# NATIONAL TRANSPORTATION SAFETY BOARD

Office of Aviation Safety
Washington, D.C. 20594

March 09, 2015

## Attachment 25 – Interview Summaries

# SYSTEM SAFETY

**DCA15MA019**

# Contents

## A. INTERVIEW SUMMARIES

### 1.0 Interviewee: Nicolette Dugué, Scaled Composites

**Date:** **December 10, 2014**
**Location:** **Scaled Composites; Mojave CA**
**Time:** **1000PST**

Present: Mike Hauf, Mike Bauer, David Lawrence, Katherine Wilson, Lorenda Ward - National Transportation Safety Board (NTSB); Will Robertson – Virgin Galactic (VG); Bob Withrow – Scaled Composites (SC); Dan Murray, Kristy Helgeson (FAA)

Ms. Dugué was represented by Mr. Gary Halbert, Attorney, Holland and Knight.

During the interview, Ms. Dugué stated the following:

Her full name is Nicolette Christine Dugue and in April 2008 she began her employment at Scaled Composites.

Her current title is Project engineer and her position is project coordinator. Her duties are to manage subcontractors and coordinate their effort in engineering and operations. She is responsible for status updates and reports.

Her employment history at Scaled – System Safety Analyst for the Tier1B project (the project name for the SpaceShipTwo (SS2) program); she took this project over from Mark Zeitlin. When she arrived at Scaled, the System Safety Assessment (SSA) for WhiteKnightTwo was mostly complete; she started working with the SS2 SSA. She also managed updates and configuration changes to the SSA, worked to start the transfer of information and parts to the spaceship company (TSC) starting in the spring of 2009 and did this until early 2010. In the winter of 2009 she also added in some speedbrake design changes and worked the pneumatics portion of the speedbrakes through fault tree analysis (FTA). She started working on the AST permit application in the spring of 2010. She was understanding the requirements for an experimental permit and transferring design information to Michelle Murray at the FAA for pre application consultation. She also stated that in the summer of 2010 she passed the permit application to Bob Withrow as she began engineering work on the rocket motor system.

Niki was asked about her training/education in system safety. She indicated that she took a system safety course in June 2010 through APT research in Huntsville AL (1 week) and was the only formal class that she took. She was also trained on the job by Mark Zeitlin (Scaled Employee) on the existing SSA analysis and methodology, as well as Drake Group on processes and guidelines.

Niki was the main system safety analyst for the Tier1B program. The process includes design engineering, project manager, and project engineers. When we go through analysis Niki does the framework, we sit down and discuss whatever the topic is for the day in detail. Come to

consensus on logic or classification of risk. Niki will then, if required create a fault tree analysis. She reviews the applicable system schematics layout what she thinks is logical path to system failure. She then makes sure everyone agrees on that. The FTA's (and FHA) are continuously updated and reviewed.
The SS2 project engineer was Jim Tighe
The design engineer depended on the system.
The Tier1B project manager was Matt Stinemetze

Some of the SS2 system safety assessment document had been written by Mark Zeitlin, and some by Steve Jones who was the analysis before Mark. Niki kept the document updated and added new material as required. The SSA was vetted through Matt Stinemetze before every release.

Asked how much of the feather FTA (13.01 and 13.02) was completed before Niki started? She said that none of SS2 analyses were complete because SS2 was still in the design phase when she started. When she started, FTA 13.01 was in a draft form but she changed the FTA quite a bit based on changes to system designs as it evolved and the hazard assessment was also updated.

She was asked to describe how human performance is captured in the system safety analysis. One of the overarching assumptions stated in the system safety analysis is that Scaled assumes that the pilots will perform their function adequately and that is due to the fact that Scaled does simulator training prior to all flights. The SSA does not account for pilot induced error. However, the FTA does account for pilot reaction when it is used to mitigate a hazardous or catastrophic event from happening (corrective action). Pilot error is mitigated through training. She does not analyze the pilot as causing a hazardous or catastrophic event.
The question was asked, if something could be mitigated by the pilot, how is this information communicated to the flight crew. She stated that this was done through the normal and emergency procedures. She keeps a record of any mitigation she enters. Every time she puts in either a procedural mitigation or a pilot action into the FTA she keeps a list of them and then the list is placed into the normal and emergency procedures as applicable.

