

FAA Certification of a MEMS Attitude and Heading Reference System

Elecia White, *Crossbow Technology, Inc.*

Jose A. Rios, *Crossbow Technology, Inc.*

1 BIOGRAPHY

Elecia White has been a software engineer at Crossbow Technology, Inc., San Jose, CA since January 2000. Her responsibilities include firmware architecture, development and hardware integration for the IMU product line. She is the primary point of contact for Crossbow's software certification effort. Before Crossbow, Elecia spent five years as software engineer and technical lead at Hewlett-Packard. She received a B.S. from Harvey Mudd College.

Jose Rios has been serving as Senior Design Engineer at Crossbow Technology, Inc., San Jose, CA, since June 1998. He is responsible for algorithm design and firmware development for a family of solid-state vertical gyro and AHRS products. From 1992 to 1998 he was a Senior MTS at The Aerospace Corporation. His work included GPS/INS sensor fusion, antenna pointing control loop stability analysis, and guidance law performance analysis. He received an Engineer's and M.S. degree from the EE/Control Systems department at UCLA, and a B.S. from Harvey Mudd College.

2 ABSTRACT

A low cost MEMS inertial measurement unit (IMU) has been developed to be submitted for FAA approval. The system is a part of the Crossbow Technology, Inc AHRS500GA family of inertial sensor products. The system is an unaided, high performance, solid-state attitude and heading reference system intended for General Aviation applications. The strap-down inertial system provides attitude and heading measurement with static and dynamic accuracy comparable to traditional spinning mass and directional gyros. The system has been designed to comply with the Federal Aviation Authority's (FAA) high standards of safety and reliability, including extensive built in test (BIT) capability. Crossbow will demonstrate to the certification authority all of the concepts and methodologies employed to produce reliable software per guidelines in DO-178B "Software Considerations in Airborne Systems and Equipment Certification." Consideration will be given to all aspects of software production: planning, design, verification,

management and quality control. Further, the system will provide an accurate inertial reference in avionic dynamic environments including altitude, temperature, shock, and vibration according to the guidelines in DO 160D "Environmental Conditions and Test Procedures for Airborne Equipment." The unit will be certified and manufactured according to the minimum performance standards described in:

- TSO-C4c - Bank and Pitch Instruments
- TSO-C3d - Turn and Slip Instrument
- TSO-C6d - Direction Instrument, Magnetic (Gyroscopically Stabilized)

In addition, a supplementary type certification (STC) will also be submitted for the unit as a primary flight instrument for Class I-III aircraft. The process of certification can be daunting, particularly the software certification effort.

3 INTRODUCTION

Most aircraft have several instruments that are traditionally driven by mechanical gyroscopes to assist in flying and navigation. These instruments are governed by technical standard orders (TSOs) written by the FAA.

The attitude indication (also known as the vertical gyro) is governed by TSO-C4c for Bank and Pitch Instruments. The turn and slip indicator is governed by TSO-C3d for Turn and Slip Instruments. Finally, TSO-C6d is for a Gyroscopically Stabilized Magnetic Direction Instrument. For the last, aircrafts typically have a compass, and in some cases a flux valve (also known as a magnetometer) to which a directional gyro is connected in order to cancel long term drift. If the aircraft does not have an electronic flux valve, then the directional gyro or DG has to be manually reset to the compass reading during straight and level flight (when the compass is accurate) on a periodic basis.

Because mechanical gyros are constructed with many moving parts with close tolerances, they malfunction easily. As the ball bearings that support the high-speed wheel and the gimbals begin to wear, they contribute to precession errors. Compounding the issue with vacuum

gyros, is that dirt and dust in the vacuum line can destroy the bearings. Another common problem is that long periods of inactivity can also cause the mechanical gyros to stop functioning altogether or reduce accuracy and increase drift rates. The recommended operating life of most mechanical gyros is only several hundred hours. In addition to the unreliability of the systems, mechanical gyros have limited accuracy and resolution. The design of the majority of mechanical gyros used in General Aviation today was done in the 1950s or before, and the manufacturing techniques have not kept pace with technology. Of course, pilots know that if they do aerobatic or other aggressive maneuvers the majority of mechanical gyros lose their minds and in some cases break.

Ring laser gyro systems, constructed without spinning wheels or gimbals, replaced the mechanical gyro systems in most military and commercial aircraft but the cost (>\$100k) is prohibitive for the General Aviation market. A breakthrough occurred when techniques in silicon fabrication technology allowed for the creation of accurate inertial sensors in silicon. This technology is known as Micro Electro-Mechanical Sensors (MEMS), and is in high volume production today.

Crossbow has been developing low cost solid-state systems that measure roll, pitch, and heading using MEMS technology in commercial, industrial and aerospace markets since 1998. All of the Crossbow Attitude Heading Reference Systems, or AHRSSs, use a 3-axis accelerometer and a 3-axis rate sensor to make a complete measurement of the dynamics of the system. The addition of a 3-axis magnetometer inside the Crossbow AHRSSs allow them to make a true measurement of magnetic heading without an external flux valve.

4 THE CROSSBOW AHRSS500GA

The Crossbow AHRSSs are a solid-state equivalent of a vertical gyro/artificial horizon display combined with a directional gyro and flux valve. All of the Crossbow AHRSS units are low power (< 4.5W), reliable (> 20,000 hr MTBF) and accurate (better than 2 degrees in roll, pitch, and heading). The Crossbow AHRSSs are designed to operate in a stand-alone mode; they do not need input from external air data, magnetometers, or GPS. This makes installation easy, and improves the reliability of the system.

