Federal Aviation Administration

--

FAA HMI Analysis and Integrity Risk Compliance Arguments (IRCA)

Presented to: CAAC

By: John Warburton
Navigation Team Manager
FAA Engineering Development Services

Date/Place: October 21 2010
Atlantic City, NJ

Overview

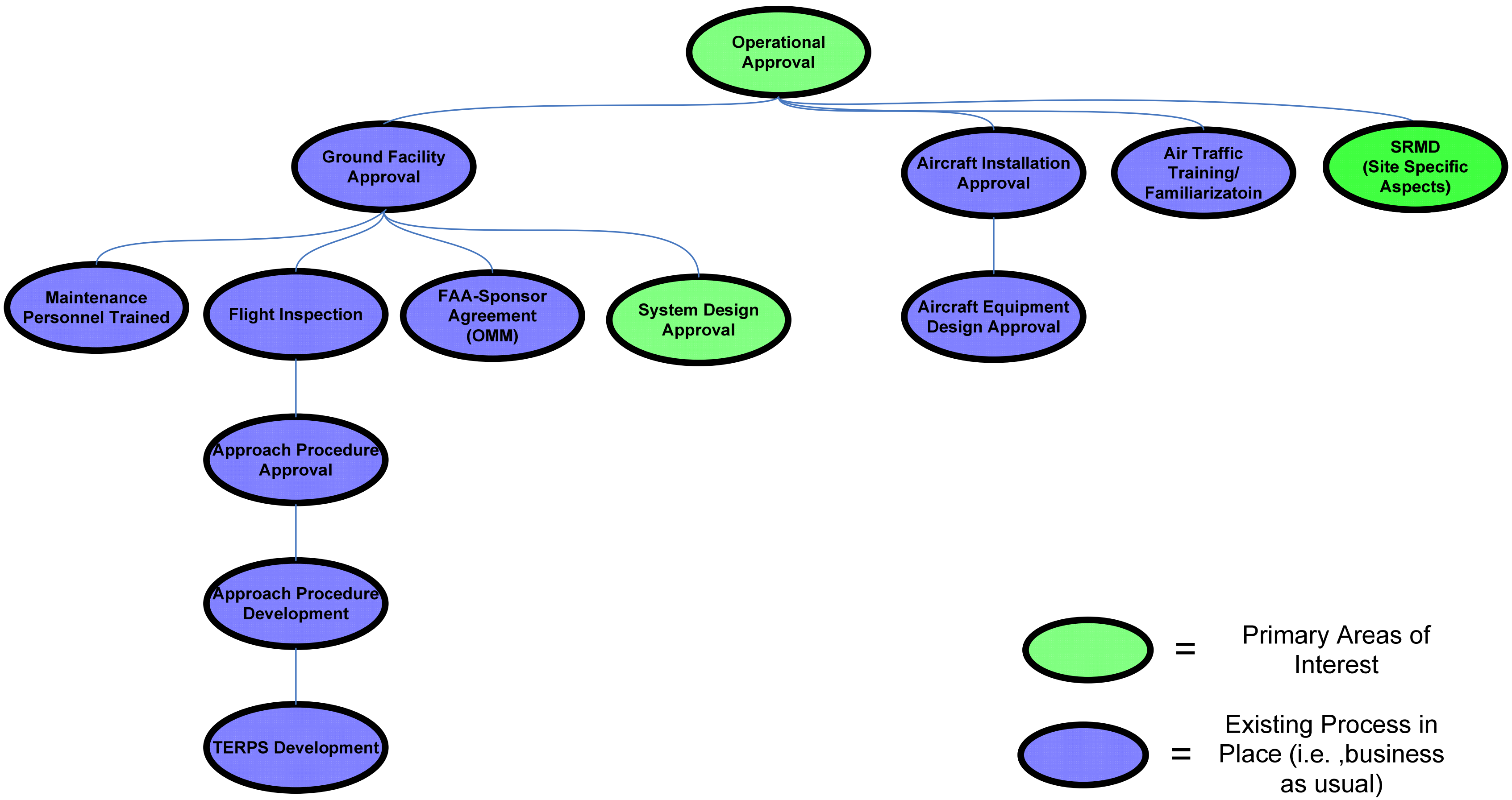
- **HMI Report Definition**
- **Operational Approval Strategy**
- **HMI Report Format**
- **Selected IRCA Examples**
- **Summary**

