GBAS Certification

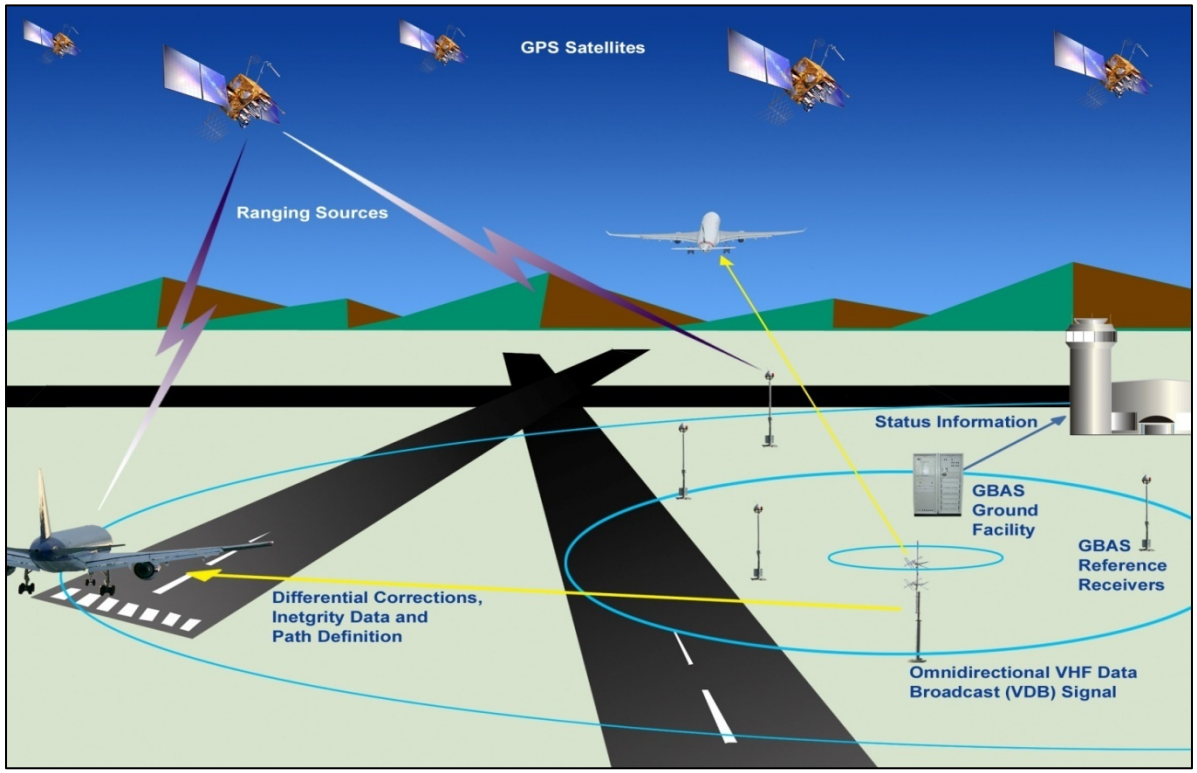
Randy Key AJW-19
WAAS Operations Group

Presented to: CAAC
October 21, 2010

Presented by
John Warburton AJP-652

Federal Aviation Administration

LAAS (Local Area Augmentation System)



- **Reference Receiver collects GPS measurements, calculates information necessary to maintain integrity/ accuracy.**
- **Central Processing Unit calculates correction, integrity, ground station and path information necessary to support guidance for precision approach.**
- **VHF Data Broadcast transmits the GBAS message information to the aircraft via a secure datalink.**
- **Air Traffic Status Unit (ATSU) provides Air Traffic Control with the ground station's current status.**

GBAS CAT I Approval

- **To be approved by FAA, system or equipment must be shown to meet ICAO, FAA and/or other (e.g. RTCA) recognized standard.**
- **The baseline for the FAA GBAS is the FAA GBAS Specification 2937a**

SYSTEM DESIGN APPROVAL

- System Safety Assessment
- System Engineering
- Software Design Assurance
- Complex Hardware Design
- System Level Verification
- Commercial Instruction Book
- Training Material Review
- System SRMD
- Operational Evaluation

