To: Distribution **Document Number: FltDyn-CCP-11-1**

From: Ryan Proud – Integrated Aborts IPT Deputy
Jason Adam – Integrated Aborts IPT Lead

Subject: One Methodology for Proving Compliance to the Commercial Crew Program (CCP) Abort Capability Requirement

Date: November 18th, 2011

Executive Summary

As of Draft 4.0 of the CCT-REQ-1130 requirements document for CCP, ISS Crew Transportation and Services Requirements Document, specific language for the verification of the abort capability requirement, 3.3.1.4, was added. The abort capability requirement ensures that the CTS under dispersed conditions is always capable of aborting from a failed LV. The Integrated Aborts IPT was asked to author a memo for how this verification might be completed. The following memo dictates one way that this requirement and its verification could be met, but this is the not the only method.

1) Background

A number of historic launch vehicle failures were ultimately a failure to control vehicle attitude. Notable examples include the first the first Delta III launch, Pegasus XL, the Conestoga launch vehicle, and the maiden flight of Ariane 5 (1), (2). In addition, both Apollo and Shuttle experienced loss of thrust launch vehicle failures.

There are number of possible failures that might cause loss of control. If the propulsion system uses a thrust vector control (TVC) system to maintain its attitude, problems may be caused by hardware issues with the actuators, power supplies, or software issues with improper commands being sent to the actuators. Critical avionics hardware could fail – leaving the propulsion system in the 'last commanded position'. These problems could manifest themselves by actuators failing to hard over (maximum angle), or failing in place, or failing to the null position.

1.1) Requirement Background

The Ascent Abort capability requirement, 3.3.1.4, is:

> "The CTS shall provide continuous autonomous launch abort capability from lift-off through spacecraft separation with a 95% probability of success with at least 90% confidence in the event of a loss of thrust or loss of attitude control. [R.CTS.058]
>
> *Rationale: Flying a spacecraft through the atmosphere to orbit entails inherent risk. Analysis, studies, and past experience all provide data supporting ascent abort as the best option for the crew to survive a failure of the launch vehicle. This does not cover assessment of catastrophic conditions assessed by Loss of Crew analysis in 3.2.1.1. These abort performance parameters will include, at a minimum, aborting spacecraft controllability, near-field re-contact with the launch vehicle, hardware thermal constraints, human g-load constraints, structural loads limits, and ability to achieve acceptable landing hardware criteria. In order to provide an effective system, the ascent abort capability shall incorporate some type of vehicle monitoring to detect failures and, in some cases, impending failures. This requirement is in addition to the failure tolerance requirements in 3.2.3.1 and 3.2.3.2."*

The verification requirement, 4.3.3.1.4 is:

> "The continuous launch abort capability requirement shall be verified through analysis, anchored in test. Failure Modes and Effects Analysis establishes the failure initiators. The tests shall determine the performance of the detection system, abort logic, and abort flight systems. Analysis shall include verified high-fidelity 6DOF simulations including appropriate modeling of all systems affecting vehicle and launch abort dynamics along with their uncertainties for all appropriate flight phases. The Monte Carlo will insert the launch vehicle failures in a random fashion, uniformly-through-time, throughout the ascent trajectory. The Monte Carlo will simulate the spacecraft's entire abort trajectory from abort initiation through landing location. This includes, vehicle rotation rates during loss of control, changes in acceleration due to loss of thrust. The abort capability shall be considered successful for each analysis if the aborting spacecraft demonstrates controllability, no near-field re-contact with the launch vehicle, operation within: hardware thermal constraints, human g-load constraints, structural loads limits, and ability to achieve acceptable landing. The verification shall be successful when a Monte Carlo simulation of the required abort scenarios with environment, launch vehicle, and spacecraft dispersions, in time bins no larger than 10s each, achieve a 95% probability of success with at least 90% confidence throughout the ascent profile.
>
> See CCT-STD-1140 Flight Mechanics and GN&C Technical Assessment section for technical verification expectations pertinent to Flight Mechanics. [V.CTS.058]"

The pointer to the 1140 section for Flight Mechanics, section 5.3, adds detail for the expectations of the technical assessment. It should be consulted if any questions arise, but the verification statement was intended to capture everything necessary without needing to go to another document. In addition the Integrated Abort Analysis section, 5.4, could be reviewed to glean clarifications where confusion occurred.

2) Requirement Piece-by-Piece

Requirement 3.3.1.4 is a high-level vehicle requirement that specifies a high bar for abort capability. This bar is different from the loss-of-crew (LOC) requirement, 3.2.1.1. The LOC requirement includes additional Launch Vehicle (LV) failure modes like catastrophic explosions. The LOC requirement uses mathematical probabilities as part of its calculation. For example, if the LV failure mode is unlikely, then the impact of low success probability abort system wouldn't be very large. The LOC requirement defines the real probability of losing a crew. On the other hand, the abort capability requirement ignores the probability of the LV failure happening in the first place. It also ignores other LV failure modes that are not specified and all SC abort system hardware failure modes. This is the reason for "continuous" in the requirement. Even if the likelihood of the two specified LV failure types is low, there still needs to be an abort capability.