- **Backup Slides**
  - IRCA Examples

Hazardously Misleading Information (HMI) Report

- **An HMI report details the process and assumptions that demonstrate a system is safe.**
  - A similar process was effective in verifying FAA Wide Area Augmentation System (WAAS) integrity
  - HMI report is a detailed summary of the integrity work
  - Tool used to help the technical team communicate with the certification authority
- **The core of the HMI report is a series of statements that, when taken together and are shown to be true, completely define the integrity safety case**
  - Called the Integrity Risk Compliance Argument (IRCA)
- **The HMI report contains the IRCA list as well as a summary of the ADD material for each IRCA statement**

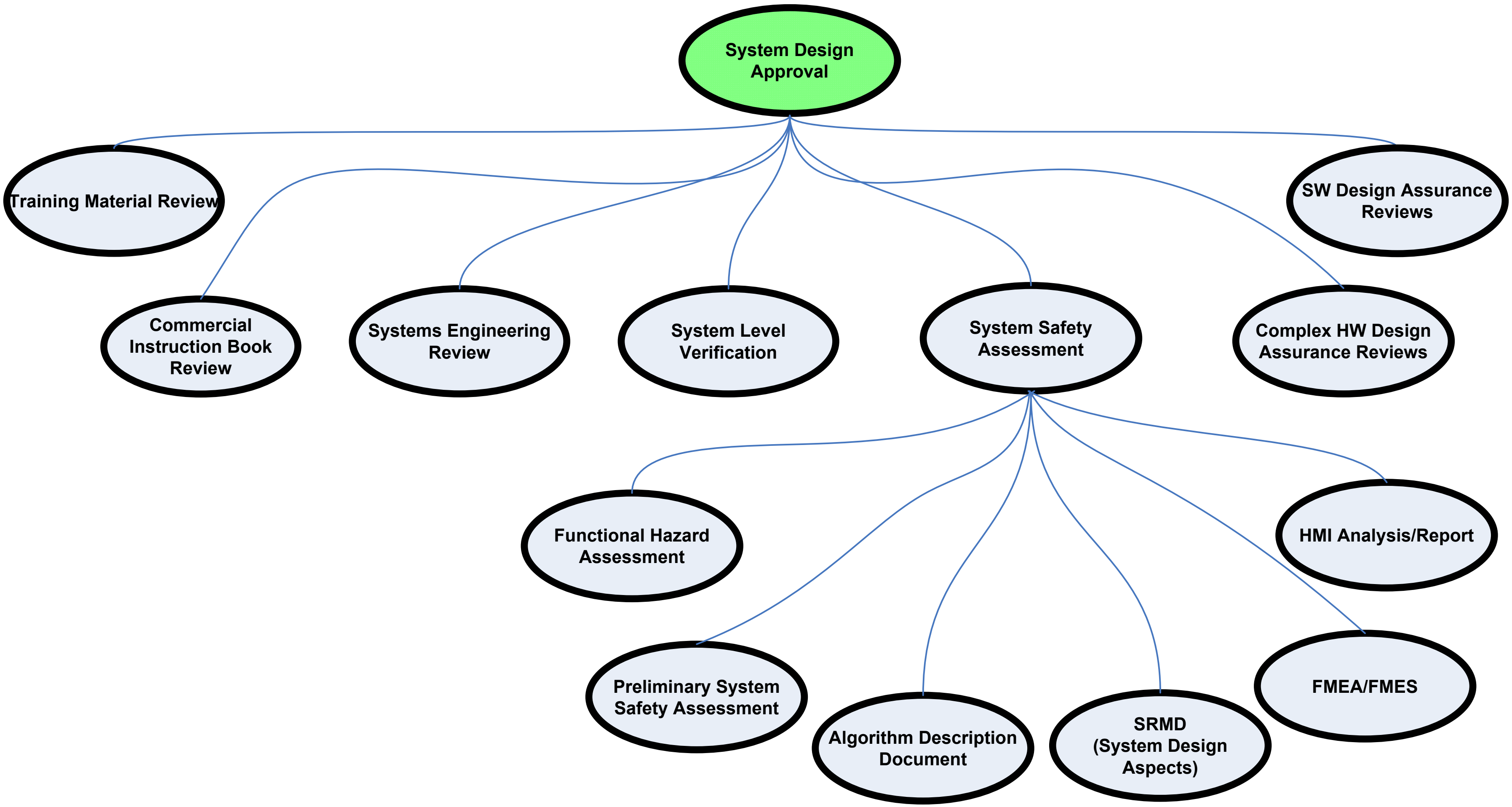
Operational Approval Strategy



Operational Approval Primary Components

- **Ground Facility Approval**
  - Ground equipment design meet safety & performance requirements (a.k.a., System Design Approval)
  - Approach procedures are developed and flight inspected
  - Maintainers are trained
  - Operations & Maintenance agreements are in place between the ground facility sponsor and the FAA
- **Site Specific Safety Risk Management Document**
  - Address any site specific risks and mitigations that were not addressed during the SDA review (i.e., during the development of the development of the SRMD for the equipment design).
  - To be developed by the Service Area Safety Assurance Group
- **Aircraft equipment and installation approval**
  - Review/approve the applicable aircraft equipment and installation (e.g., TSO, STCs, etc.)
- **Air Traffic Training/Familiarization**
  - Ensure that new procedures are briefed to the AT crews, new phraseology understood, etc.