⇨

FACILITY APPROVAL

- Installation Requirements
- O&M Manual
- Operator training
- Local SRMD (installation)
- Flight Procedures
- Flight Inspection

⇔

SERVICE APPROVAL

- Aircraft Installation Approval
- ATC Training
- Pilot Training
- Instrument Flight Criteria
- Flight Procedures
- Local SRMD (procedures)

GBAS Integrity

- **Responsibility for GBAS Integrity resides in the Ground Facility**
  - The user (aircraft) receives a set of integrity parameters from the LGF and applies those in a set of standardized equations to determine protection levels
  - A protection level bound, or Alert Limit, is transmitted from the LGF with each procedure
  - The aircraft must check the calculated result against the requirement
- **The Service Provider is responsible for ensuring that the uplink integrity parameters are accurate and that they provide the required function**
  - Ensuring the uplink integrity will require a review of the equipment design, siting methods/processes, installation methods/processes, and the methods/processes used to characterize the actual/installed system performance

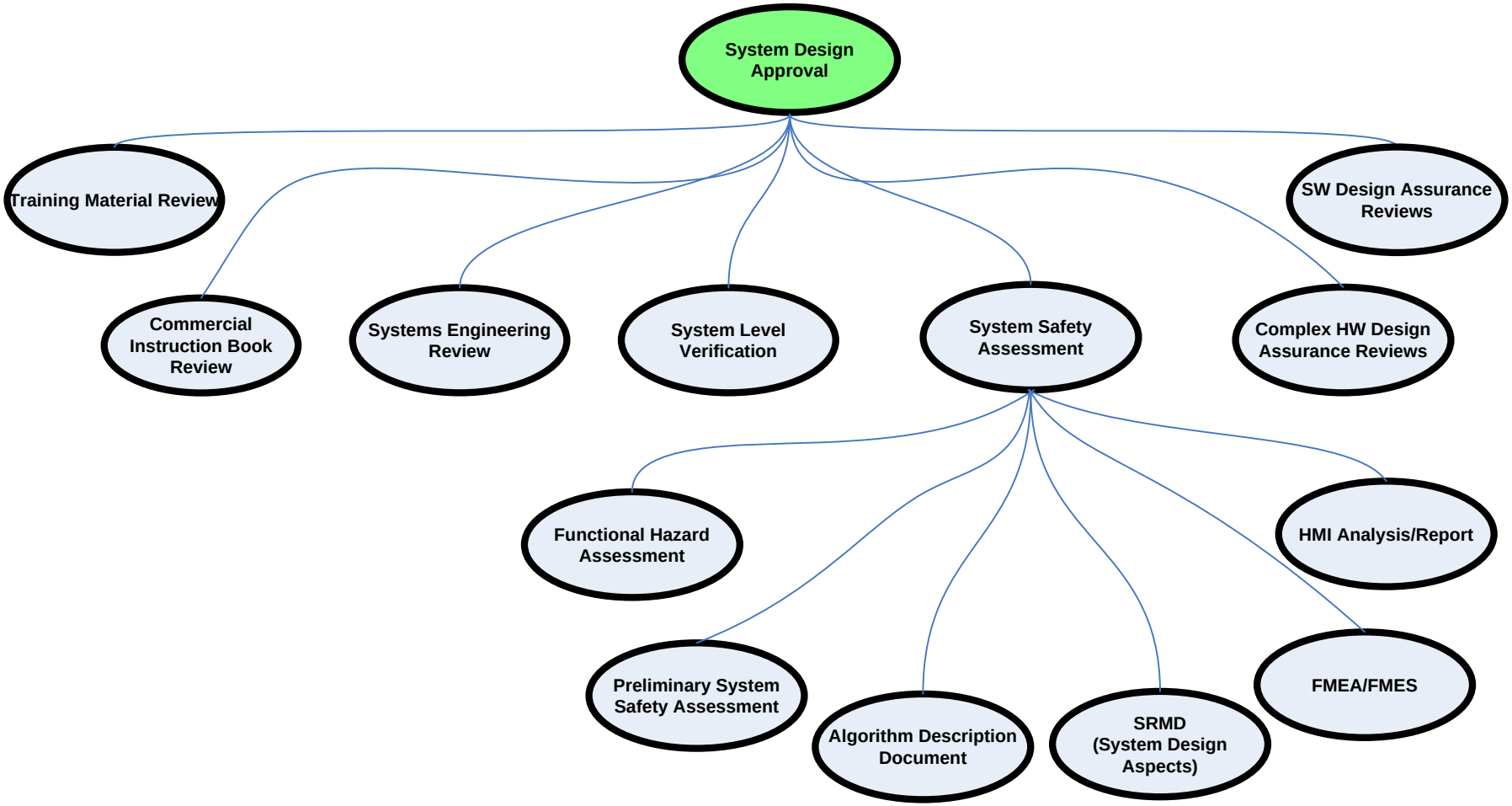
GBAS System Design Approval (SDA) Requirements