The Crossbow AHRSS500GA is the latest generation of vertical gyro systems in the AHRSS family. It is able to provide stable roll, pitch and heading measurements under high dynamic conditions; thus, it overcomes the drawbacks of conventional attitude measuring devices, which corrupt under acceleration. Furthermore, the

device provides a self-tuning system that automatically compensates for errors in the gyros. The system is unaided from any external sensors; it does not use air data, GPS or wingtip magnetometers.

The system can generate accurate attitude data based on measurements obtained from relatively inexpensive, mid-level performance sensors. An in-house developed factory calibration process allows characterization of the sensors for known deterministic errors and writes a compensation table to non-volatile memory in the system.

4.1 AHRSS500GA Description

Accurate attitude sensing is accomplished by measuring acceleration and angular rate about each axis to compute roll and pitch attitude relative to the gravity vector. Solid-state accelerometers and rate sensors are assembled into a small common housing for applications in rugged environments. Measurement errors attributable to fabrication misalignments are calibrated out following initial assembly for highly reliable and accurate outputs from a compact, robust assembly of components.

The angular-rate sensors and accelerometers are integrated into an Inertial Sensor Assembly (ISA) that is shock and vibration isolated. Vibrating silicon elements operate as rate sensors responsive to Coriolis forces to produce angular rate outputs independent of acceleration. Micro machined silicon devices operate as differential capacitors to sense acceleration in aligned directions independent of angular rate about the orthogonal axes. The three-axis magnetometers are high accuracy fluxgate sensors. They are mounted on an internal circuit board, and attached with the other electronics. The ISA is packaged with the electronics and magnetometer into a single unit.

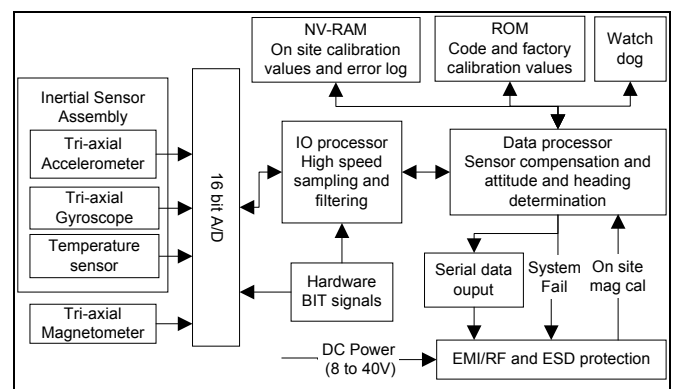


Figure 4-1 AHRSS500GA System Architecture

Analog sensor output is converted to digital data via a simultaneous sampling A/D converter system at a very high frequency. The signals are filtered via an FIR filter and output to the data processor at a frequency well

beyond the expected dynamic range (1kHz). The system's frequency response characteristics have been analyzed in detail to mitigate random vibration effects.

After the information is transferred to the data processor, it is further smoothed with an IIR filter on a floating point DSP. Temperature variations, misalignment, scale factors and bias errors are removed according to the calibration tables generated in the manufacturing process.



Figure 4-2 AHR500GA system

The attitude and heading determination algorithm is divided into two separate entities. Gyro measured angular rate information is integrated in the attitude processor. If the initial attitude of the vehicle could be known, and if the gyros provided perfect readings, then the attitude processor would suffice. However, the initial attitude is seldom known, and gyros typically provide corrupted data due to bias drift and turn-on instability. Both gyros and accelerometers suffer from bias and bias drift terms, misalignment errors, acceleration errors (g-sensitive), nonlinear (square term), and scale factor errors. The magnetometers are also susceptible to magnetic disturbances, which corrupt their measurement of the Earth's magnetic field. These hard iron errors are calibrated out once the system is installed in its final mounting position. The largest error in attitude and heading propagation is associated with the gyro bias terms. Without a filter structure and separate independent measurements from the accelerometers, gyros and magnetometers, the attitude processor would diverge from the true trajectory. The Kalman filter attitude correction component therefore provides an on-the-fly calibration for the gyros by providing corrections to the attitude processor trajectory and a characterization of the gyro bias state. The accelerometers provide an attitude

reference using gravity, and the magnetometers provide a heading reference using the Earth's magnetic field vector.

Data collection and attitude and heading determination occurs internally at 1kHz with response to 50Hz dynamics. The fast internal rate allows the system to make minor corrections very rapidly.

The system outputs the calibrated sensor data and calculated attitude and heading via serial link (RS232 or 422).

4.2 Built in Test

The AHR500GA has extensive built in test capabilities. Most of the system is monitored on a continuous basis. Almost all of the system is verified upon power on. See Table 4-1 AHR500GA Built in Test.

Table 4-1 AHR500GA Built in Test

Test	Method	On	Cont.
Power supply voltage	ADC	Y	Y
ADC integrity	Reference voltages	Y	Y
Gyro integrity	Monitor current draw	Y	Y
Accelerometer integrity	Monitor current draw	Y	Y
Temperature sensor integrity	Monitor current draw	Y	Y
Temperature Sensor	ADC	Y	Y
Magnetometer integrity	Supplied by magnetometers	Y	Y
RAM memory integrity	Write/Read 80% of RAM	Y	N
ROM memory integrity	Check sums through data	Y	N
Processor integrity	Errors reported in processor registers	Y	Y

The hardware BIT will check the current draw of each sensor as well as various reference and diagnostic voltages throughout the system.

The software BIT will check memory through checksums and write/read verification. The code has many checks (asserts, flags) that are reported to the user. The software BIT also examines the system for conditions that are abnormal but recoverable, such as sensor saturation and mathematical errors flagged by the software or by the processor. Finally, the software BIT also checks for conditions that are normal but may be interesting to the user such as a coordinated turn flag.