System Design Approval Strategy



HMI Report Sections and Status

Section	Title	Pages	Key Risk Area	Status
1	Introduction	25	N/A	Complete
2	Fault trees	9	Overall Risk Compliance	Complete
3	Common Methods	10	Timelines, TTA, Bound descriptions	Complete
4	Data and Tools	1	Techniques and Programs	Complete
5.0	Fault-Free Integrity	1	Nominal Error Bounding	Complete
5.1	Sigma PR ground	79	Protection Level Bounding	Complete
5.2	Nominal troposphere	15	Tropospheric Error bounding	Complete
5.3	Nominal ionosphere	9	Ionospheric Error Bounding	Complete
5.4	Range to Position	8	Position Domain Bounding	Complete
6.0, 6.1	H1 integrity	12	Single Receiver Faults	Complete

HMI Report Sections and Status

Section	Title	Pages	Key Risk Area	Status
7.1	Signal Deformation Monitor	86	Satellite Signal Deformation Faults	Complete
7.2	CCD	11	Satellite Code Carrier Divergence	Complete
7.3	Low Power	12	Satellite Low Power Faults	Complete
7.4	Excessive Acceleration	9	Satellite Excessive Acceleration Faults	Complete
7.5	Ephemeris	51	Ephemeris B, A1 and A2 Faults	Complete
8.1	Sigma Monitor	20	Environmental Changes	Complete
8.2	Dual RR	18	Simultaneous Faults on Two References	Complete
8.3	Dual RS	25	Simultaneous Faults on Two Satellites	Complete

HMI Report Sections and Status

Section	Title	Pages	Key Risk Area	Status
8.4	Anomalous Ionosphere Error Bounding	56	User Protection (Limits on the Total User Error) During Anomalous Ionospheric Conditions	Complete
8.5	Anomalous Troposphere Error Bounding	11	User Protection (Limits on the total user error) During Anomalous Tropospheric Condition	Complete
9.0	Miscellaneous Sections	1	Additional Operating Conditions, Requirements, or Uplink Parameters	Complete
9.1	RFI	17	Integrity During Radio Frequency Interference	Complete
9.2	Uplink Parameters	11	Setting for All Uplink Parameters	Complete
9.3	Autoland	3	Use of the CAT I System for Practice Autoland Operations	Complete
10, 11	References, Acronyms	4	N/A	Complete

Integrity Risk Compliance Arguments (IRCA) Examples

- **IRCA Examples are provided in backup slides**
  - Two are repeated next
- **Motivation: To provide insight into the high-level statements that lead into the full compliance argument**
  - Threat and mitigation method summary
  - Mitigation details are design specific

HMI Report IRCA Contents

- **All sections of each IRCA compiled for the HMI report will conform to the following:**

  X.X.1 Threat Discussions (high level)
  X.X.2 Algorithm Description (high level)
  X.X.3 Integrity Risk Compliance Argument (assertions, etc.)
  X.X.3.1 Threat or Threat Model
  X.X.3.2 Method (Higher-level method techniques)
  X.X.3.3 Models / Methods (details of implementation)
  X.X.4 Justification of All X.3.3 Sections
  Detailed Algorithm
  Analyzed Data
  Validation
  X.X.5 Dependencies
  X.X.6 Conservative Methods
  X.X.7 Data Sets (locations and quantity of days….)
  X.X.8 Conclusions

IRCA Examples
Nominal Ionosphere Integrity 5.3 Threat

- **The treatment of the residual ionosphere errors in the MOPS protection level equations is appropriate.**
  - Nominal ionosphere delays observed by the LGF are sufficiently similar to delays observed by LAAS users that residual ionosphere errors can be bounded by a single added term in the H0 and H1 protection level equations.
  - The residual ionosphere delay difference between LGF and user can be modeled as growing linearly with effective LGF-to-user separation. Thus, the value σ_{vig} of broadcast by the LGF will have units of m/m (expressed as mm/km for ease of use in this report).
  - The residual error in the nominal ionospheric spatial gradient can be bounded by a zero-mean Gaussian distribution with a fixed standard deviation.
  - The resulting nominal ionosphere error contribution to the H0 and H1 protection level equations is sufficiently statistically independent from other error sources that it can be “RSSed” into the other error sigmas making up the total range error sigma in VPLH0.