- **System Design Approval activities are based on:**
  - FAA Order 6700.20A, Non-Federal Navigational Aids and Air Traffic Control Facilities
  - 14 Code of Federal Regulations (CFR) Part 171.75 allows for FAA approval of new or non-standard systems and equipment.
  - Baseline is the FAA Non-Federal LAAS Specification, *FAA-E-AJW44-2937A Category I Local Area Augmentation System Ground Facility*
- **GBAS Facility Approval and Service Approval follow SDA**

GBAS System Design Approval Planning Documents developed by FAA

- **Role of applicant is to show compliance; role of FAA is to find compliance via reviews, audits, independent verification**
- **System Design Approval Plan**
  - Establishes SDA requirements, responsibilities
  - Establishes process for Waivers, Engineering Change Proposals
- **System Design Approval Process**
  - Outlines detailed FAA processes and procedures
    - Purpose, scope of specific activities
    - Objectives and evaluation criteria
    - Guidance documents
    - Procedures necessary to find compliance
  - Defines the design data, artifacts that substantiate compliance
  - Compliance Matrix captures the approved hardware and software configuration

System Design Approval



SDA Compliance Matrix

- **The Compliance Matrix captures activities, resources, procedures, objectives, and documentation necessary to:**
  - **Identify** what needs to be done (i.e., what the applicant needs to show compliance to, tailored to the applicant's approach)
  - **Show progress** on the review (i.e., how many of the compliance elements have been found acceptable? Are we done yet?)
  - **Document what was reviewed** to show compliance with each individual requirement (i.e., gives us a record of what was reviewed, and what version)
- **Includes FAA specification requirements (Traceable to ICAO SARPS)**
- **Includes design assurance requirements for software, complex hardware, systems safety, etc.**
- **Automated tool to track compliance matrix activities, data, actions and status**

Compliance Matrix

ID	Task Name
1	**Honeywell Submittals**
2	**Deliverable Data**
63	**Auditable Data**
184	**Systems Engineering Process**
197	**System Safety Process**
219	**Software Design Assurance**
227	**Complex Hardware Design Assurance**
232	**Commercial Instruction Book Review**
237	**Training Review**
242	**System Level Verification**
243	**Coverage volume**
252	**Integrity**
278	**Continuity**
281	**States**
285	**Modes**
311	**Fault monitoring**
347	**Fault recovery**
355	**Alerts**
378	**Alarms**
389	Software
390	**Complex hardware**
394	**Data broadcast**
541	**RF transmission**
545	**RF monitoring**
553	**System requirements**
596	**Fault diagnostics**
602	**Reliability and maintainability**
607	**Security**
628	**Physical design**
654	**Control and display**
745	**Recording**
755	**Interface requirements**

Sub Category

- Compliance Matrix
  - 750 + items

← Main Category

ID	Task Name	Duration	Start
390	**Complex hardware**	**1 day?**	**Mon 8/14/**
394	**Data broadcast**	**1 day?**	**Mon 8/14/**
395	3.2.1.4.1: Message Types	1 day?	Mon 8/14
396	3.2.1.4.2: Parameter Storage	1 day?	Mon 8/14
397	3.2.1.1: LAAS Message Block	1 day?	Mon 8/14
398	3.2.1.1.1.1: Non-Test Mode	1 day?	Mon 8/14
399	3.2.1.1.1.2: Test Mode	1 day?	Mon 8/14
400	3.2.1.1.2: Ground Station Identification	1 day?	Mon 8/14
401	3.2.1.1.3: Message Type Identifier	1 day?	Mon 8/14
402	3.2.1.1.4: Message Length	1 day?	Mon 8/14
403	3.2.1.2: Cyclic Redundancy Check (CRC	1 day?	Mon 8/14
404	3.2.1.2.9.1: Broadcast	1 day?	Mon 8/14
405	3.2.1.2.9.2: Ranging Sources	1 day?	Mon 8/14