In addition to the errors reported to the user via the normal serial packet, an error log is stored in non-volatile

memory. The error log contains all actual BIT errors (not the informational only) sent to the user. The error log allows the factory to debug intermittent problems in the field.

4.3 Internal magnetometers

The magnetometers for the system are internal to the unit. The 3-axis magnetometers are strapped down. During the installation procedure, a hard iron calibration is performed. A hardware line triggers hard iron calibration. A series of maneuvers are performed; a two-dimensional calibration can be performed on the ground by turning the plane in circle. A better, three-dimensional calibration can be performed through a series of simple flight maneuvers. The software (via the BIT mechanism) provides status information for completion of calibration.

Because the magnetometers are internal and thus fixed to the plane, the hard iron calibration works tilted as well as straight and level. Due to the gimbals, standard direction instruments hard iron calibration does not work when the unit is tilted. Crossbow has extensive experience with internal magnetometers on small aircraft and hard iron calibration.

One advantage to certification is that installation into each plane is completely specified with detailed installation documents (see 5.2). Since the hard iron effect drops off with the cube of distance, finding a desirable location away from moving metal in each plane is achievable.

4.4 System Display

The AHRS500GA is an inertial measurement unit that outputs digital data in a serial manner. This data must be presented to the pilot in an FAA accepted manner. A display example of a Bank and Pitch Instrument and Direction Instrument is shown in Figure 4-3. A Turn and Slip Instrument will need to be added to the display.



Figure 4-3 Attitude and heading reference display example

The Crossbow AHRS500GA has a digital computer compatible output. Packets of digital information containing roll, pitch, heading, acceleration, and turn rate are sent out in standard serial format up to 160 times per second. This makes it easy to connect to digital displays – like those in the new glass cockpit systems. Several companies are now releasing General Aviation glass cockpits systems that will work with the AHRS500GA.

4.5 AHRS500GA Performance Results

In order to evaluate the performance of the Crossbow AHRS500GA, several flight tests were conducted, which were designed to compare the outputs of a unit against a high performance military navigation grade INS system. The reference INS chosen was the Litton LN-100G INS.

A test procedure was designed which enabled a real world side-by-side comparison of the AHRS500GA with the Litton LN-100G. The aircraft chosen for the tests was a twin-engine, six-seat Piper Seneca. Both units were mounted onto a plate fixture, which could be easily snapped into the mounting brackets of one of the passenger seats. The plane then flew a profile designed to tax the attitude estimation algorithm and approximate most flight mission profiles. While still technically non-acrobatic, the flight test maneuvers at times reached 2G accelerations. Benign coordinated turns were flown to prove the stability of the algorithm. Aggressive high dynamic maneuvers were flown to test the algorithm's performance.

A representative set of the maneuvers is presented in the figures below. Each plot contains the AHRS500GA attitude results (blue) along with the Litton LN-100G results (red).