Asked if she thought if the waiver issued by FAA was necessary? She believes that the public safety was covered by simulation sessions and flight test training. It was not needed because Scaled's system safety analysis covered the requirements for safety analysis.

She was asked to describe the general process used to perform the FHA's specifically what standards or guidance was used to create the FHA. She indicated that: Standards/guidance – Drake Group had a process that was provided and taught to Scaled on how to start and maintain a system safety analysis.

To perform an FHA, she meets with the applicable engineer/group and discusses all the possible ways that function or system can fail during a specific flight phase. They don't assess probability of failure at first, just the hazard. They determine the effects of that failure and classify it as minor, major, hazardous or catastrophic. They continue to do that throughout program as things (systems) change, nuances of aircraft learned, can upgrade or degrade status. This was done in group setting, talk about many things including meteor strike etc, for this

project anything Hazardous or Catastrophic required further analysis (FTA), set goal to 1 in 100,000 for Hazardous and 1 in one million for Catastrophic.

She indicated that a failure mode and effects analysis (FMEA) wasn't done. How were failures of actuator determined? Like any other actuator it can fail in a number of ways. The feather actuator was designed in house so for those things and things used outside of their typical uses, I would make a separate FTA for my own understanding, break it down into seals, pistons, cylinders etc and do a FTA to determine probability of failure and compare to database I used for component failure. Did you coordinate with engineers? Yes, of course, they helped determine interaction failure modes. Michael Fuchs was the design engineer for feather actuator.

Three catastrophic hazards were identified for feather system can you go over them? She indicated that when we went through the functional hazard assessment for the feather actuation system, the purpose of feather was for carefree reentry (FTA 13.01). The feather is needed for reentry, if the feather deploys during boost we know it is a catastrophic event and we knew that because the rocket motor is still firing, there would be excessive forces and it could induce pilot controllability issues.

In FTA for 13.02, due to the fact that the locks whole purpose is to hold the feather down in the gamma turn in the high load area, we determined that the FT did not need to include the locks because it wasn't hazardous or catastrophic due to the reliability of the locks themselves. FTA 13.02 was the feather failing after the locks were unlocked was the failure condition that Scaled analyzed.

The feather locks have to be unlocked for the feather system to fail (excluding structural failures).

A question was asked if there was consideration of the hazard for the locks failing or not holding in the gamma turn (high load area). Niki stated that they never didn't consider it a hazard, but they knew that the probability of the locks failing, which was within the 1 in 10 million range. So if the locks are unlikely to fail during this time, the time that it is catastrophic is when the locks are no longer in the picture.

Once the SSA is complete what is the release process? – I wouldn't say it is ever complete but when a revision is released, it is reviewed by Matt S (the program manager). It's open for review on a shared drive. Anyone in the project can look at it. It can be provided to VG. Also updates are delivered to AST to inform them of a change.

Asked if this was the first SSA that Scaled performed? Yes, the first program with a full blown SSA. They had done individual hazard assessments for Tier1 (SpaceShipOne, not Tier1b, which is SpaceShipTwo) but it was not a formal SSA. (Tier1 includes the SS1, RM1 and WK1). She learned system safety from SpaceShipOne. Also provides something to provide to the customer.

You said you would meet with engineers, would they be briefed? Yes, they were briefed on assumptions and if they started going down a road violating assumptions I would redirect the

discussion for example that maintenance is done properly and verify through test that the system can perform the job it's designed to do.

In the 13.02 FTA, you mentioned it was based on the locks being opened at proper time? Yes it assumes everything is nominal up till then. Were there any discussions related to something overpowered the actuators? No, because that assumes something has failed or that they were undersized. We sized the actuators based off of loads we believe would be seen during nominal flight. We do testing to make sure they can handle the loads during a nominal flight.