"Autonomous" is included to specify that the CCP Partners can't rely, as its primary means, on ground based assets, like flight controllers or other ground based hardware, to provide the abort capability. Everything necessary to abort needs to be contained within the onboard integrated system, the LV,Spacecraft (SC), and crew. While it may sound silly, this says that an abort landing design that relies on someone at the ground catching the spacecraft with a net isn't allowed. It also says that all the primary decision-making necessary to diagnose the abort condition and execute the abort is performed onboard by the LV, the SC, or the crew. Secondary paths that include ground-based flight controllers are certainly allowed, however they cannot be in the critical path.

"Lift-off" specifies the start of the requirement. There is a separate requirement, 3.3.1.3, for a pad abort capability that covers the pre-lift-off timeframe. For requirement 3.3.1.3, it can be assumed that a similar level of rigorous flight dynamics analysis will be applied to the pad abort condition as to the post lift-off condition. Though, the math on how to compute success may be somewhat different.

This abort requirement and verification stops being applicable at "Spacecraft separation" from the LV. This stopping point was chosen to include any failures that occur during LV thrust tailoff and during the post engine cutoff attitude control phase prior to separation. The period of time following spacecraft separation is covered by the requirement verification for 3.4.1.3, "The spacecraft shall have the capability to autonomously target and perform a deorbit, entry, and landing to a designated landing site upon initiation of a post-separation abort sequence. "

2.1) 95% Success

Because aborts always rely on at least one failure occurring before the abort has been initiated, there has been a historical decision to certify aborts to 2-sigma output success values. Historically, all nominal mission requirements have been certified to 3-sigma bounds or ≈99.7%.Mathematically, a double-sided normal distribution has 95.4% of the data inside +/-2 sigma bounds and 99.7% of the data falls inside +/-3 sigma bounds. This can be seen in Figure 1 - Normal Distribution Curve (from Wikipedia). However, using the words "2-sigma" assumes that all input data is distributed normally. It is possible that there will be non-linear distributions,

uniform distributions, single-sided distributions and other distributions defined by the designer for the input parameters. Thus, the requirement calls out an actual percentage number, 95%, that is an accepted approximation of what the combined distributions should combine to look like. For 95% on the results to be valid, the input parameters must be allowed to vary according to their statistical distributions, without clipping.

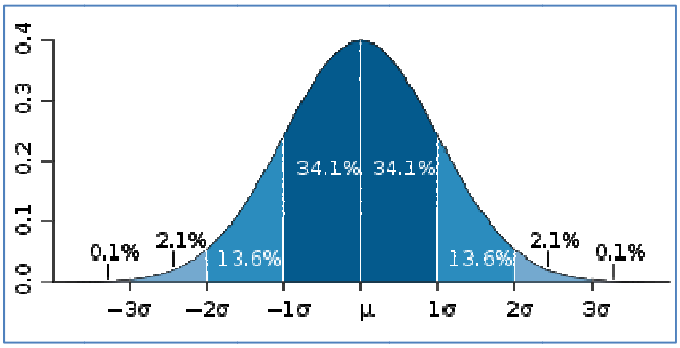

Figure 1 - Normal Distribution Curve (from Wikipedia)

Each trajectory either completely passes or completely fails. If a trajectory fails multiple success criteria it will only be counted as one overall trajectory failure. A trajectory must pass all listed criteria to be deemed successful.

2.2) 90% Confidence

Simply defining a success criteria like 95% without a confidence interval is inadequate for verification. It implies 100% confidence. The problem of defining adequate sample sizes in order to achieve confidence intervals is detailed in (3).

The CCP accepted 90% confidence as the interval, in part due its use on the Constellation (CxP) requirements. The CxP designers found that this confidence interval was useful for yielding an adequate design. For 2-sided output distributions (you can fail either high or low), you could choose to run a Monte Carlo sample size of 3000 runs. In order to claim 95% success with 90% confidence, you can allow no more than 134 failures in those 3000 runs. If the sample size is 100 runs, you can only fail 1 run to still meet the requirement. A sample size of 45 runs that yields 0 failures has a just greater than 90% confidence that the entire universe of runs will yield 95% probability of success. Note: other requirements may need different numbers of trajectories to support their verifications.

Finally, the statistical formula for determining success probability and confidence is not a function of the number of input variables that are being dispersed. If you are dispersing 500 terms or 5 terms the statistics on acceptable passes and failures is the same.