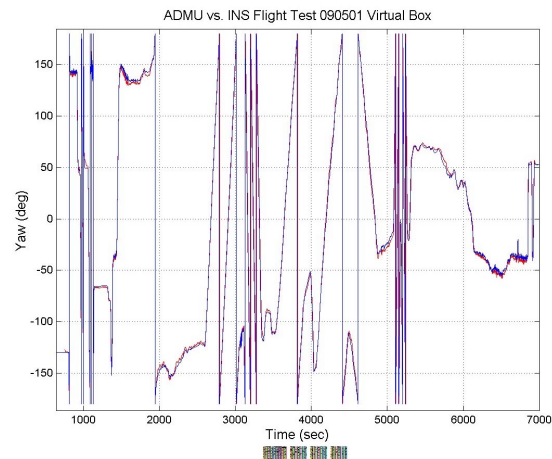


Figure 4-4 Heading over flight

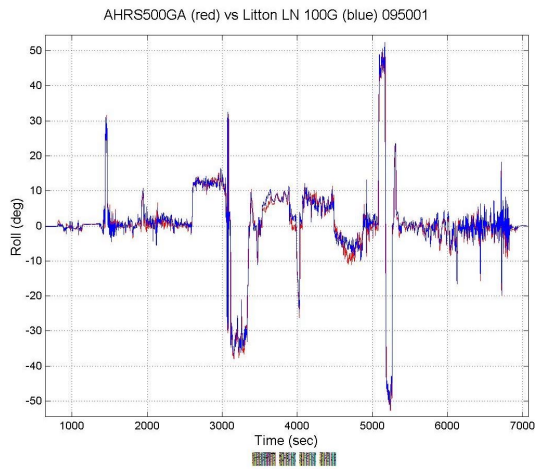


Figure 4-5 Roll over flight

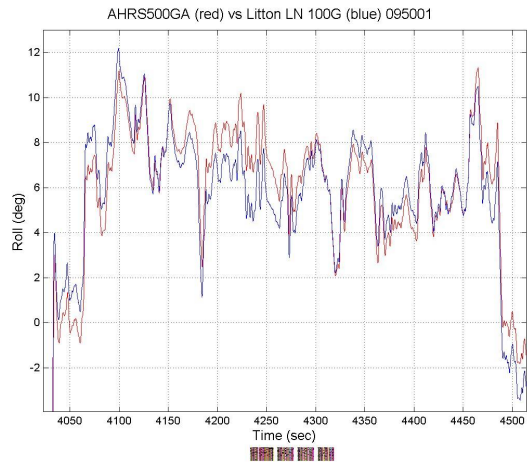


Figure 4-8 Roll during fugoid maneuver

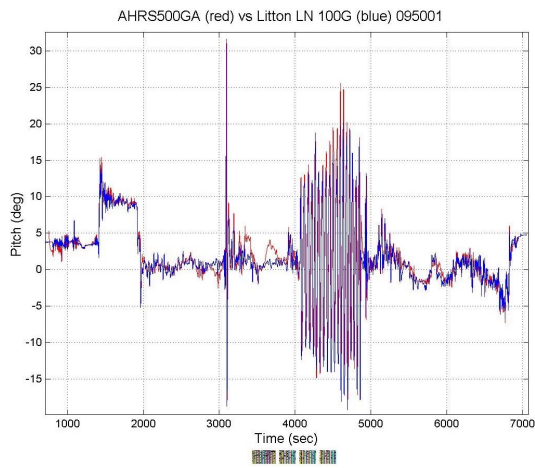


Figure 4-6 Pitch over flight

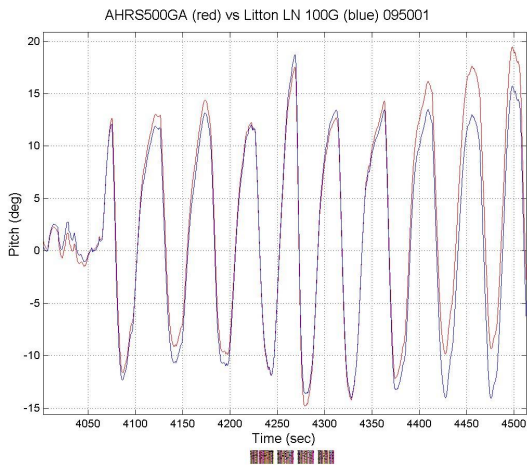


Figure 4-9 Pitch during fugoid maneuver

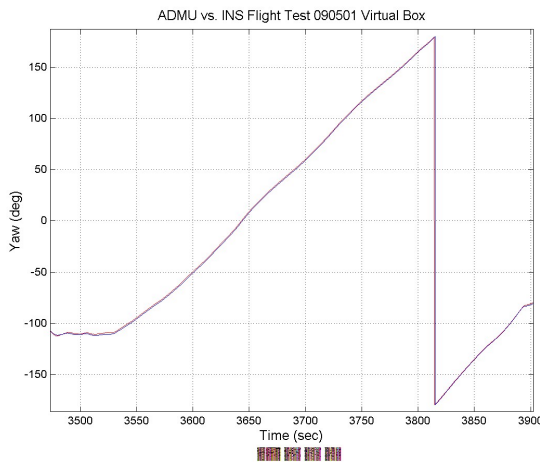


Figure 4-7 Heading in shallow turn maneuver

For the entire mission profile, the absolute attitude error never exceeded 5 degrees even under extreme duress (fugoid), with an average error of less than 1 degree regardless of the maneuver. This makes the AHR500GA a very powerful vertical gyro replacement.

5 CERTIFICATION PROCESS

The certification process is non-trivial. The process is designed to ensure that failures occur infrequently and that the failures that do occur are not severe and provide adequate warning to the crew. This section provides a general overview of the process; the following sections give a more in depth view of the various documents provided and required by the FAA.

Aircraft are divided into classes; classes I-IV are considered General Aviation with class IV being commuter aircraft. Federal Aviation Regulations Part 23 governs the certification of General Aviation avionics. It is a complex document. However, FAA Advisory Circular 23.1309-IC is the best initial source of information involving certification of a General Aviation

system. It has the background and definitions necessary to get the process started.

The instruments are certified according to specifications set forth in technical standard orders (TSOs) provided by the FAA. AHRS500GA will be certified using TSO-C4c for Bank and Pitch Instruments, TSO-C3d for Turn and Slip Instruments and TSO-C6d for Gyroscopically Stabilized Magnetic Direction Instruments. These TSOs reference other documents for the minimum display, performance and environmental specifications for avionics equipment. The standards are clearly targeted toward mechanical gyroscopes that can fail in dynamic situations instead of MEMS sensors that are far more difficult to damage. In addition, some of the possible malfunctions are inconceivable in MEMS sensors (i.e. caging and speed problems). In addition, customers demand superior performance than is specified in the TSOs. The tests are a minimum set, not a complete set. Crossbow will demonstrate a much greater range of operating environments.

The standards are supplemented by very detailed documents in several areas. Environmental requirements and performance will be verified using DO-160D. Software requirements and performance will be verified using DO-178B. DO-254 shall be used as a reference and guide for hardware design. The AC 23-1309 provides a reference to these documents.

Creating an instrument that meets the TSO requirements does not mean it is flight worthy. The next step in the process is obtaining approval to actually put the instrument in an airplane. If the instrument is an integral part of the airplane, a Type Certification (TC) is required and developed during the certification of the airplane. For replacement equipment, a Supplemental Type Certificate (STC) is required. A guide to the STC process can be found in AC 21-40.

While the TSO certifies that the instrument meets a minimum standard, it does not ensure that the unit is safe. Further, it does not ensure that the unit does not interfere with the function of the other equipment in the airplane. An STC allows the instrument to be placed in a specific airplane. It is necessary to get a certificate for *each* airplane for which the instrument is intended. The approval process for an STC is more rigorous than the TSO approval process. For companies with no history with the FAA, many regional districts strongly suggest that an STC be a part of the initial TSO certification. This allows the FAA more involvement in the design, manufacture, and installation of the product.