Can you clarify who was with the Drake Group? Niki indicated that Bob Honzic (DER) provided guidelines to Scaled in the form of a document with a process for SSA based off of SAE guidelines. Where there other guidelines? No we read AST guidelines and felt we were going above and beyond

You mentioned that there were changes to the FTA, do you recall those changes? No particular changes, but the pneumatic system was adjusted and the FTA was updated. One big change was introducing a pneumatic jam causing feather to not actuate or retract.

The methodology section of the hazard analysis indicates that the pilots will perform their job adequately, is that common? How did you make that assumption? The assumption was made before I started, but had conversation with Matt and Jim to make sure we were doing right thing. We have a long history of flight test. Pride ourselves on having very good test pilots. SS1 showed us simulator was very helpful on training crew on how to do job. Determined that would cover that part of the hazard analysis.

Do you recall if the guidelines required human error? No I don't recall. Were the pilots involved? Many pilots have other engineering duties so they would be involved if their system was being analyzed. They were involved in flight test readiness reviews where we go over the system safety analyst findings and any limitations or concerns.

The SSA class you took, was that because you would be doing SSA for this program? She took the class a couple of years after she started as Scaled. She had learned the process through on the job training up to that point. She wanted to take a formal class to see if there was something I was missing or different analysis that we could do that might be useful. The class was pretty rudimentary.

Asked who signed off on the system safety analysis? Project Manager Stinemetze.

Can you describe the safety culture at Scaled? Scaled believes that every design engineer is responsible for their system from conception to implementation. Each design engineer is responsible for the safety of their system and every person is responsible for understanding what they are working on for flying or training for and that they ask all the questions that they need to ask in order to keep everyone honest and safe. While I say that every design engineer is responsible for their system, they also have people they rely on to ensure that they didn't miss anything and they do that through subject matter experts, bosses or project engineer.

my job was more of an outside audit and it didn't necessarily focus on the reliability of the system, but the reliability of the function which can contain many systems and how they interact. So if she found that the design of a system affected a different system in a negative way we would talk about that and change one or another in order to mitigate that issue.

Any concerns about how the SSA was conducted? I can't say I was uncomfortable with anything, it was new to Scaled, challenging for the engineers (getting them into the mindset was initially a struggle) to help someone review schematics and look for changes that help understand how their system could affect SSA, it's still on me to go ask the individual system designer if something has changed, a lot of what I know is what the design engineer or project engineer informs me of. I'm not doing the job 100% anymore only about 5%. If a big revision was coming up, I'll send out an email asking if anything affected the SSA. A lot of what I know is based on what I'm informed about.

Were there any major changes to the FTA or SSA prior to PF04? Mainly to do with the rocket motor

IF you didn't feel comfortable what would you do? I would bring it up to project engineer or to the project manager. We would discuss it and come to a consensus. If still something left open, that would be presented in a FRR as still being up in the air or something worried about and group decides to accept risk or not. Wont' proceed with test unless all agree.
One item came out of PF04 TRR (test readiness review) that had to do with the rocket motor qualification testing for future flights.

Who do you report to for this project? Matt.

Did you have any concerns about PF04 about analysis? I was comfortable

During the FTA, you make the assumption that the pilots will perform their job adequately. Yes, that is correct.

Did you say you sit on SIMs? – No, the pilots are trained in the simulator and I do not sit in on the sessions.

You said you assume a pilot can intervene is that correct? I assume a pilot can perform a corrective action given a failure.

Is there any analysis done on an inadvertent action performed by a pilot? No

From guidance you have, is it normal that pilot actions are not considered? I can't answer what is normal.

About the waiver what was your involvement with the waiver? Not involved in waiver at all. Only involvement was to answer questions from AST about SSA.

Did Scaled apply to waiver? We did not apply for the waiver. Bob Withrow could answer why waiver not applied for.