2.3) LV Failure Cases

The requirement specifies two flight mechanics LV failure scenarios to cover. Loss of thrust and loss of attitude control are both abort-able conditions that could possibly happen at any time during the ascent. For both of these failures, the SC cannot just wait on the LV to try to fix the problem on orbit (a few systems failures fit this description). Each failure type should be treated separately. The abort capability results must be shown separately between the loss of thrust failure type and the loss of attitude control failure type.

Loss of thrust is typically a benign failure condition leading to an abort. It is often triggered by analyzing filtered accelerometer data to diagnose the failure. A loss of thrust failure mode only applies to liquid engines that can be shut off or to air-start solid rockets that never ignite. To avoid stacking failures in the vehicle design, only one engine is modeled as failing at a time. Though, the abort separation may require the other engines to be shutdown to be successful. For LV with multiple engines, some loss of thrust scenarios do not result in loss of mission (or cause an abort). Though, for every loss of thrust failure scenario that precludes a successful mission, an abort capability is required.

Loss of attitude control is typically the most difficult LV failure to accommodate with an abort capability. Depending on the type of failure within the vehicle, loss of control can manifest itself slowly or very quickly. Attitude control loss can show up as a slow-acting failure where the LV engines lock up at some fixed attitude and the trajectory slowly diverges from the planned trajectory. To model TVC fail-in-place, actuators are frozen at whatever position they are currently set for flight control[1] under current conditions. Failure is in rock, tilt, or rock plus tilt (randomly chosen). (4), (5) This failure mode is often diagnosed with filtered rate gyro data integrated to show a trajectory certification envelope attitude exceedence.

Attitude control failures can also manifest themselves by a failed actuator that pegs the engine to the worst possible hardover angle. These are fast diverging scenarios. They are often diagnosed with filtered rate gyro data showing an attitude rate exceedence. On the Space Shuttle Program for fast diverging scenarios, like a TVC hard-over, the flight dynamics and range safety analysis randomly failed launch vehicle actuators in rock, tilt or rock plus tilt, and the direction of the failure is randomly chosen during the burn. (5) Each failure is to the hardware limit.

The combination of these 2 types of attitude control loss failures lead to some stressing abort initial conditions. In some cases there will be enough time for the LV to shut off the engines before initiating the abort to make the conditions more benign. In other cases the divergence may be progressing to a structural breakup condition for the LV and the abort needs to be initiated prior to LV engine shutdown.

The close interaction between LV failure scenarios and the driving abort design cases for the SC necessitate early communication between the 2 engineering design teams to clearly define how the integrated system will respond to failures.

[1] Driven by gimbal authority needs to maintain a nominal flight path

3) Verification Piece-by-Piece

”Verified through analysis, anchored in test” ensures that the verification of the abort capability requirement will be in analysis and simulations. Tests will provide data to anchor models that are used in the analysis. Tests can include integrated abort flight tests, stand-alone propellant system tests, wind tunnel tests, etc. As written, this verification statement does not mandate the type or amount of tests necessary for “anchoring”.

On the LV side the reason to initiate an abort needs to be defined through a rigorous process. Failure Modes and Effects Analysis, FMEA, is the required process for defining the abort initiators. These initiators are included in the complete abort capability performance evaluation. The SC abort logic and abort systems are also included ensuring that the capability is defined as an integrated system.

“Analysis shall include verified high-fidelity 6DOF simulations including appropriate modeling of all systems affecting vehicle and launch abort dynamics along with their uncertainties for all appropriate flight phases.” High-fidelity ensures that the models that are being used are sufficient for answering the questions being asked and accredited for use in the abort context. 6DOF ensures that the simulation can accurately model attitude in addition to the simpler position and velocity pieces. 6DOF is critical for analyzing GN&C performance. Models for the SC and the LV need to work both for nominal conditions and with uncertainties. Uncertainties during the design phase should be able to bound the potential inputs that may occur as the design matures. It is expected that the uncertainties will shrink as design moves into certification and ultimately into day-of-flight readiness evaluation.

“The Monte Carlo will insert the launch vehicle failures in a random fashion, uniformly-through-time, throughout the ascent trajectory.” This is the first place where it is specified that a Monte Carlo style simulation is expected with all the details that assumes on input dispersions and output statistics. (3) Since this requirement specifically doesn’t include the probability of the LV failure occurring, it is necessary to define when the LV failures will be inserted. Uniform-through- time was selected to ensure that enough failures would be simulated in each time bin to get statistical significance in each time bin. There will be the same number of LV failure IC’s between 10-20s as between 210-220s. By defining the failure time as an input into the Monte Carlo dispersion, it is expected that in each 10s bin the LV failures initiations will be seen throughout the 10s time-space. There should not be more than 1s between each run and its closest neighbor. Any separation between runs inside a 10s bin of less than or equal to 1s is adequate.