The FAA approval process ensures that the safety of the system is fully addressed in the design process. Failures must be determined to be extremely improbable. Further,

failures must be detected by the system so that the crew can be alerted to the malfunction and discontinue use of the instrument. The extensive built in test functionality of the AHRS500GA (see section 4.2) is designed around this intent. Crossbow's Certification Plan includes:

- Goal TSOs (TSO-C4c for Bank and Pitch Instruments, TSO-C3d for Turn and Slip Instruments and TSO-C6d for Gyroscopically Stabilized Magnetic Direction Instruments)
- STC information regarding the plane to be modified
- Safety assessment and failure analysis
- Software development assurance level determination
- Environmental considerations

From the Certification Plan, the TSO environmental, performance and display, and Crossbow's market analysis, a system specification is generated to list requirements. These requirements are then allocated to necessary sub-sections (i.e. environmental, mechanical, electronics, software, display) and they flow down through the design process. This flow-down must be well documented to enable the FAA to trace each requirement from specification to implementation.

Traceability is very important in the certification process. For example, one possible failure in the AHRS500GA (though improbable) is an accelerometer failure. A requirement to monitor accelerometer health on a continuous basis is added to the system specification. This is allocated to both software and electronics. It flows to the hardware/software interface documentation where it is specified that the current draw of the sensor will be monitored. The software requirements document specifies the monitoring shall be done on a regular basis and that the value will be compared with a nominal. If the value is outside the acceptable range, a severe error will be flagged for the user in the data packet indicating that all information from the instrument is invalid. The source code shall implement this in the acquisition of the data, the checking of the data against the window, the determination of severity and the indication in the user packet. These modules should indicate the section of the design documentation they are based upon. The design documentation references the software requirement. The software requirement references the hardware/software interface, which references the system specification.

Tracing the system requirements to implementation verifies that no additional and unsafe features are added without due consideration. Further, it provides a path to prove all intended safety features were implemented correctly. Keeping the requirements organized and traceable through the system is a matter of extreme bookkeeping.

The AHRS500GA would be difficult to certify alone. The display is an integral part of the complete system. For Crossbow, all certification paths include our display partners. The AHRS500GA provides all of the necessary information to drive indicators for each of the aforementioned TSOs. Manufacturers of glass cockpit displays are responsible for displaying the information in an FAA acceptable manner. The entire system (AHRS500GA and display) will be presented to the FAA for TSO and STC certifications.

5.1 AC 23.1309-IC

The FAA has put out an Advisory Circular addressing new technologies in the General Aviation market: *AC 23.1309-IC Equipment, Systems and Installations in Part 23 Airplanes*. It provides guidance for showing compliance with Federal Aviation Regulations Part 23.1309. These regulations specify that the system must not adversely affect other systems in any way: response, accuracy, or operation. Further, the design of the system and each of its components must be examined separately under any foreseeable operating condition. Failures that prevent continued safe flight and landing must be extremely improbable and the crew must be warned of failure. Finally, the system must be operable through other catastrophic system failures such as a partial engine loss, temporary or partial power loss.

Particularly for General Aviation, pilot error causes most accidents. The primary purpose of the Advisory Circular is to improve the safety of airplanes by fostering the incorporation of new technologies:

“Pilot error accidents, the largest single cause, often are the result of a lack of situational awareness relative to terrain or weather, or to a loss of control due to excess workload. Incorporating technologies that exceed the capability and reliability of the systems found in the current fleet.... should improve safety.” [2]

In the General Aviation, there are four classes of aircraft:

- Class I (Typically single reciprocating engines under 6,000 pounds)
- Class II (Typically multiple reciprocating and single turbine engines under 6,000 pounds),
- Class III (Typically reciprocating and turbine engines equal or over 6,000 pounds), and
- Class IV (Typically commuter category).

The Advisory Circular describes the relationship among airplane classes, probabilities of failure, severity of failure conditions and software development assurance levels.

The Advisory Circular discusses the certification basis in which the probability and severity of failure are presented. A safety assessment includes a Functional Hazard Assessment (FHA) that describes the failure

probability and severity of each component in the system. A description of various safety analysis techniques is described in the Advisory Circular. The Advisory Circular also gives a description of the electromagnetic protection necessary on the system (i.e. radiated field, lightning strike). Finally, a description of determining the software development assurance level is provided.

5.2 AC 21-40

AC 21-40 is also an Advisory Circular from the FAA, which provides an application guide for obtaining a Supplemental Type Certificate. If AC 23.1309-IC is the initial document for companies interested in certification, AC 21-40 document is a close second. It provides a certification guide, checklists and flowcharts for obtaining an STC.

The Advisory Circular discusses the data needed by the FAA for the certification process. The data documents are divided into descriptive (what the instrument should do) and substantiating (what the instrument did in verification). The descriptive data must completely describe the modification to the plane. The substantiating data must demonstrate that the modification meets the applicable regulations.

The Certification Plan is the first piece of this data. The Advisory Circular provides an outline of the Certification Plan (see section 5.3) and discusses the scheduling of project with the FAA. The level of FAA involvement depends on the applicant’s history with the FAA and the complexity of the modification to the airplane.

In obtaining an STC, an airplane must be modified and shown to the FAA to prove its compliance with the applicable regulations. The instrument is put in the aircraft, replacing the current instrument(s). Design feasibility should be discussed with an FAA engineer before an airplane is modified.

During the certification process, the FAA conducts inspections for conformity and compliance. The conformity inspections verify that the modification to the airplane conforms to the certification data while a compliance inspection verifies the modification meets the applicable regulations.

FAA Designated Engineering Representatives (DERs) can (for a price) expedite the approval process as they are authorized to approve data, witness tests, and conduct inspections. The level of DER involvement depends on the project.

5.3 Bank and Pitch Instruments (TSO-C4c)

TSO-C4c for Bank and Pitch Instruments governs the attitude indication. It directs the reader to *SAE AS 8001, Minimum Performance Standard for Bank and Pitch Instruments*. AS 8001 is short (6 pages) and it provides standards on the method of display as well as the accuracy of the unit.