You mentioned pilot reliability changing what did you mean by that? For FTA, we assume a conservative failure rate for components of 1 in 1000. For pilots, we don't assume that. It is based on a high workload environment. Human is not a component. If the pilot is under a high workload, his reaction time will be slower (a probability of 1 in 100 to 1 in 10 depending upon the situation – case by case)

What's considered high workload phase? Takeoff, landing, and boost. Boost is high workload and high stress which is why we have RMC (Rocket Motor Controller).

What would you say the normal reaction time of a human is? it depends on the failure and the time to react. Some things can't be reacted which is why we have a RMC. If we felt we needed to investigate further, we would go off to test.
Did you do that for PF4? No.

System Safety is a small part of your job, what are some of your other functions that take you away? I work as project coordinator on a different program, and the reason that system safety does not take a lot of my time is because the system is mature and doesn't require full time work. I come in for updates but they are rare.

Outside scaled do you have any other experience in system safety analysis? No

Do you have other SSA experience? No.
Did you attend any other training? No, didn't attend a course provided in Mojave because it was the same course I already attended.

Would Scaled's FTA cover underperformed or under designed components? No. Assumption is system is properly designed to perform job it's supposed to do.

Does Scaled have a System safety culture? Yes, we do have a safety culture.

Are engineers concerned about safety? Yes the engineers I work with are concerned about safety. "Question, do not defend"? Means always feel free to question a system, design, process, make sure you get an adequate answer. Don't defend for defense sake.

For PF04, what modifications were most recent updates made to the SSA? The SSA modifications included Rocket motor, system (b) (4) and not directly related to the SSA but we changed fuel grains. Feather system not something that changed before PF04.

Can you describe the process with regard to traceability particularity for procedural mitigations when you have analyzed the hazard and you identify a mitigation that can be applied through procedure? What is the traceability for how that procedure is traced back to the hazard itself?

Whenever we implement a procedural mitigation, there is a note box in the FTA that states that mitigation. That mitigation is also stated in a column in the functional hazard assessment and will state what the procedural mitigation is for that failure condition that is then transferred via email to put into the emergency procedures or normal procedures depending on what the mitigation is.

And it is then updated? Yes it is reviewed and then it is used.

How many would you say are procedural mitigations? For hazardous and catastrophic hazards, procedural mitigations are fairly rare.

Are they tracked differently as updates through configuration management? Once they're entered they stay in procedure. I keep a list of all procedural mitigations and review against FTA. If something got missed, then I would fix that.

Can you speak to flight test training? What was the unlock procedure? I can't speak directly to the flight test training itself because I am not involved in it. I can't speak to the emergency procedures writing and the hours spent validating. We spent many hours in the simulator performing normal and emergency procedures to make sure correct and pilots can do them. In the FTA, we correct by design first. The last step is a procedural mitigation.

Were you aware of the alert at Mach 1.5 if the feather was not unlocked? No, not aware of an alert to crew that feathers not unlocked at 1.5 mach.

For the system safety side, was there any analysis done for that alert to be put in? No, on the system safety analysis side, the indication for the crew to unlock the feather system was a rocket motor firing time. Alert did not come through system safety side.

As far as guidance did you look at FAA ACs? Yes, 1309.1
How about NASA guidance? No
How about MIL Standards? No

Who did you interact with at FAA? Many people but the main person within AST was Michelle Murray.

So if you were to provide the hazard analysis to the FAA to meet the requirements, would it go to Michelle? Actually it would go to Bob Withrow and Bob would distribute to who was relevant.

So, Bob was you supervisor? Bob was leading the permit application process, so everything that either the FAA (AST) asked of us came through Bob.

Did you have any direct contact with the FAA AST? Yes, mostly through telecons to review documentation that Scaled provided.

Would there be multiple people during the telecon with AST? Yes

And what group of AST was that? It was always changing.