The launch vehicle failures that cause loss of control could be inserted randomly, uniformly across failure initiators. The actual probabilities of failing an actuator in one axis or the other or in both at the same time is not required to be accounted for. Whether using uniform or some other probability distribution, the data supporting the failure initiator probability distribution should be included in the deliverables . Unless there is a single failure mode identified that could fail the actuators in multiple engines, it is not necessary to include failures in multiple engines if the chosen LV has multiple engines. If the LV has multiple engines, the actuator failures should be randomly inserted across all engines. This includes solid engines that use active control.

“The Monte Carlo will simulate the spacecraft's entire abort trajectory from abort initiation through landing location.” This sentence was included to ensure that the abort capability was clearly defined as being assessed both during powered flight and under unpowered flight from initiation through landing. The immediate dynamics post abort initiation will be dominated by “vehicle rotation rates during loss of control” failures and by “changes in acceleration due to loss of thrust”. This was added to ensure that the abort sequence includes the LV added dynamics post abort trigger passage.

3.1) Defining Verification Success Criteria

To provide actual design value, the requirement must have clear definition of success. The verification includes specific categories that need to be included for the abort capability calculation. The actual values for success vs. failure will depend on the CCP Partners vehicle design (i.e. one SC structural limit will be different from another). It is up to each partner to define these values for their vehicle. These are typically defined as children requirements. Each category needs to be accounted for. “Controllability” is a GN&C and Propulsion driven item. The design doesn’t fail this requirement if open-loop instability occurs as long as there is enough closed-loop control margin. Loss of control often manifests itself in large errors between true attitude and commanded attitude. It can ultimately lead to vehicle tumbling which, depending on the aero forces, may lead to structural breakup.

“No near-field re-contact with the launch vehicle” ensures that the intact and separated SC and LV do not recontact each other. Recontact can be calculated by simulating the separation event with the planned timeline and disturbance torques on both vehicles in dispersed situations. Recontact is a rigid body calculation that doesn’t include flexible structure accordion modes or hardware that is designed for contact like bumpers. This calculation typically needs to be performed while the SC abort propulsion system is firing to achieve positive position, velocity, and acceleration relative motion. Later, far-field, recontact of the two bodies, when the LV is no longer thrusting or the SC is no longer firing to achieve deltaV in the velocity vector, is not a part of this requirement. This later timeframe is excluded due to the difficulty in accurately modeling the free flight or the structural integrity of the LV long after the initial failure occurred.

“Hardware thermal constraints” ensures that the vehicle design be evaluated against thermal criteria while evaluating trajectory designs. This criteria could essentially be summed up as “ensure the heating applied to the vehicle does not compromise the functionality of the necessary abort systems. ”. For abort situations the thermal limits for the design are often beyond the limits for the nominal design. This allows the vehicle to enter more stressing environments to save the crew and not worry about vehicle re-use. A historical region of concern for abort thermal criteria are second stage aborts that re-enter the atmosphere and have re-entry profiles that are significantly different from the nominal re-entry.

The ultimate goal of the abort capability is to save the crew. Thus, remaining inside the “human g-load constraints” is an obvious criteria. CCT-REQ-1130 Appendix H draft 4.0 specifies the acceleration limits for nominal ascent, abort and earth re-entry in both the positive and negative direction on each of the three body axes centered at each crew member’s seat location. These

accelerations are often maximized during the abort system thrusting and during the atmospheric drag slow-down or pullout. In addition, the requirements include rotational acceleration limits which are often maximized under parachute flight. Both sets of human acceleration or g-load requirements are defined as a peak vs. duration criteria. Any g-load constraints related to touchdown dynamics must be included.

"Structural loads limits" can take multiple forms. One form is a general indicator metric that takes a standard trajectory parameter like dynamic pressure times angle of attack or angle of sideslip and maps it to indicators of structural failure. The expectation is that this kind of metric indicates no structural failure if the trajectory stays below the indicator, but that if the trajectory goes above it then further analysis will be necessary to determine if it actually is a failure or not. The second form of structural load limits comes from the detailed analyses and modeling in a CAD and other analytical computer program which would take the trajectory and the loads environment, and determine exactly how the loads would be distributed throughout the vehicle. Indicator metrics should include any necessary touchdown load constraints that are related to the abort trajectory. For vehicle designs that plan for aborts to be certified at one-time use limits, it is possible that the structural constraints will have different factors of safety between the nominal trajectory and the abort trajectory. JSC 65829, Loads and Structural Dynamics Requirements for Spaceflight Hardware, provides guidance for the loads analyses (6).