IRCA Examples
Nominal Ionosphere Integrity 5.3 Method

- **The method is to determine broadcast parameter values for any local region in the CONUS so that they never have to be updated.**
  - The broadcast value determined, along with other nominal error descriptions, is verified to be acceptable by historical data analysis and other appropriate methods.
  - A measure of adequately in calculating the parameters which characterize the ionosphere error model is demonstrated.

IRCA Examples
Code Carrier Divergence Faults 7.2 Threat

- **Faulty satellites can transmit signals with a constant rate of code-carrier divergence.**
  - Nominal variations in satellite CCD divergence are covered by the broadcast σ_{pr_gnd}.
  - Two effects on the corrected pseudorange.
  - The aircraft and ground filters may have different start-up methods (time variant, time-invariant, faster/slower sample times), causing a difference between the ground and aircraft filter transient responses.
  - The aircraft and ground filters may start at different time for the anomalous satellite, causing a difference between the ground and aircraft filter transient responses.

IRCA Examples
Code Carrier Divergence Faults 7.2 Method

- **The general method is to implement a real-time monitor in the ground facility to detect the satellite CCD fault.**
  - The CCD divergence rate can be estimated from the ground reference receiver measurements by calculating the difference between the code and carrier measurements.
  - In the presence of CCD, divergence rate estimates with raw measurements will be different than rate estimates calculated with the smoothed measurements
  - A simple threshold test can detect SV faulted CCD within 1.5 seconds.
  - The nominal ionospheric divergence rate in the region of ground facility service must be accounted for in setting the monitor threshold.
  - The standard deviation of ranging error on a CCD-faulted satellite is the same as the fault free case.

IRCA Examples
Excessive Acceleration 7.4 Threat

- **Excessive Acceleration Integrity Threat**
  - Faulty satellites can transmit signals with a constant rate acceleration in both the code and carrier.
  - Nominal accelerations are covered by the broadcast σ_{pr_gnd}
  - The error in the differentially-corrected pseudorange due to excessive acceleration is given by $E = 0.5at(t+DT)$ where a is the acceleration, t is the latency and DT is the differential correction update interval.

IRCA Examples
Excessive Acceleration 7.4 Method

- **The general method is to implement a real-time monitor in the ground facility to detect the excessive acceleration fault.**
  - The acceleration on a pseudorange can be estimated from the ground reference receiver measurements by calculating the difference between successive smoothed, clock adjusted pseudorange corrections.
  - In the presence of excessive acceleration, the calculated estimate will deviate from the nominal performance
  - A simple threshold test can detect faulted acceleration within the allocation
    - The nominal acceleration rate of the ground facility equipment must be accounted for in setting the monitor threshold.
    - The standard deviation of ranging error on an EA-faulted satellite is the same as the fault free case.

IRCA Examples
Nominal Troposphere Integrity 5.2 Threat

- **The threat is that the broadcast nominal tropospheric parameters do not adequately describe the nominal troposphere delay and variation. The effect on integrity for the nominal residual troposphere is through the appropriate H0 and H1 protection level bounding. If the nominal parameters are set incorrectly, the resulting integrity risk could be higher than anticipated.**
  - This could occur by not determining the parameters correctly.
  - This could occur by not updating the parameters as often as necessary to protect specific integrity risk
- **The treatment of the residual troposphere errors in the MOPS protection level equations is appropriate.**
  - Nominal troposphere delays observed by the LGF are sufficiently similar to delays observed by LAAS users that residual troposphere errors can be bounded by a single added term in the PL equations.
  - The residual troposphere delay difference between LGF and user can be modeled with the altitude function expressed in the MOPS.
  - The residual error in the nominal troposphere can be bounded by a zero-mean Gaussian distribution with a fixed standard deviation calculated by the expression in the MOPS.
  - The resulting nominal troposphere error contribution to protection levels is sufficiently statistically independent from other error sources that it can be combined in accordance with the MOPS into the other error protection level error estimates making up the total range error sigma in the protection level equations.