Did you meet with The SpaceShip Company (TSC)? Yes, can't recall the year but we met early on when they were starting up their system safety analysis, I had a list of components that I felt needed further scrutiny as far as determining its failure probability to determine if the number I used was too conservative or that given the environment that we were using it in we may want to do additional testing on it to verify that its cycle life (mean time before failure) was still applicable. We did do environmental testing on components that we were using outside of their normal use to make sure it was adequate for our use, but for commercial use I felt that maybe more scrutiny was needed and I gave them that list.

Do you recall your peer equivalent at TSC? No, I met with multiple people including Will Robertson.

Clarification, you said people at Scaled engineering were concerned about safety, were they concerned something was unsafe, or were they concerned about safety? Everyone designing is concerned about safety and trying to make sure they are doing their best to perform their job and considering as many issues to mitigate hazards.

Can you clarify Feather unlock risk analysis based on boost time not speed? Correct.

So the risk analysis was not done based on a 1.4 Mach but was based on the time of the boost? Yes.

Because the boost times are different for PF01, PF02, PF03, and PF04 (38 second boost) Was there a different analysis done for the feather unlocking on each one of these flights?
No, so the FTA was done for a full duration flight. When we were not doing a flight that was not based on the full duration, I would go back and review the FTA and update it per the flight. This flight (PF04), the pull up maneuver, was going to be similar to what a normal flight would be, just the duration was shorter. So that the high load area was still within the boost timeframe that my FTA indicated.
The procedure for unlocking is at 1.4 correct? Correct

From what the NTSB has learned, there is a transonic region, which is speed associated between about .8 to about 1.1. Was there a risk of lift on the feathers that would overpower the feather. Yes, the locks are in place to hold the boom down because the feather actuators themselves cannot hold it.

But that is based on speed? It is based on speed. Now, initially when we were talking about whether or not to unlock the locks in boost to mitigate their potential failure for re-entry, the cue we had was time based. The change from time to speed was not relayed to me so that is why the FTA was not updated.

Was there any analysis done on a speed basis for the unlocking of the feathers? Not in my SSA.

Where is the time indicated in the SSA. It is located in 13.01.

Before working for Scaled, she worked for propulsion and fuel mods for commercial aircraft Boeing in Long Beach. Prior to that, maintenance manual updates in San Diego for the 787.

You said this was the first time a SSA done Tier1B, are other programs going forward doing it now? Yes, certain programs on a case by case decided by Scaled and the customer.

Concerning the use of the word cue and not the letter Q, which may be confusing, the word cue was used in how the pilot knows when to do something as opposed to the aerodynamic cue? Yes, correct.

You stated that the SSA was designed on a full duration flight primarily and that you go back and review if it was not a full duration flight? Correct

Was there a variable trajectory or a fixed trajectory for the flights given burn time? The trajectory was based on the envelope expansion.

Was there a relationship between Mach and burn time? I cannot answer this question as I have not seen the loads document based on burn time and speed.

Drake group used info from SAE and some of layout for standardization of how layout should look came from AC.

On guidance you said no use of guidance did you mean directly or indirectly? The drake group was used which may be based on other guidance, I believe how hazards are rated are based on AC, failure rate classifications are based on FAA guidance

Niki wanted to elaborate on training early on : When I started, Mark Z was working on the SSA. He did have some background in system safety, although, I can say exactly what is was. I spent a month with him learning the process reading documentation to make sure I understood his methodology. As far as drake group, number of sit down meetings where they discussed their process that they use and work with the FAA on. If I was unsure of a logic tree they were available for help.

The interview ended at 1135

## 2.0 Interviewee: Terry Hardy, Great Circle Analytics

**Date: January 22, 2015**
**Location: via telephone**
**Time: 0900 EST**
**Present: David Lawrence, Katherine Wilson, Mike Hauf, Mike Bauer - National Transportation Safety Board (NTSB).**

Mr. Hardy declined representation.