Finally, the SC must prove the "ability to achieve acceptable landing" for an abort at any time during the ascent trajectory. For vehicles that require runways, this means a runway landing must be achieved. For vehicles that need land landings, the ability to reach land at all times is necessary. For vehicles that are only water landing capable, the ability to avoid land for all conditions is necessary. If a successful landing requires parachutes, then the sequence must allow for the time and trajectory conditions required by the parachute system. This is similarly true for thrusters or other landing systems. This criteria historically has been difficult to meet in the pad and near-pad abort region. The verification trajectories need to continue all the way through touchdown, 0ft altitude above ground level. Any abort trajectory constraints that are a result of touchdown dynamics should be included. For example, if the crew seats are designed with a specific stroke to absorb energy that puts a limit on vertical impact velocity, then the vertical impact velocity at touchdown should be included as a part this success criteria. When coupled with the Down Range Exclusion Zone (DAEZ) requirement, 3.3.1.7, this criteria can also become difficult to meet for the DAEZ boundary cases.

3.2) Verifying in Time Bins

"The verification shall be successful when a Monte Carlo simulation of the required abort scenarios with environment, launch vehicle, and spacecraft dispersions, in time bins no larger than 10s each, achieve a 95% probability of success with at least 90% confidence throughout the ascent profile." Earlier it was mentioned that the Monte Carlo method would need to be used including dispersions from the LV, the SC, and the natural environment. In addition to vehicle propulsion dispersions and navigation dispersions the atmosphere and winds need to be accounted for in the dispersions.

10s time bins were chosen as the maximum amount of time to allow the designers to average across. This means that between 0 and 10s 95% of the cases need to work with 90% confidence. Between 30 and 40s, 95% of the cases need to work with 90% confidence. Between 210 and 220s 95% of the cases need to work with 90% confidence. Etc. This binning verification was added to ensure that risk isn't averaged out by having a large portion of the trajectory 100% successful and a brief period 0% successful. If the verification allowed time averaging, feasibly there could be a black zone that didn't have any abort option. In addition, there could be a region of the trajectory that was never evaluated and its own risk was hidden.

Time binning doesn't mean that the design only has to be evaluated every 10s. Earlier it was specified that the LV failures must be uniformly distributed through time, thus providing failure cases throughout each 10s bin that must be evaluated. While requirement verification can add up to many thousands of runs, it doesn't preclude doing worst on worst analysis for early design studies. The design team should feel free to use bounding cases for early analysis, but can't rely on it for ultimate requirement verification.

4) One Adequate Abort Analysis Methodology

Figure 2 shows one methodology for calculating abort capability. This is not the only methodology that works. Each CCP partner is free to define its own method for how to show requirement compliance. Other requirements, like coupled loads assessments, may follow a completely different methodology.

The top half of the figure shows a few of the input dispersions necessary to run the Monte Carlo simulation. These dispersions and associated models include LV, SC, and environment. In this methodology the LV trajectory simulation is completely separate from the SC trajectory simulation. Accuracy between the 2 sims is ensured through state vector and dispersion file matching between the sims. Thus, it is not necessary that one sim includes everything.

The bottom half of the figure depicts the output calculation for success vs. failure. For this methodology where the LV and the SC are in separate simulations, the launch to land trajectory performance is calculated for one LV trajectory and one SC trajectory. The Monte Carlo does not have to run multiple SC trajectories for every LV trajectory as long as a statistically significant (enough to give 90% confidence) number of LV trajectories from the pad up to the abort initiation time are generated. The calculation of success vs. failure is made for each abort capability success criteria. The rolled up risk for each time bin can then be generated separately for each of the abort initiators, loss of control and loss of thrust. An alternate ways to do the time binning includes rolling 10s averages. This alternate option is not described in this methodology example, but it is not precluded by the verification statement.