IRCA Examples
Nominal Troposphere Integrity 5.2 Method

- **The method is to determine broadcast parameter values for the local region so that they never have to be updated.**
  - The broadcast values determined, along with other nominal error descriptions, are verified to be acceptable
  - Some measure of adequately calculating the parameters which characterize the troposphere error model.
  - Sensitivity of correction to changes in parameters of error model
  - Done once during this PHMI analysis. It is used to generate the requirements and method for the site-specific installation analyses.
  - Sensitivity of σ_{tropo} to changes in parameters of error model
  - Accuracy (appropriateness) of correction and uncertainty
- **The installation manual will describe how to calculate parameters and enter into ground facility**

IRCA Examples
Fault Free Integrity Sigma Ground 5.1 Threat

- **The pseudorange corrections broadcast by the LGF contain non-differential errors (measurement, site-specific, uncertainty) that will produce errors in the user navigation solution and must be bounded by one of the protection level equations.**
  - The fault-free protection level, H0, is covered in this section.
  - The fault-free protection level equation uses several integrity parameters, only σ_{pr_gnd} is discussed in this section
  - The airborne error contribution estimate, σ_{pr_air}, is assumed to be an overbounding sigma of the airborne multipath and airborne receiver noise defined in the MOPs.
    - The single-receiver fault protection level is covered in section 6.1
    - The ephemeris protection level equation is covered in section 8.4

IRCA Examples
Fault Free Integrity Sigma Ground 5.1 Method

- **The true distribution of errors in the differential corrections can be characterized by a zero-mean, normal distribution with a standard deviation equal to broadcast σ_{pr_gnd}.**
  - Error distributions for any broadcast σ_{pr_gnd} component were estimated from data or "first principles" or otherwise modeled.
  - Any dependency of error as a function of satellite position has been identified.
  - Any time-varying characteristics have been identified.
  - Any correlation between satellites or measurements across reference receivers has been identified.
  - Any characteristics assumed or requirements levied on the installation process have been identified including site specific parameters quantification.

IRCA Examples
Signal Deformation Faults 7.1 Threat

- ***The transmitted satellite signals can have signal deformation such that the differential corrections will have errors for some set of users***
  - ICAO defined the threat model details for deformations when the satellite has a failure.
    - The "natural" correlation peak distortion results from the nominal signal deformation of a non-faulted satellite will be bounded by s_{PR_gnd} as described in section 5.1 and reflected in the monitor detection analysis.
    - The natural correlation peak distortion, and the resulting discriminator and measurement output and resulting error, can be re-created using an ICAO threat model signal deformation
  - There are four failure cases.
    - SV fails while out-of-view of LGF and rises with fault already present
    - SV fails while in view of LGF
    - A new SV is launched with failure already present
    - Satellite set unhealthy and reset to healthy after maintenance action for a clock change or other redundant equipment swap (concern: natural bias value may have changed)
  - Fault onset occurs as an instantaneous step or as a gradual increase in the signal deformation
    - Faults of concern are those that result in measurement errors that can not be characterized by the broadcast σ_{pr_gnd}. User receiver design space is limited by MOPS
    - Nominal behavior is defined to all behavior where the natural biases resulting from signal deformation remain within a bound, i.e., the difference between the minimum natural bias and the maximum natural bias remains less then some determined acceptable level.
  - The probability of a SD satellite failure occurring and causing a simultaneous user-smoothing filter reset while the LGF receiver filters do not reset is negligible

IRCA Examples
Signal Deformation Faults 7.1 Method

- ***The method is to monitor signal deformation and cease broadcast of satellites that have signal deformation beyond the acceptable level.***
  - Real-time monitoring
    - The ground facility can estimate signal deformation using a combination of its correlation peak measurements and detect instantaneous changes in the correlation peak.
    - Show that errors induced by the non-natural bias portion of the ICAO threat model can be detected with the required probability of missed detection within the TTA.
    - A simple threshold test can detect faulted signal deformation within the threat model within 1.5 seconds.
    - The standard deviation of test statistic on an SDM-faulted satellite is the same as the fault free case.
    - The natural correlation peak distortion must be accounted for in setting the monitor threshold.
  - Satellite initialization
    - The natural bias of any satellite must be determined and verified to fit within the σ_{pr_gnd} allocation for SDM.
    - Any new satellite's bias must be verified to be below the allocation before being broadcast in the uplink.