During the interview, Mr. Hardy stated the following:

His name was Terry Hardy, and he was the Director of Safety and Risk Management for Great Circle Analytics. His background included over 30 years engineering experience in government commercial organizations, including 15 years at NASA, and 4 years at the FAA. Some of his experience included space propulsion and cryogenic fuels, software development, launch vehicle safety, human spaceflight and satellite safety and assurance. He started at the NASA research center, left after about 12 years and worked for some startup companies in software and risk management. He came back and worked with the FAA, then left and had been doing consulting work with Great Circle Analytics since 2010. In that role he provided system safety and software safety work for the government and commercial organizations.

In the FAA, he was an aerospace engineer developing hazard analysis regulations, and wrote a number of guidance documents including advisory circulars on system safety and reliability, and software safety. In 2011, he started providing consulting services to the FAA on an as-needed basis through a subcontract with ACTA, Incorporated. When he was in FAA, he was in AST 300, the group currently headed by Stewart Jackson.

With Great Circle, for commercial space he only contracted with the FAA. His other contracts were with NASA, developing hazard analysis and system safety work. His role consulting with the FAA was a maximum of about 40 hours per month, giving advice and reviewing documents, in large part trying to help the group process. He stopped consulting with the FAA on his own choice right after the SpaceShipTwo accident. When asked why he stopped after the accident, he said after 3.5 years he did not feel his recommendations or the work he did was improving the safety process. He felt that after offering recommendations to the FAA he was "spinning my wheels" until the FAA made significant changes to the way they approached system safety and their evaluations. He let the FAA AST managers know this.

In 2011, he was asked to start evaluating Scaled and SpaceShipTwo, in part because of his background and experience in developing hazard analysis regulations, and his work on the SpaceShipOne evaluation. He saw that Scaled was not meeting the hazard analysis regulations,

in his opinion, specifically the 437.55 regulation. After nearly a year of follow up from 2011 to 2012, he viewed there were few answers to his questions, and the FAA issued Scaled the permit without meeting the regulations, which was frustrating to him. There were follow up conversations and a few calls he was allowed to sit in on with the applicant. In 2013, when Scaled was up for renewal of their permit, there were many discussions with the FAA on whether or not Scaled met the regulations. The FAA eventually concurred with his conclusions that Scaled had not met the regulations from 2012, and the vehicle had flown since then without meeting the regulations. He proposed a "get well" plan for Scaled. Instead of the FAA ensuring that Scaled met the regulations, they issued Scaled a waiver. That showed that the FAA was not making sure Scaled met the regulations, and instead they just waived the requirements.

He said from 2003-2007 while he was at the FAA, there were a number of commercial space permits that came through his office, and he worked on most of them. He was tasked under the current contract to review 3 other applications and parts of those applications. His caveat was that as a contractor, he did not have access to all the safety decisions and documents, and his recommendations were solely based on the information the FAA provided him. There could be other documentation and information the FAA had that could have answered some of the questions on the permit that he had. When he was given the contract to analyze Scaled's application for an experimental permit, he was not allowed to speak directly with Scaled or any other applicants. He did have a few conversations with the applicant, but they were always facilitated by the FAA. AST 300 was the division that would facilitate the meetings.

Going back to late 2010 and early 2011, he worked primarily with Jay Naphas at the FAA, who was the system safety lead at that time, and it was Stewart Jackson who originally requested the analysis on the permit. When asked if it was typical for the FAA to contract 3rd parties to conduct permit analysis instead of doing it in house, he said for SpaceShipOne, the FAA contracted with Aerospace Corporation to do an independent analysis, so the FAA had done it before. In this case, the FAA had a limited number of system safety people, and they had a large number of applicants, and it was difficult for them to get through them all with the limited number of people and the limited experience of those people. The person leading system safety did not have much experience. Since that time, Tom Martin became the system safety lead, and he wanted his help from a workload standpoint. He said these systems were very complicated, and having only one or two people looking at them was tough. It helped having other people take a look at it. He was sure some of the management had lots of experience in the field and some did not. Some people like Jay Naphas were younger people with limited experience, compared to Tom Martin.