System Design Approval Areas

- System Engineering
- System Level Verification
- Software Design Assurance
- Complex Hardware Design
- Commercial Instruction Book
- Training Material (Maintainer Training)
- System Safety Assessment
- Operational Evaluation

System Engineering Review

- **Review of applicant's system engineering processes and products**
  - Human Factors
  - Personnel Safety
  - Security
  - Reliability/Availability
  - Spectrum
  - Requirements Management process
  - Configuration Management process
  - Quality Assurance process

System Level Verification Review

- **Intent is to find compliance with every system requirement in the Specification**
  - Review of applicant's verification processes and products
  - For each requirement in the non-Fed specification:
    - Trace Requirement from non-Fed spec through design
      - Requirements decomposition, implementation
    - Review Test Plan, Procedures and Results
      - Hardware/Software integration plans, procedures, and results,
      - Inspection procedures and reports,
      - Analysis and simulation files and reports
    - Ensure test approach is adequate

Software Design Assurance Review

- **Intent is to find compliance with the applicable objectives listed in RTCA DO-278**
  - Review of applicant's (and sub-contractors') software development processes and products
  - Perform desk reviews and on-site audits at key points during the SW development lifecycle
    - Review planning documents, standards,
    - Review requirements, design, code, & integration artifacts,
    - Review verification plans, procedures, & results,
    - Review CM & QA records,

Complex Electronic Hardware Review

- **Intent is to find compliance with the appropriate objectives listed in RTCA DO-254**
  - Review of applicant's (and sub-contractors') complex electronic hardware (CEH) development processes and products
  - Perform desk reviews and on-site audits at key points during the CEH development lifecycle
    - Review planning documents and standards,
    - Review requirements, design, simulation, & integration artifacts,
    - Review validation and verification processes, procedures, & results,
    - Review CM & process assurance records,

Commercial Instruction Book Review

- **Intent is to find compliance with FAA-D-2494/b**
  - Contains all necessary information, is up to date with the as-built equipment and has been validated by the applicant
  - In-Process Reviews of the applicant's Commercial Instruction Book (CIB) development activities
    - Technical descriptions, standards & tolerances, maintenance schedules & procedures, parts lists, installation procedures, etc
  - Review of applicant's CIB Validation
    - FAA review and hands-on verification of maintenance procedures (periodic and corrective), operations, troubleshooting, installation procedures

Training Material Review

- **Review of the training development process and training materials**
  - Intent is to ensure that training materials:
    - Are consistent with the equipment design,
    - Appropriately cover periodic and corrective maintenance, and
    - Appropriately cover operations activities (installation, calibration, normal operation, etc.)

System Safety Assessment Review

- **Review of applicant's system safety processes and products using:**
  - ARP 4754, Certification Considerations for Highly-Integrated or Complex Aircraft Systems
  - ARP 4761, Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment
  - FAA-prepared Operational Hazard Assessment (OHA)
- **The FAA's Safety Management System (SMS) must be employed IAW FAA Policy**
  - FAA-developed Safety Risk Management Document (SRMD) must be coordinated and approved
    - Residual risks are acceptable
  - Disposition of system risks required prior to System Design Approval

System Safety Assessment

- **Standard Safety Documentation**
  - Applicant System Safety Assurance Plan
  - Functional Hazard Assessment (FHA)
  - Preliminary System Safety Assessment (PSSA)
  - System Safety Assessment (SSA)
- **Additional Safety Related Documentation**
  - Algorithm Design Document
  - HMI Analysis/Report

Hazardously Misleading Information (HMI) Report

- **An HMI report details the processes and assumptions that demonstrate a GBAS is safe.**
  - A similar process was effective in verifying FAA Wide Area Augmentation System (WAAS) integrity
  - HMI report is a summary of the integrity work, detailing the information in the system algorithm description documents
  - Tool used to help the technical team communicate with the certification authority

Hazardously Misleading Information (HMI) Analysis

- **The five steps in the HMI analysis are:**
  - Formalize and obtain approval for the top level integrity architecture;
  - Approve the fault trees;
  - Approve the complete list of threats;
  - Approve specific integrity analysis methodologies for each of the monitors; and
  - Complete and obtain approval for the HMI analysis document.