Table 5-1 Bank and Pitch Instrument Requirements

Specification	Requirement
Resolution	+/- 1.25 deg
Range	360 deg
Starting time	<3 min
Bank Accuracy	+/- 2.5 degrees in 30 degree bank
Pitch Accuracy	+/- 2.5 degrees in 15 degree pitch
Turn Error	< 3 degrees in a 38 degree coordinated turn of 180 degrees for 1 minute
Loop Error	On test stand, rotate in pitch 30 deg/s through 360 degrees. No damage to unit
Roll Error	On test stand, rotate in roll 15-20 degrees per second through 360 degree bank and returned to level. Error must be <2 upon completion.
Settling Error	<1.0 degree at 30 min of simultaneous three axis oscillations of +/- 7.5 degree amplitude at 5-7 RMP.

5.4 Turn and Slip Indicator (TSO-C3d)

The turn and bank indicator is governed by TSO-C3d for Turn and Slip Instruments. It provides the reference *SAE AS 8004, Minimum Performance Standard for Turn and Slip Instruments*. However, it was written to describe a purely mechanical device and the display of the turn and slip. The derived requirements to allow a display to create a turn and slip indicator include outputting the angular rate and the lateral acceleration of the unit.

5.5 Gyroscopically Stabilized Magnetic Direction Instrument (TSO-C6d)

Finally, TSO-C6d is for a Gyroscopically Stabilized Magnetic Direction Instrument. It refers to *SAE AS 8013, Minimum Performance for Direction Instrument, Magnetic (Gyroscopically Stabilized)*. AS 8013 is also a short list of requirements.

“During dives, climbs and banks of up to at least 55 degree displacement from level attitude, the instrument shall remain functional; however, the heading error involved in the gimbal system need not be corrected.”[9]

The AHRS500GA will significantly improve on these requirements with its fully attitude compensated heading. Static error will be less than one degree. Dynamic error will generally be less than two degrees after compensation.

Table 5-2 Direction Instrument Requirements

Specification	Requirement
Range	360 degrees
Starting time	< 3 Min
Scale error	Place on magnetic headings at 30 degree intervals, starting from north, each indication shall correspond to actual magnetic heading within two degrees.
Turn Error	With system synchronized on east heading, set unit to south for one minute, return unit to east for two minutes. <2.0 degrees difference from initial reading.
Heeling Error	< 4 degrees when unit tilted +/- 10 degrees in roll or pitch
Field Strength Variation	<2 degrees when dip angle of magnetic field is changed from 72 to 80 deg at field strength of 0.57 Gauss

According to the TSO, a means must be provided for compensating hard iron error. A description of the hard iron calibration for the AHRS500GA is included in Section 4.3.

6 AHRS500GA CERTIFICATION

This section discusses the documentation required by the FAA for the AHRS500GA system. As previously mentioned, the glass cockpit display manufacturers are an integral part of the certification process.

6.1 Certification Plan

The Certification Plan is written to introduce the project the FAA and begin the process certification. While it is the formal start of the project for the FAA, it does not have to be the first contact with the FAA. Informal discussions with the local Aircraft Certification Office (ACO) should occur, especially for companies new to the certification process. AC 21-40 provides extensive information regarding the Certification Plan’s contents (outline in Figure 6-1 taken from Advisory Circular).

The project is broken into environmental concerns, software concerns, and manufacturing concerns and the means for compliance are determined for each. For all three, the basis for certification is 14 CFR part 23 (regulations for small aircraft). The environmental concerns are addressed in AC 21-16D which specifies DO-160D Environmental Conditions and Test Procedures

for Airborne Equipment as the means for compliance. The means for software compliance is in AC 20-115B which specifies DO-178B.

I. Introduction
II. System Description
III. Certification Requirements
• 14 CFR part/CAR (etc.)
• System special requirements, unique or novel aspects
• Compliance checklist
IV. Method of Compliance
• Analyses – failure, safety, performance, etc.
• Tests – qualification, flammability, laboratory, simulator, ground, flight, etc.
• Software compliance
• Design
V. Functional Hazard Assessment Summary
• System criticality
• Software criticality
• Functional failure conditions summary
VI. Operational Considerations (if required)
VII. Certification Documentation
VIII. Certification Schedule
• Descriptive data submittal
• Substantiating data submittal
• Test schedule
• Conformity inspection schedule
• Compliance inspection schedule
• Final approval
IX. Use of Designees and Identification of Individual DER/DAR

Figure 6-1 Certification Plan Outline

The AHRS500GA is a primary flight system for attitude and heading. Its loss will unquestionably have an effect on the safety of the airplane. There are multiple classifications of failure conditions described in AC1309.23-IC. The system obviously does not fall in the “no safety effect” or minor classes. The major failure includes significant reduction in the functional capabilities or safety margins of the airplane. This type of failure is associated with physical distress to passengers, possibly including injuries. The hazardous failure class is for instruments whose failure results in a large reduction in functional capabilities or safety margins. It can cause serious or fatal injuries to an occupant. The worst sort of failure is a catastrophic failure, which generally results in hull loss and multiple fatalities. Under Instrument Flight Rules, the loss of the primary attitude system has the potential to result in the loss of the aircraft. Therefore, the failure classification for the AHRS500GA will be catastrophic. A more detailed description of this decision is the Certification Plan.

The timing and schedule necessary for obtaining FAA approval varies with the complexity of the project. Inspections, meetings, tests, etc. should be planned with the FAA well in advance to assure the correct personnel are available. Since the FAA must allocate resources to the project, the schedule provided in the Certification Plan should be as accurate as possible.

The Certification Plan also provides a description of the data involved in the certification process. As the AHRS500GA is a relatively complex system involving software, an additional section addressing software concerns is necessary.