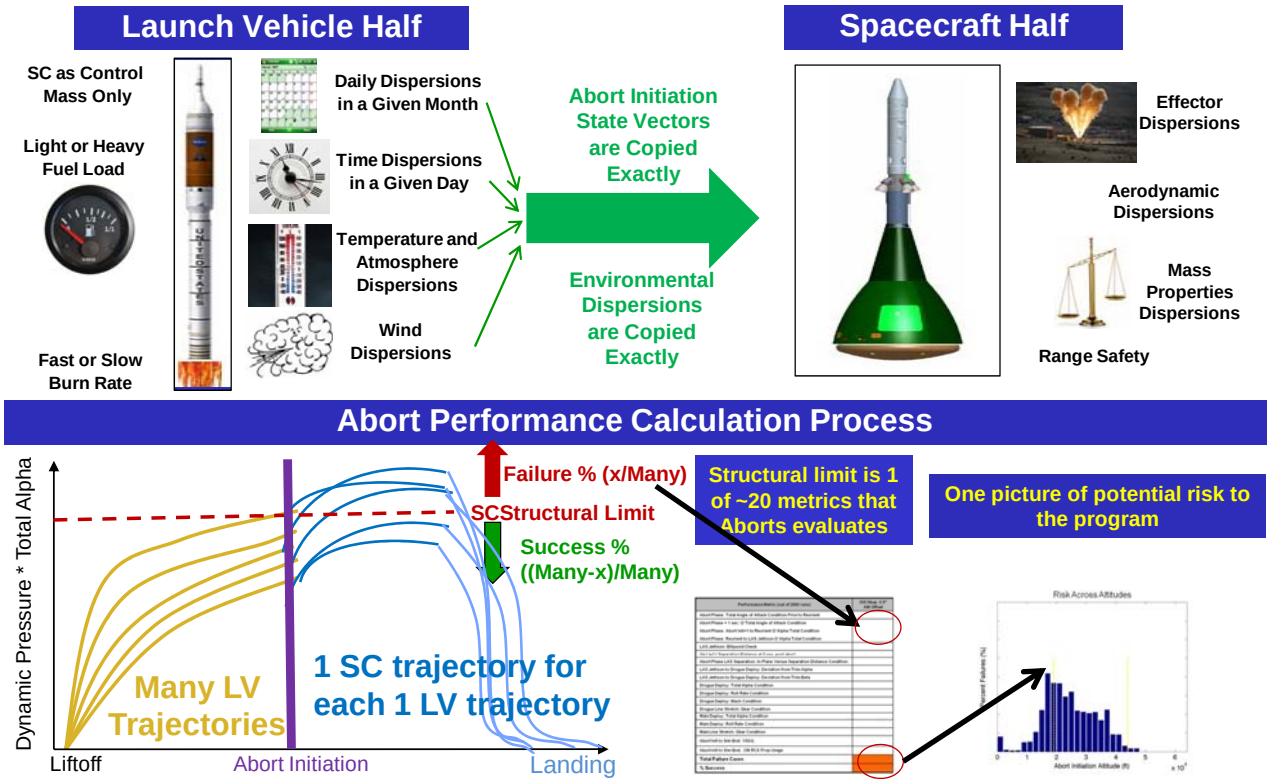

Figure 2 - A Graphic of One Method for Calculating Abort Capability Performance

As each CCP Partner determines its own methodology for calculating abort capability performance, it is recommended to work backwards from defining the output product, to defining the tool requirements necessary to generate the output, and finally to defining the inputs into the tool that are necessary. Working in this direction can often eliminate unnecessary model buildup where it didn't provide added value into the output product. The following sections go into detail on each step proposed.

4.1) Define Output Product

Every customer of abort trajectory data requires different products: single trajectories in Matlab, Excel, or ASCII; data in different coordinate systems that make sense to them; Monte Carlo trajectory data for specific LV conditions or every LV condition; abort capability success metric performance tables; and rolled-up abort capability requirement compliance data. Often, the first products mentioned will be requested by other, non-abort, subsystems to support their designs. For example, the parachute designers may ask for stressing abort conditions. To show CCP requirement compliance, ultimately only the last data product is necessary. However, building a tool that can accomplish all these needs may reduce work duplication.

Figure 3 - One Method for Documenting Abort Capability Performance in Each Time Bin, is a sample plot for documenting the abort capability results for a fictional 500s LV ascent trajectory. One plot will be created for vehicle response to loss of thrust failures and another plot will be created for loss of attitude control failures. Each 10s time bin is a bar in the histogram. Every time bin is plotted on the x-axis with the failure percentage of that time bin on the y-axis. If any individual time bin shows a failure percentage greater than 5%, then the 95% success requirement for the entire vehicle is failed. Figure 3 shows a design that fails to meet the requirement. Alternate ways to plot could include success percentage on the y-axis or to break each histogram bar up into the specific success criteria that was failed.