Summary

- **SLS-4000 HMI report has been completed**
  - Was submitted as part of the overall System Design Approval (SDA) package.
- **FAA completed SDA process with HI**
- **HMI IRCA high-level threats and monitor examples were provided to give insight into the integrity proofs**

Questions

IRCA Examples
Range to Position Domain Integrity 5.4

- **The MOPs defined combination of all determined integrity values is an appropriate bound of the user position error for any user.**
  - The broadcast σ_{pr_gnd}, σ_{vig}, σ_{tropo}, and the broadcast CAT I probability multipliers are appropriate for any user.
  - The airborne sigma is a combination of a defined airborne multipath allocation and the airborne receiver noise.
  - For the purposes of ground analysis, the airborne noise portion will be set to zero.
- **Method: Multiple combinations possible**

IRCA Examples
Faulted Integrity and B-Value Monitor 6.1

- **Threat: The threat is that the H_1 protection level equation will not provide bounding.**
  - B-values are not representative of the true error difference among the reference receivers and do not provide bounding in accordance with the MOPS. *(when the B values are small but should be large because of correlated multipath for example)*
  - The broadcast σ_{pr_gnd}, (potentially inflated for use in the H_0 equation), is not appropriate for use in the H_1 equation and does not provide bounding in accordance with the MOPS.
- **Method: Broadcast H1 parameters are accurate and computed in accordance with the specification**
  - B-values are calculated in accordance with the specification.
  - Siting document mitigates correlation among measurements.
  - The broadcast σ_{pr_gnd}, when calculated for H_0, is appropriate for H_1.

IRCA Examples
Low Power Faults 7.3

- **Satellite signal levels below those specified in Sections 3.3.1.6 and 6.3.1 of ICD-GPS-200C for C/A code L1 condition does not automatically cause misleading information for either precision approach or DCPS users.**
  - The low signal power threat during satellite acquisition has no impact on integrity or continuity
  - Carrier cycle slips due to low received satellite signal power do not pose an integrity threat if measurements with Carrier-to-Noise Ratios above the minimum tracking capability of the receiver are used.
  - Carrier phase and code phase noise due to low received satellite signal power do not pose an integrity threat
  - Code phase cross correlation due to low relative received satellite signal power does not pose an integrity threat unless certain conditions exist.
- **The method is to implement a real-time monitor in the ground facility to detect low received power levels and low relative power levels.**
  - Low received power is detected by verifying that the received signal to noise ratio is above a threshold that can be effectively tracked by the reference receiver.
  - All monitors are designed to operate at this threshold.
  - Code phase cross correlation due to low relative received satellite signal power does not pose an integrity threat unless certain conditions exist. These conditions can be excluded with simple tests.

IRCA Examples
Excessive Acceleration 7.4

- **Excessive Acceleration Integrity Threat**
  - Faulty satellites can transmit signals with a constant rate acceleration in both the code and carrier.
  - Nominal accelerations are covered by the broadcast σpr_gnd
  - The error in the differentially-corrected pseudorange due to excessive acceleration is given by $E = 0.5at(t+DT)$ where a is the acceleration, t is the latency and DT is the differential correction update interval.
- **The general method is to implement a real-time monitor in the ground facility to detect the excessive acceleration fault.**
  - The acceleration on a pseudorange can be estimated from the ground reference receiver measurements by calculating the difference between successive smoothed, clock adjusted pseudorange corrections.
  - In the presence of excessive acceleration, …how the test statistic reacts
  - A simple threshold test can detect faulted acceleration within the allocation
    - The nominal acceleration rate of the ground facility equipment must be accounted for in setting the monitor threshold.
    - The standard deviation of ranging error on an EA-faulted satellite is the same as the fault free case.

IRCA Examples Sigma Faults 8.1

- **The threat is that the broadcast σ_{pr_gnd} no longer reflects the actual error distribution present within the broadcast corrections. Error level increases, associated with external effects in the installation environment beyond what is protected by the broadcast σ_{pr_gnd}, must be detected so that protection level bounding is maintained. External threats mitigated are:**
  - Changes in the environment due to construction which was unanticipated by the siting criteria limitations.
  - Changes in environment due to weather.
  - Undetected error in the broadcast σ_{pr_gnd} established during installation. Changes in the environment which affect single references receivers
  - Changes in the satellite orbits which affect single references receivers
  - Changes in the procedures regarding surface vehicles and taxiing airplanes are mitigated by following the siting criteria clear areas.
- **The method to ensure that the broadcast σ_{pr_gnd} is valid is to use monitors to ensure that the broadcast σ_{pr_gnd} is within acceptable limits of the baseline sigma established at installation.**

IRCA Examples
Dual Reference Receiver Faults 8.2

- **Receivers which have common failure modes or those that are exposed to the same error sources could potentially have the same errors.**
  - The common error will not be reduced by averaging or identified in the b-value tests
  - Occurrences of erroneous data due to HW faults are independent from reference receiver to reference receiver
  - Occurrences of erroneous data due to excessive multipath are independent from reference receiver to reference receiver
  - Occurrences of erroneous data due to a hardware fault are independent from occurrences of erroneous data due to excessive multipath
- **The potential for common mode errors will be mitigated**
  - Common mode software errors will be prevented by executing a safety-assured software design program.
  - Common mode hardware errors are prevented by executing a safety-assured hardware design program.
  - Common mode errors at each reference receiver will be mitigated by siting and installation practices
  - Common mode specular multipath caused by objects will be mitigated by applying the design LAAS Obstacle Consideration Area (LOCA) at each reference location
  - At locations where the LOCA contains an object and masking is required, no references will have common masks.
  - Common mode specular multipath caused by the ground will be mitigated by varying the installation height of references where the ground where the antennas are to be installed in within x ft.