6.2 Software Aspects of Certification

In 1985, DO-178 was developed to establish software considerations for developers, installers, and users. It provides a means (not the only means) to secure FAA approval of the digital computer software. It is an intricate document that seems to provide comprehensive instructions for the software certification process. Actually, it provides a path but it is not as detailed about the actual process as it appears at first glance; it provides insight into the process but it is not a systematic cookbook.

In the software aspect of certification, it is important to show that the software lifecycle is reasonable and that the software is created using the lifecycle. Again, traceability of requirements is a theme in certifying software: from the system level to the actual implemented source code and the verification test for it. The first piece of the puzzle is the Plan for Software Aspects of Certification (PSAC). It describes all of the concepts and methodologies that Crossbow employs to produce reliable software per DO-178B guidelines. In the document, consideration is given to all aspects of software production: planning, design, verification, management and quality control. Further, the PSAC sets up a road map to the entire set of software data for certification.

6.2.1 Software Criticality

Software development assurance level or software criticality is based upon the contribution of software to potential failure conditions as determined by the system safety assessment process. The software level implies that the level of effort required to show compliance with certification requirements varies with the failure condition category. The software level definitions are in line with the classification of failure conditions. Malfunction of level A software would result in a catastrophic failure condition for the airplane. Level E software would have no effect on aircraft operational capability or pilot workload.

As the AHRS500GA provides attitude and heading information, safety assessment would indicate that anomalous behavior of the AHRS500GA would cause or contribute to a catastrophic condition for the aircraft. Typically, the software would be designed, verified, and validated using DO-178B Level A guidelines. However, AC 23.1309 provides some relief from this level to improve the safety of airplanes by fostering the

incorporation of new technologies. Thus, the FAA allows the software assurance level to be reduced to Level B guidelines.

Level A certification has extremely stringent verification requirements, including complete path analysis in the executable. The difference is between white box testing for level A and black box testing for level B. Further, certification to level A requires more independence between design and verification than level B does.

6.2.2 Software Lifecycle: Planning

Before the software development efforts can take place, standards must be in place to control the generation of said software. Once these standards are in place, all software generated by Crossbow will adhere to the guidelines set forth in such documents. All software for the AHR500GA will be developed following the DO-178B guidelines. The Software Development Standards (SDS) document serves as the central guideline for directing and managing all software development efforts. The SDS addresses the three main areas of software development as defined by DO-178B. These are software requirements, design, and coding standards. The standards have been incorporated as different sections in a single document.

The planning phase offers the first opportunity to derive the overall strategies that will be employed throughout the software life cycle. The main areas of concentration are certification considerations, software development, verification, configuration management, and quality assurance. The outputs of the planning phase are several items that are described below. These data items are then provided to all involved in the development effort. The pertinent certification authorities may use these plans to get early visibility of the planned development effort. This serves two purposes: to offer complete understanding of the project and to acquaint the Certification Authority with the AHR500GA software system.

- The PSAC lays out the overall strategy for software development. Its focus is on certification issues for obtaining early feedback from the Certification Authority.
- The Software Development Plan (SDP) lays out the strategy of how the actual software is to be designed, coded, debugged, and verified.
- The Software Configuration Management Plan (SCMP) outlines the procedure used to manage and control software product identification, and storage methods. It also delineates how problems are to be reported and handled.
- The Software Quality Assurance Plan (SQAP) discusses how transitions between life cycle processes are to be made. Validation methods

are discussed and, in general, all quality assurance functions (as they relate to software) are described in this document.

- The Software Verification Plan (SVP) covers methods that will be utilized to verify correctness of the software product. Both high- and low-level requirements are discussed.

While these plans are focused toward the AHR500GA project, they are based on general processes used for every Crossbow product.

6.2.3 Software Lifecycle: Development

After the planning process is complete and the initial product requirements have been captured in the system specification, overall software system design and development begins. The development plan (SDP) governs this portion of the lifecycle.

High-level requirements are developed and partitioned into hardware and software. The software requirements are captured in the Software Requirements Document (SRD).

Top-level software design commences based on the requirements set forth in the SRD. A Preliminary Design Review (PDR) is held to verify that the initial designs adhere to the original system requirements. After the successful completion of the PDR, designs are firmed up and the implementation phase begins. The software architecture and low-level requirements are developed and captured in the Software Design Data (SDD).

Next, source code is developed that is traceable, verifiable, and consistent, which correctly implements architecture and low-level requirements. A prototype hardware and software integrated system is constructed. The resulting system is presented at the Critical Design Review (CDR) to verify that the original requirements were met. Note that the CDR is the last chance to change the direction of the design effort before final designs are completed. After the successful completion of the CDR, final design and integration stages are completed, while verification efforts continue.

6.2.4 Software Lifecycle: Verification

The goal of verification is to detect and report errors (in requirements, design, code, and/or documentation) that may have been introduced during the software development processes. It begins upon completion of the software planning process and occurs in parallel with the development process. While the types of verification activities are provided in the verification plan (SVP), the particular AHR500GA verification activities are provided in the Software Verification Cases and Procedures (SVCP). The test cases and procedures in the

SVCP are traceable to the requirements in the design document (SDD), which are traceable to the requirements document (SRD).

The verification activities include review and analysis of high- and low-level requirements, software architecture, source code, integration process outputs, test cases and procedures. The verification activities also include executing the test cases on the software to test all features. The results these activities are captured in the Software Verification Results (SVR), which are generally a set of completed forms from the SVP or SVCP.

6.2.5 Software Lifecycle: Configuration Management

Management of the software development effort is necessary to provide the desired level of traceability and reproducibility. Proper storage and retrieval for the software and reliable problem reporting are also important configuration management functions. The Software Configuration Management Plan (SCMP) provides the details on the implementation of configuration identification, change control, baseline establishment, and archiving of the software product. A standard version control system provides the necessary tools to do this.

