNSS</td>
<td>☑ L1, L2, L1OF, L2OF migrating to GNSS</td>
</tr>
</tbody>
</table>

DSP = Digital Signal Processing (e.g., frequency notching)
Issues with Open Service GNSS in Critical Applications

- Lack of signal validation
  - Susceptible to interference/spoofing
  - Little or no signal integrity/authentication
- Lack of design assurance
  - Hardware and software designs could have hazardous faults
- Lack of cyber protection
  - Vulnerable to malware, viruses
- Lack of long term product support
  - COTS receiver market requires frequent software revisions & model changes
  - Limited obsolescence management
- Lack of standard interfaces & form factors
  - Industry accepted interface definitions are limited
  - Few standard form factors
# Robust Open Service (ROS) GNSS Receiver Defined by PNT Assurance Standards

## Open Service Receiver Classes

<table>
<thead>
<tr>
<th>Feature</th>
<th>Consumer</th>
<th>Aviation GPS</th>
<th>High-grade COTS GNSS</th>
<th>Robust Open Service GNSS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design Assurance</td>
<td>✗</td>
<td>✅</td>
<td>✗</td>
<td>✅</td>
</tr>
<tr>
<td>Security (Anti-Spoofing)</td>
<td>✗</td>
<td>Not presently required</td>
<td>✅</td>
<td>Improved Signal Checks</td>
</tr>
<tr>
<td>Integrity Monitoring</td>
<td>✗</td>
<td>✅ RAIM/FDE</td>
<td>✅ RAIM/FDE</td>
<td>✅ RAIM/FDE</td>
</tr>
<tr>
<td>Interference Mitigation</td>
<td>✅ DSP</td>
<td>Not presently required</td>
<td>✅ DSP, Antenna AJ interfaces</td>
<td>✅ DSP, Antenna AJ interfaces</td>
</tr>
<tr>
<td>Rugged</td>
<td>✅</td>
<td>✅ Avionics Environment</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Accuracy</td>
<td>✅ L1 GNSS, L1OF</td>
<td>L1 /SBAS, migrating to L1/L5 GNSS</td>
<td>L1,L2, L1OF, L2OF migrating to GNSS</td>
<td>L1,L2, L1OF, L2OF migrating to GNSS</td>
</tr>
</tbody>
</table>

DSP = Digital Signal Processing (e.g., frequency notching)

- Good
- Marginal
- Unsatisfactory
Need for PNT Assurance Standards

- Critical applications are demanding a new class of receivers: Robust Open Service (ROS)
  - Address issues associated with low-end Consumer GNSS receivers
  - Add signal integrity to assure PNT performance
  - Protect against ‘malware’ in ASICs and software

- PNT Assurance Standards for ROS receivers do not exist today
  - No basis for assessing performance, or protection
  - No industry accepted definitions and criteria
  - No method for determining whether the receiver is trustworthy
PNT Assurance Standards Development

PNT Assurance Standards should address:

- **Integrity Monitoring**
  - Recommend leveraging aviation standards for RAIM/FDE
- **Signal Authentication**
  - No prior standards exist, especially for authentication between constellations
- **Interference Mitigation / Spectrum Compatibility**
  - Few prior standards exist, especially for intentional interferers
- **Hardware Design Assurance**
  - Recommend leveraging RTCA standards for hardware
- **Software Design Assurance**
  - Recommend leveraging RTCA standards for software
- **Exportability**
  - Need standards that are widely accepted internationally
- **Interface definitions**
  - Need standards that ease integration and encourage multiple vendors
- **Form factors**
  - Need standards that support diverse applications and encourage multiple vendors
- **Certification**
  - Recommend leveraging avionics certification standards
Summary

- There is a strong need for PNT Assurance Standards for Critical Applications
  - Not available in low-end consumer GNSS receivers
  - Critical Applications need a method to procure Robust Open Service (ROS) GNSS receivers

- Key Challenges
  - Critical applications industry base is large, so agreement on standards will take time
  - Policies in some countries will preclude trusting designs from other countries
  - Cost for complying to new PNT Assurance Standards could be prohibitive for some vendors

- Recommendations
  - Start with civil aviation standards
  - Define different categories of ROS receivers to address new market space