The process he started with when reviewing the Scaled permit was comparing it to the regulations; did they meet the regulations. He then looked at the advisory circulars. He also had his own checklist, and also used his experience having looked at hundreds of NASA reports and performing dozens of analysis. He looked for things in particular that applicants typically

missed. He also reviewed other guidance material. He found after reviewing the Scaled permit that there was insufficient evidence that the regulations had been complied with, specifically 437.55 with regards to hazard analysis and hazard identification. He found a number of hazards that had not been addressed like software and human error, design inadequacies, and these were explicitly mentioned in the hazard analysis regulations. Risk assessment also had a requirement to show risks before and risks following mitigation. The point of the process was to show that the applicant identified the risks and put in the appropriate risk mitigations, and show that risks were actually reduced. He also found that their risk mitigation measures had not been shown. Part of this was the approach that Scaled used, which was a quantitative analysis, and they did not put any risk mitigation measures in their functional analysis. The result was that the FAA did not have insight into Scaled's risk mitigation measures that had been implemented. He also found the verification to the regulation had not occurred, and the applicant had not shown they had been testing their analysis or inspections to show that the risk mitigations had been effective. Then he dug deeper, and had questions related to elements of the vehicle, and could not find information to validate that Scaled had considered various aspects of risk, particularly in software, which was his expertise from working at NASA. He had questions related to the vehicle that he asked the FAA to give to the applicant. He was very concerned with the process, that the FAA had accepted an application at the end of development. The vehicle had been built, and everything done, and then the paperwork was approved. The FAA did not have insight to what was being done during development. This was a general concern that Tom Martin and he tried to improve the process on; getting the FAA involved earlier in the process. Without that, it essentially became a paperwork exercise where you did not see the process and how the vehicle was developed. There was also pressure on the FAA to get a permit out in 120 days.

In general, he was concerned with Scaled's use of quantitative analysis for an experimental permit, which Scaled relied heavily on. Scaled's process was that they would have a top level hazard concern, then they would do a fault tree analysis to analyze that concern and come up with a quantitative number. If that quantitative number met those criteria, they were done. They did not have to document all the mitigation measures that they used. Those mitigation measures used to reduce risk were not shown by Scaled, because they felt they had done a quantitative analysis and that was enough. The idea of using quantitative analysis on an early vehicle that had never flown could be used as a tool, but should never be used alone. His concern was the data that had gone into that quantitative analysis, especially when a component and system had not been flown. They had data that could have been in environments or configurations that this vehicle would not be flown in. If you read 437, the FAA expressed specific concern about using quantitative analysis.

When the regulations were first made, Congress said to make the regulations for a license easy. It was a chance for the industry to experiment and do things that would get them to a license regime to fly passengers. They used a three-prong approach to safety: system safety, quantitative

analysis in the form of casualty analysis, and operational restrictions to keep them in an operating area. The FAA decided in the effort to make it easier for a permit since the data had not been developed, they said to not include quantitative analysis. That was stated in the preamble to 437 dated March 31, 2006, yet Scaled was an example of an applicant using quantitative analysis to justify not doing a system safety analysis.

He was not making any statement about the vehicle being high risk or low risk, since he really did not know. His biggest concern was the missing information and not having that information made it difficult in making a credible risk assessment. There was just a lack of information, and because of that he did not feel that he or the FAA could make a proper assessment from a process standpoint. The FAA used later in the justification of the waiver that Scaled was relying on the pilot's control of the vehicle, yet the FAA did not have the procedures in hand, and they had not considered human error and human factors, and it did not make sense to him that if you were relying so much on the humans than why did you not do that analysis. He said he did not see the procedures, and assumed the FAA had it, but the fact that the FAA was not even asking for it from the applicant seemed disturbing. He was sure the applicant had done a number of things to reduce these risks, and knew the pilots had procedures, but he had not seen them.