IRCA Examples
Dual Ranging Source Faults 8.3

- **The dual fault threat addresses the probability that two ranging sources to have failed within the applicable operational period.**
  - The dual fault analysis demonstrates that the probably of a dual fault is remote, and fits within the allocation in the fault tree.
    - Integrity Risk Compliance Argument
      - *Threat: Two ranging sources will be failed at the same time*
        - » There are five ranging source fault modes, four that are relevant for dual faults
        - » Code Carrier Divergence
        - » Excessive Acceleration
        - » Signal Deformation
        - » Low Power – The integrity threat is conditional on low power occurring and associated cross correlation between satellites. Therefore there is no direct integrity threat due to low power, and is not an issue for dual faults
        - » Erroneous Ephemeris – There are protection levels (ephemeris bound) on each ranging source, so there are independent tests on each ranging source. Therefore dual faults are not an issue.
        - » Ephemeris should be added into the relevant faults since in the PLe equations, there is a fault free portion of other failure modes.
        - » The first fault can occur on any of 18 satellites
        - » The second fault can occur on any of 18-1 = 17 satellites

IRCA Examples

Anomalous Ionospheric Integrity Compliance Faults 8.4

- **The aircraft may experience a differential ionosphere error that is not bounded by the protection level equations in the event of a large ionosphere disturbance. Position errors greater than the alert limit are possible and have been observed.**
  - The state-of-the-art physics modeling of the ionosphere is either too complex or insufficient to characterize the propagation errors in GPS signals through a disturbed or anomalous ionosphere (non-normal) environment. As such, observations of these errors must be used to formulate a model.
  - For the purposes of aircraft approach and terminal area operations, all observed threats can be acceptably modeled for impacts by a linear front characterized by speed, width, and gradient.
  - CONUS observations compiled to date are sufficient to model the errors that would have occurred with GBAS within the CONUS over the period of compiled observations.
  - The mitigation approach and analysis provided herein are not necessarily applicable to ground equipment installed outside CONUS. A separate approval would be required.
  - Variations in ionosphere activity occur both within and between solar cycles. Limited observations are available for modeling.
  - Continued observation of the ionosphere is required and can be accomplished in conjunction with implementing early systems.
    - The service provider responsibility is to perform this continued observation and identify any required threat model changes.
    - Observations in operationally relevant configurations (that is, shorter baselines) are required and can be obtained in conjunction with implementing early systems.
    - The service provider responsibility is to perform this continued observation and identify any required threat model changes.
    - The ground system design must have the demonstrated capability to support the service provider by having the capability to adapt/tune monitoring/screening parameters in response to an updated threat model.
  - Limited observations are available for modeling the short baselines applicable to the aircraft and ground station.

IRCA Examples
Anomalous Ionospheric Integrity Compliance Faults 8.4

- The ground system design and/or analysis will mitigate the risk posed by all threats in the ionosphere threat model.
- The FAA will agree to a difference with the Annex 10 standards in assessing the acceptable risk. The standard integrity methodology (that is, SIS protection level bounding and the aircraft application of standard alert limits) does not need to be applied in the design of monitoring for or the analysis of ionosphere anomalies. However, safety in any one approach for a minimum user must be determined to be acceptable or that user's approach must be denied by action of the ground facility in concert with a MOPS-compliant user with no special capabilities.
  - A "safety case" (defined herein as an argument that demonstrates an equivalent level of safety through alternate means) must be prepared for and agreed to by the FAA prior to ground system design approval. This section documents this argument and constitutes the "safety case".
  - Use of this methodology in states other than the US will require a similar commitment by the governing state.
- A particular ionosphere front in the model (or point in the threat space) may cause significant error for one user while contributing negligible or no errors for other users. In all cases, the errors experienced depend on the runway and procedure orientation relative to the ionosphere front, the ground and aircraft position relative to the front, and the current ground-aircraft-satellite geometry. Different airports may experience different ionosphere fronts (during the same active ionosphere period), no abnormal ionosphere disturbance at all, or delayed activity. Some airports may be more prone to experience active periods due to their location relative to the geomagnetic equator.
- Every affected user must be accounted for in the "safety case" and each such user's approach demonstrated to be safe.