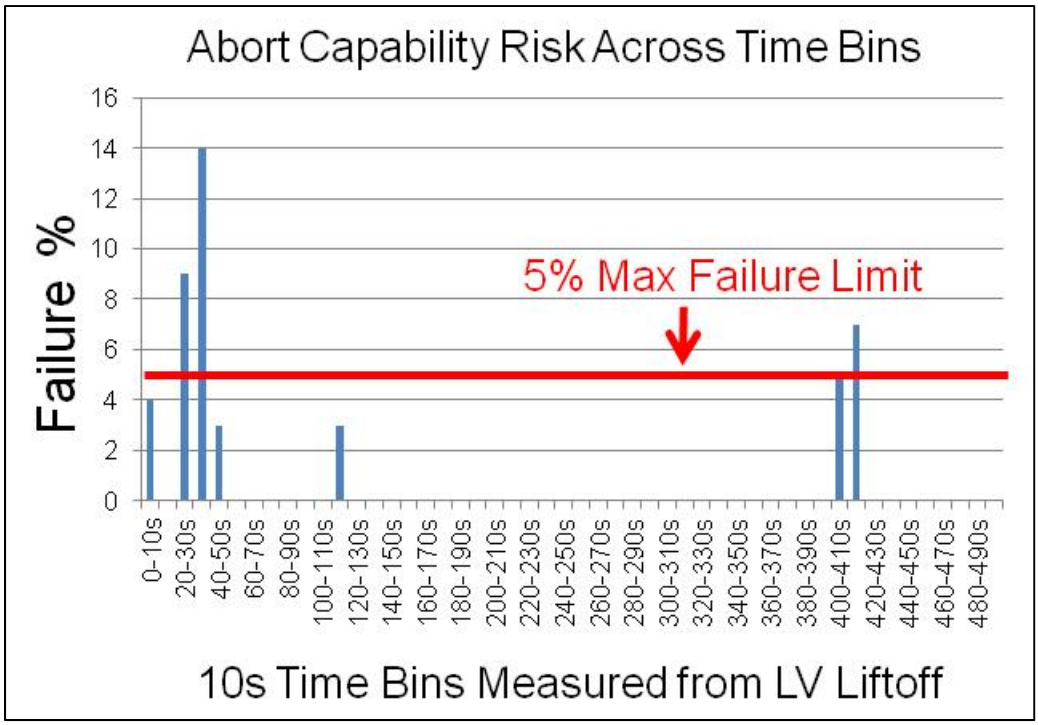

Figure 3 - One Method for Documenting Abort Capability Performance in Each Time Bin

The rolled up abort capability requirement compliance data can also be used to aid in vehicle-level architecture trade studies. For example, this methodology can be used to understand the potential impacts of changing the OML, changing the target mass properties, or changing the CG location. These parameters are often changed in the context of the nominal mission design activity, and a robust abort capability analysis process can be used to insert an understanding of how these changes impact the residual abort risk.

4.2) Define Tool Requirements for Achieving the Output Product

In order to produce output products that analyze trajectory data, a simulation must be created or repurposed to generate the trajectory data. When a simulation is going to be created, it is often best to detail the necessary models and to set a fidelity schedule that defines the fidelity of the model necessary to achieve the next milestone's level of rigor. Having this plan up front ensures a clear development path towards final requirement compliance. Each model must be accredited

that its fidelity and accuracy is sufficient for the intended purpose. Reference (7) describes one way to accomplish this.

When a simulation is repurposed for use on a new program, the path to accrediting the models for the new purpose is often easier. Typically, there will already be data in hand that unit tests the models and proves necessary accuracy. When models are changed for the new simulation, then the unit tests will need to be performed again to show the changes are correct. In this context, model changes refer to the actual algorithms themselves and not just an input data change.

4.2.1) Simulation Model Definition Databook

In this methodology example, the simulation models that are used for the abort capability calculation are defined in a simulation model definition databook. The databook would be a deliverable that provide the traceability necessary for requirement certification. The databook lists out the version of the model that is to be used and any relevant caveats. For example, GRAM is one atmosphere model that could be chosen. The simulation model definition databook will specify which version of GRAM, like 2007 version 1.4, is to be used. Any known issues should be written as well. For example, if the LV is using GRAM version 1999 and the SC wants to use GRAM version 2010, then there will be a guaranteed error in the abort initiation states. If this error is accepted for the level of fidelity required in the analysis, then that should be noted.

4.3) Define Inputs

The input gathering process can be the most problematic and time-consuming of the 3 steps. It relies on multiple subsystems to produce models and data prior to an abort capability calculation commencing. The types of model inputs include: time of year, temperature and atmosphere, winds, propulsion, mass properties, and aerodynamics. All of these inputs have average/nominal/mean values in addition to dispersion profiles. The staggered way the design updates are released from other subsystems can lead to discrepancies in release data. For example, the parachute design team might release models and data for parachute performance using one set of mass properties. By the time the abort calculation process can occur the target mass properties may have changed. If the abort capability calculation takes in the new masses then the final results are not case-consistent with the parachute results.

During the design phase of a program, prior to CDR, it can seem that during every cycle every input changes. This makes it very problematic to pinpoint whether a trajectory response issue was due to new SC mass properties, new separation aerodynamics, new LV failure models, etc. The abort capability methodology should include a check to see that the inputs are consistent and intended to be used together.

4.3.1) A Simulation Input Databook

Similar to the Simulation Model Definition Databook described in section 4.2, a databook that defines the inputs into the models is created in the example abort capability methodology. This databook also would be a deliverable that provide the traceability necessary for requirement certification. This databook is used to document both the nominal or mean inputs that are used

for every model, and it also includes the dispersion values that are used. The input databook can include pointers to other version controlled documents where appropriate. For example, if the simulation includes an off-the shelf environment model, then the actual input data into that model does not need to be included. Though, a document reference pointer is included. If any default data in the off-the shelf model is over-written, then those changes should be included in the input databook. For input dispersions, the model driving data should include any assumptions about its statistical properties. Is the input dispersion number a max/min, one-sigma, three-sigma, etc.?