LAAS Integrity Panel (LIP) and HMI

- **The LAAS Integrity Panel or LIP was group of experts used by the FAA to evaluate the HMI products**
- **LIP Members included:**
  - Ohio University, Stanford University, Illinois Institute of Technology, Oakland University, MITRE, FAA, and Honeywell
- **Approval was granted via consensus vote on each of the Integrity Risk Compliance Argument (IRCA) statements**
  - Sixteen formal LIP Meeting and countless teleconferences were convened to achieve and verify consensus

Safety Risk Management (SRM)

- **Design specific Safety Risk Management Document (SRMD) will be generated to address generic "design" risks**
  - To be generated with no particular facility, installation, or airport in mind
  - Developed by the GBAS program office SDA System Safety Team
    - SRM Principals Inherent in the SDA Process
      - Hazards identified
      - Safety Requirements Identified/Allocated/Verified
      - Mitigations defined and verified
  - Leverage information contained in the developers system safety assessment and analysis documentation
  - Intended to be referenced by the site specific SRMDs generated by the service area safety assurance groups

Safety Risk Management

- **Site specific SRMDs to address site specific risks**
- **Intended to address risks that could not be addressed during the development of the generic design SRMD**
  - GBAS Installation impact
    - Facility Approval (i.e., 6700.20a),
    - installation issues associated with satellite masking due to local terrain, etc
  - GBAS Operations impact
    - Approach Procedure Development and Approval,
    - AT Training/Familiarization, AT status display information (or lack thereof)

Operational Evaluation

- **The purpose of this activity is to review the operation of the system in the installed configuration.**
  - **Evaluation Criteria**
    - The system is operated in accordance with the operating instruction provided in the Commercial Instruction Book to ensure that the system operates as intended.
    - System Stability Test
      - Operate the system over continuously over an extended period of to evaluate the basic stability of the system.
    - System Log Event Recording
      - Review of system event / fault logs for false alarms, false exclusions, missed detections, etc.)
  - **Evaluation of System Operation**
    - Review independent user performance data to verify that the information reported in the event log is correct. This is done by comparing the system data to data recorded by an independent system such as the FAATC's GAEM
    - Evaluate the system behavior when confronted with obstructions and reflectors (this is done to verify that the system responds appropriately with an excluded RR, an event log entry, etc)

GBAS CAT I Approval

- **To be approved by FAA, system or equipment must be shown to meet ICAO, FAA and/or other (e.g. RTCA) recognized standard.**
- **The baseline for the FAA GBAS is the FAA GBAS Specification 2937a**

SYSTEM DESIGN APPROVAL

- System Safety Assessment
- System Engineering
- Software Design Assurance
- Complex Hardware Design
- System Level Verification
- Commercial Instruction Book
- Training Material Review
- System SRMD
- Operational Evaluation

⇨

FACILITY APPROVAL

- Installation Requirements
- O&M Manual
- Operator training
- Local SRMD (installation)
- Flight Procedures
- Flight Inspection