IRCA Examples

Anomalous Ionospheric Integrity Compliance Faults 8.4

- The perspective of safety for a single airport's operations must be accounted for in the "safety case". (For example, are there any conditions when a particular airport's GBAS operations should be suspended?)
- The safety case must demonstrate that the design provides adequate performance across CONUS airports, or the limitations of the design are documented. (That is, a "point solution" that that is adequate for only one location is not generally sufficient for a design approval.)
- Some threats are observable to the code-carrier divergence monitor implemented to detect satellite failures.
  - The ionosphere divergence rate generated during anomalous ionosphere conditions is observable to the ground CCD monitor.
- For the approach service, threats that cannot be observed by the ground station without a far field monitor or distributed regional monitors can be mitigated by making user geometries sensitive to such threats unavailable for use by the avionics through the inflation of broadcast integrity parameters used in the protection level and error bounding equations.
- The ground system can not observe if the ionosphere is in an active state or if fronts are present. User risk from errors due to unobservable ionospheric anomalies can be characterized, assessed if acceptable, and if not acceptable mitigated by denial of service for users with weak satellite geometries.
- Ionosphere anomaly-induced errors can be characterized by a simulation.
  - These ionosphere anomaly-induced errors are characterized by *simulating a storm front between the LGF and the user.*

IRCA Examples

Anomalous Ionospheric Integrity Compliance Faults 8.4

- Conditions that must conspire in order to experience the most extreme errors can be identified and modeled, although the ground facility may not in realtime be able to determine that these conditions exist at any given time.
- The simulation will generate constellation and location-specific results.
- The simulation will use a combination of worst-case parameters for those ionospheric anomaly parameters that could be known and random parameters for those conditions that can not be known. A uniform distribution is taken for two reasons: (1) to provide the range of possible errors experienced by the user and (2) so those inclined may argue that the histograms are conditional probability density functions.
- Front direction will be selected worst-case, perpendicular to the known approach direction.
- Denial of service limits the worst case error due to ionospheric anomalies.
- The maximum simulated error and a histogram of all conditions which produce non-zero errors will be used to characterize the ionospheric anomaly impact on the user.
- These errors are assessed to be acceptable and denial of service is not used to limit these errors.
- The vertical and horizontal protection levels , as defined in the DO-253B MOPS, may not fully bound all the anomalous ionosphere errors within the coverage volume.

- **The "safety case" or "inflation analysis" above indicates the end-to-end system performance is commensurate with that required for some aircraft.**
  - If the CAT I transition to visual case is acceptable, the visual autoland case is acceptable because both rely on having adequate and timely pilot cues for a judgment to continue the approach.
  - It is appropriate and sufficient to rely on aircraft approvals to address any detailed analysis, demonstration, or engineering judgment required. The ground facility approvable is only responsible for the monitoring and analysis above and making information available that characterizes the potential errors the aircraft may experience in the presence of anomalous ionosphere disturbances.

IRCA Examples

Anomalous Tropospheric Integrity Compliance Faults 8.5

- **The treatment of the residual troposphere errors in the MOPS protection level equations is appropriate, but is inadequate to bound tropospheric errors when there is a weather front between the ground facility and the user**
  - Troposphere delays observed by the LGF may be significantly different from delays observed by LAAS users.
  - The effect on integrity for the non-nominal residual troposphere is through the appropriate H0 and H1 protection level bounding. If the additional inflation is not set incorrectly, the resulting integrity risk could be higher than anticipated.
  - The “Through weather wall model” (Ref: Skidmore) is used to estimate the non-nominal troposphere error in the service region of the ground facility.
  - Account for this error in the H0 and H1 hypotheses at all times for all user locations for the worst conditions anticipated.
  - Aircraft and ground measurements of current conditions (P, T, RH) are not required; storm prediction not required.
  - Since it accounts for non-uniform conditions with horizontal distances the errors due to non-nominal tropospheric error variation can be effectively incorporated into σvig.
  - Nominal ionospheric activity and tropospheric events are independent so the σvig needed for bounding these troposphere events can be RSSed with the σvig needed to bound the nominal ionosphere.
  - Unlike sigma tropo, σvig scales with distance and allow bound of larger errors farther out without penalizing users who are not exposed to the weather wall.
  - Non-Nominal tropospheric error bound was determined by data collection and simulation.
  - “svig” = 5 mm/km for tropo covers the model outputs for the temperature, relative humidity, and pressure variation expected within CONUS.