A Software Environment Configuration Index (SECI) provides the build and verification environments. It also specifies computers, compilers and all of the tools necessary for the software lifecycle.

The Software Configuration Index (SCI) lists the source code components with its version information, storage mechanism and instructions for regeneration. It also lists the software lifecycle data and version information for the released software version. Problem reports are used to track issues determined by the verification and quality assurance processes.

Finally, the Software Configuration Management Records will show change history, release records, configuration lists. They can be generated directly from the version control system.

6.2.6 Software Lifecycle: Quality Assurance

The software quality assurance (SQA) process ensures that software development and integral processes comply with approved software plans and standards; that transition criteria for life cycle processes are satisfied; and that a conformity review of the software product is conducted. The process occurs in parallel with the other process and the output is a series of SQA records that show the software lifecycle was followed.

6.2.7 Software Lifecycle: Certification Liaison

The purpose of putting certification liaison as a process in the software lifecycle is to establish communication and understanding between the applicant and the Certification Authority throughout the software life cycle to assist the certification process. The Software Accomplishment Summary (SAS) is part of this process. It shows that the project was completed in compliance with the PSAC.

6.3 Plan for Hardware Aspects of Certification

With the understanding that modern electronics can be just as complex as software, the FAA has begun to implement controls in this area as well. DO-254 is a new document used by some local offices. It provides a means for compliance regarding hardware design, implementation and verification process. Largely, it parallels DO-178B for the software process.

6.4 Environmental Requirements

The AHRS500GA and internal magnetometer shall meet the appropriate environmental requirements. These requirements are taken from the TSOs and DO-160D. In all cases, DO-160D is the primary source for the environmental requirements.

The AHRS500GA must meet the aforementioned performance specifications after being subjected to the environmental conditions specified by the TSOs. A partial list of requirements is provided in Table 6-1. In cases where the applicable class is not clear from the TSO, the more stringent requirement shall apply.

Table 6-1 Environmental Requirements

Requirement	DO160D Cat	AHRS500GA-101 Specification
Operating Low Temperature	C4	-40°C
Operating High Temperature	C2	+70°C
Altitude	C4	35,000 feet, ambient temperature
Decompression	C4	8000 feet stabilize. Decompress to 35,000 feet in 15 sec.
Temperature Variation	B	5°C/minute rate, from low operating temperature to high operating temperature
Operational Shock	B	Shock: 6g, 11ms, 3 saw-tooth wave shocks in each of 6 axes.

Requirement	DO160D Cat	AHRS500GA-101 Specification
Standard Vibration	S	Curve M. 1.5 g peak sine, sweep 5 to 500 Hz for 1 hour each axis
Vibration		Roll and pitch angle shall change less than $< 1.0^\circ$ While operating through Category S, Sine Vibration M, 1.0 hr. each axis.
Fungus	F	Show by material composition that it does not promote growth
Normal Operating Voltage	B and Z	30.3Vmax, 11V min; 9V emergency
Voltage Spike Conducted	A	A = 600v @ 10usec 50 transients of each polarity within 1minute
Electric Field Induced on Cables	C	5400V-m from 380Hz to 420Hz to 135 V-m at 15 kHz ramp.
Lightning Induced Transient Susceptibility-Pin	A	A3XX Pin Test – 600V @ 24A and 300 V @ 60A

6.5 Manufacturing

Certification of manufacturing facilities is beyond the scope of this paper. It is a monumental task covered by 14 CFR part 23 and FAA Order 8100.7A. The appendices of that document provide an in depth checklist used by FAA representatives during audits.

7 CURRENT STAGES

The AHRS500GA proof of concept system was designed with certification in mind. It is reliable and robust as well as accurate (see Section 4.5 AHRS500GA Performance Results). It is in the process of design verification testing. Crossbow is concentrating on completing the certification data necessary to share with our display partners. Display partners are verifying that the initial requirements have been met with the proof of concept system.

Crossbow has started a dialog with the FAA through the LA ACO and through DERs. As a new applicant with a critical flight system, the FAA will be extensively involved in the design and verification of the AHRS500GA.

8 REFERENCES

Note: Many of these documents are available via the FAA website (www.faa.gov).

1. *Software Considerations in Airborne Systems and Equipment Certification*, RTCA/DO-178B, December 1, 1992.
2. *FAA Advisory Circular Equipment, Systems, and Installations in Part 23 Airplanes* AC 23.1309-IC
3. *AS8001 - Minimum Performance Standard for Bank & Pitch Instruments*, Published by SAE International, September 1975, Reaffirmed - May 1991
4. *AS8013 Minimum Performance Standard for Direction Instrument, Magnetic (Gyroscopically Stabilized)*, Published by SAE International, June 1983, Revised - September 1996
5. *AS8004 Minimum Performance Standard for Turn and Slip Instruments*, Published by SAE International, September 1975, Revised - October 1984
6. *Environmental Conditions and Test Procedures for Airborne Equipment*, RTCA/DO-160D, 1997
7. TSO-C4c - Bank and Pitch Instruments
8. TSO-C3d - Turn and Slip Instrument
9. TSO-C6d - Direction Instrument, Magnetic (Gyroscopically Stabilized)
10. *FAA Advisory Circular Radio Technical Commission for Aeronautics, Inc.* Document AC 20-115B.
11. 14 CFR part 23: Title 14 of the Code of Federal Regulations, Airworthiness Standards: Small Airplanes.
12. *Application Guide For Obtaining A Supplemental Type Certificate*. AC 21-40.