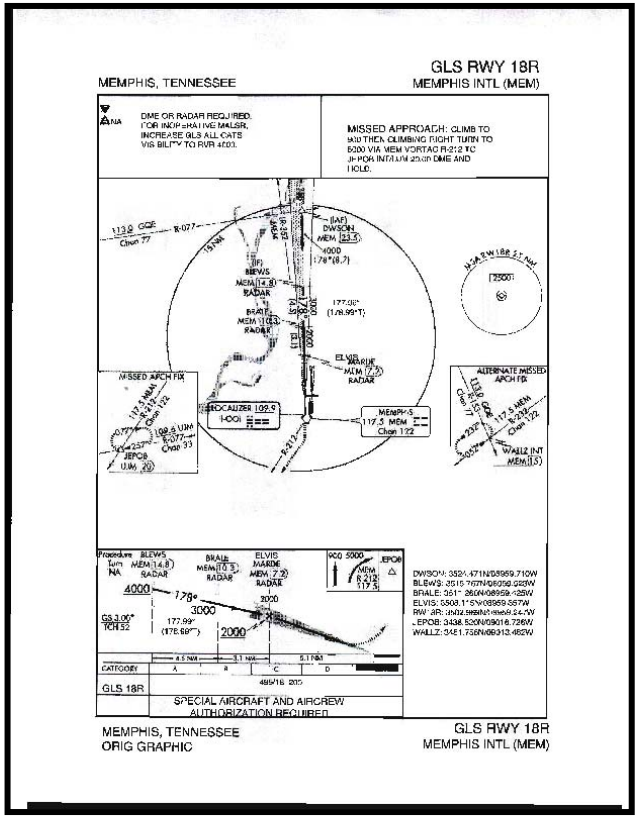
⇔

SERVICE APPROVAL

- Aircraft Installation Approval
- ATC Training
- Pilot Training
- Instrument Flight Criteria
- Flight Procedures
- Local SRMD (procedures)

Key Components/Considerations of the Facility Approval Plan

- **The Facility Approval Plan describes the activities, objectives, and documentation necessary to address:**
  - Installation
  - System Operations
  - Security
  - Spectrum
  - Personnel
  - Test and Evaluation
  - Maintenance
- **Local SRMD**
- **Flight Procedures**
- **Flight Inspection**



GBAS CAT I Approval

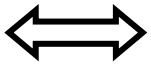
- **To be approved by FAA, system or equipment must be shown to meet ICAO, FAA and/or other (e.g. RTCA) recognized standard.**
- **The baseline for the FAA GBAS is the FAA GBAS Specification 2937a**

SYSTEM DESIGN APPROVAL

- System Safety Assessment
- System Engineering
- Software Design Assurance
- Complex Hardware Design
- System Level Verification
- Commercial Instruction Book
- Training Material Review
- System SRMD
- Operational Evaluation

FACILITY APPROVAL

- Installation Requirements
- O&M Manual
- Operator training
- Local SRMD (installation)
- Flight Procedures
- Flight Inspection



SERVICE APPROVAL

- Aircraft Installation Approval
- ATC Training
- Pilot Training
- Instrument Flight Criteria
- Local SRMD (procedures)

Service Approval – User Requirements

- **Aircraft Equipment**
  - Aircraft equipment designs approved via FAA Technical Standard Orders (TSOs)
    - TSO-C161 (GBAS equipment)
    - TSO-C162 (GBAS VHF Receiver)
    - TSO-C190 (Active Antenna)
  - Aircraft installations approved via existing FAA processes (e.g., TC, STC, etc)
- **User/Airlines**
  - Coordinating Approval with FAA Flight Standards POI (Principle Operations Inspector) assigned to an air carrier certificate holder and responsible for the approval of this training
  - Continental and Qantas use Aircrew Bulletins
- **ATC Training**
  - Computer based training
    - GBAS technology, procedures, phraseology, etc.

GBAS Avionics Integration

- **GBAS/LAAS CAT I avionics documents completed**
  - (MASPS / MOPS / TSO / SARPS)
- **LAAS Integration into Multi Mode Receiver (MMR) completed**
  - Rockwell Collins MMR
- **Boeing**
  - 737- 800 series GBAS capable,
  - B787 and B 747-800 GBAS as standard capability
- **Airbus**
  - A320/A380 certification completed
  - Planning for GBAS option in all new generation aircraft

Summary

- GBAS System Design Approval completed in Sept 2009 for Honeywell SLS 4000 “SmartPath”
- Certification process divided into System Design Approval, Facility and Service Approval
- Honeywell System Design Approval lasted approximately 3 years
- System Design Approval Process defines design data, artifacts that substantiate compliance with GBAS Specification and a compliance Matrix capturing the approved hardware and software configuration