As designs mature, actual model data will be created that shows the true, expected nominal and dispersed performance of the system being described. If the designers met their requirements, then this true model nominal and dispersed performance will be inside the system requirement bounds. In the example abort capability process, both inputs are included in the input databook and used for different purposes. For some trade studies, the abort capability will need to be calculated using the spec model nominal and dispersed values to ensure robustness against future design changes. For requirement compliance, using the true expected nominal and dispersed performance model data is one option. An additional option is using every system's worst case specification performance at its dispersed limit.

5) Requirement Value: Finding Hidden Risk

The value of looking at the abort capability risk using the verification path defined in 4.3.3.1.4 is that it unmasks hidden risk. During initial design studies, trajectory analysis is often performed at one or a few assumed critical points. This can be useful for quick turn-around analysis but it won't reveal the complete picture.

Near-pad aborts can be more difficult than pad aborts due to the added LV dispersions that are not present during on-pad aborts. Aerodatabase iterations may shift the region of least control margin (or worst instability) as fidelity in the model grows. LV trajectory changes, from additional lofting or changed insertion altitude, can shift the timeframe with the most exposure to the DAEZ. New success criteria may be added if the abort capability analysis shows that a system originally designed only for nominal cases has difficulty meeting abort environments even with a change in the required success criteria and/or factor of safety.

Ultimately, the real risk that is known at the end of the abort capability verification is how much residual risk exists for a failed abort sequence at any time along the LV trajectory. This requirement will prove if there are any "black zones" along the LV trajectory where there is no chance of executing a successful abort for the loss of control or loss of thrust LV failure modes. It accomplishes this by limiting the ability of the designers to average out risk only across one 10s time bin. Inside one time bin, one second of 100% failure and 9s of 0% failure still average out to 10% failure across the time bin. Thus, the problem areas will be found. Averaging out risk across the entire LV profile is not allowed.

6) Conclusion

The CCP Integrated Aborts IPT was asked to provide detail, context, and examples that would clarify the abort capability requirement and verification, 3.3.1.4 and 4.3.3.1.4. The requirement and verification statement were expounded upon. An example abort capability calculation methodology was described. This methodology is not simple. It will take some time to set up if starting from scratch and some computing resources to actually run. But, it is a tenable problem that has been proven successful, effective, and necessary on prior human spaceflight programs.

(Signature of Author)
Ryan Proud
CCP Integrated Aborts IPT Deputy
EG/Aeroscience and Flight Mechanics Division
NASA-JSC Engineering Directorate

(Signature of Author)
Jason Adam
CCP Integrated Aborts IPT Lead
EV70/Systems Engineering and Analysis Division
NASA-MSFC Engineering Directorate

References

1. **Harland, D. M. and Lorenz, R. D.** *Space Systems Failures: Disasters and Resuces of Satellites, Rockets and Space Probes.* s.l. : Springer, May 2005.
2. *Launch Vehicle Failure Dynamics and Abort Triggering Analysis.* **Hanson, John M., Hill, Ashley D. and Beard, Bernard B.** Portland, Oregon : AIAA Guidance, Navigation and Control Conference, August 8-11, 2011. AIAA 2011-6502.
3. **Hanson, J.M. and Beard, B.B.** *Applying Monte Carlo Simulation to Launch Vehicle Design and Requirements Analysis.* Alabama : Marshall Space Flight Center , September 2010. NASA/TP—2010–216447.
4. *CxP 72069-06, Ares I Guidance, Navigation and Control (GN&C) System Definition Document (SDD) Volume VI: Abort and Failure Modes.* Huntsville, AL : National Aeronautics and Space Administration - Marshall Space Flight Center, April 16, 2010.
5. *Ascent Trajectory Simulation for the Space Shuttle Launch Area Risk Assessment.* **Gowan, John W.** s.l. : AIAA Atmospheric Flight Mechanics Conference and Exhibit, August 2005. AIAA-2005-6505.
6. *Loads and Structural Dynamics Requirements for Spaceflight Hardware.* Houston, TX : s.n. JSC 65829.
7. *STANDARD FOR MODELS AND SIMULATIONS.* NASA-STD-7009.

Distribution
Ryan Proud\JSC
Jason Adam\MSFC
Ed Burns\JSC
Steve Sullivan\KSC

Steve Schenfeld\JSC
Joseph Brunty\MSFC
Chris Iannello\KSC
Mike Gilbert\LaRC