He said the FAA did go back to Scaled following his analysis, but it was limited. There were conversations in May 2013 before the Scaled renewal where they were asking questions about their application, and it was concluded that Scaled had not met the regulations. That was when they decided to do the waiver. They did not ask Scaled to update their renewal application; the FAA just went along and issued the waiver. There were some updates to the application in terms of questions and answers provided by Scaled that he thought became part of the application.

Regarding the waiver, there were 4 or 5 mitigations identified. From his previous knowledge, they were doing training and definitely had simulators. The two major ones were the operating area restrictions and the controllability of the vehicle. The FAA stated that the risks associated with an inadequate hazard analysis could be mitigated by operating the vehicle such that it remained contained within an operating area. But as he mentioned to the FAA, part 437 explicitly stated that you had to do both a system safety analysis and remain within the operating area. What the FAA was saying that if you complied with one regulation you did not have to comply with another, which he found inconsistent, and not correct. They were saying that Scaled pilots could control the vehicle so that it stayed away from populated areas. But that may not be a sufficient risk mitigation measure if a potential hazard causes and risk mitigation were not understood for events that could lead to loss of control. Just being able to control the vehicle did not mean you could mitigate the risk, for example if the pilots were receiving false information from their displays that caused them to fly over a populated area. There were a number of hazard conditions that he felt Scaled had not adequately addressed. Scaled may have had that information, but the FAA did not have it or did not provide it to him for his analysis. He said the

FAA likely did not ask for the information since they issued a waiver based on risk mitigation measures that had not been met.

During his analysis of the permit for SpaceShipTwo, he never went to Mojave. He had been there before for his work on SpaceShipOne, and was there for one of the flights as a safety inspector within AST 300. In 2004, the process changed and AST 400 did inspection duties.

All questions that came from the technical team went through a management review and were reduced in number and scope before they were received by the applicant. He did not know of any cases where AST 300 talked directly with an applicant without going through FAA management. Any questions that reached the applicant had been reviewed by FAA management. When asked why, he said "that's a really good question." In November 2004, after they had a "lessons learned" following SpaceShipOne, the team came up with a number of issues including communications that were overly strained. The FAA safety engineers were not allowed to talk directly to the applicants, and this was based on political pressures to reduce the burden on applicants. That was what they felt in 2004. What he felt now was that culture of not wanting to over-burden the applicant still remained. As a result, there was a screening of questions and a limitation on direct communication with the applicant.

He worked with various companies where there was a free flow of information, and through that there were a lot of problems headed off with the gathering of information. He felt the FAA was missing an opportunity to do that with a free flow of information. He said it was FAA management that was primarily behind the effort to reduce the regulatory burden on applicants, based on their review in 2004. He felt that it still continued.

He did not have any role in writing the waiver. There was a memo in May 21, 2013 that characterized the issues, and was an internal memo that summarized what he had in his analysis previously. He saw the waiver the first time when it was published, and he was really surprised what was written in the waiver. One question he asked was that if no human error analysis was required to be performed, how a determination could be made that the mitigations identified in the waiver would be effective. He did not know about Scaled's use of the simulator run at 1.4 times the speed. He knew of others on the technical team at FAA that had problems with the waiver, certainly the system safety folks. Another concern was the waiver had been written by FAA management and not the applicant. It seemed a little odd that the FAA was writing a waiver, and to his memory he did not think Scaled even wanted the waiver, instead wanting to show that they complied with the regulations. The waiver came from the FAA, and he had never seen the FAA write a waiver for a public applicant.

Scaled relied a lot on redundancy and failure tolerance. There may have been single point failure considerations but he was not familiar with those, other than the pilots making a mistake. He said

Scaled was concerned about the feather locking system, going back to the SpaceShipOne days, but from a mechanical knowledge he was not familiar with it.

The concerns he had with the application were voiced to Jay Naphas, then to Stewart Jackson and Randy Repcheck, then to Ken Wong, who signed the permit. Management knew of his concerns prior to the issuing of the waiver.

The wavier was renewed again in October 2014 prior to the accident. To his knowledge the waiver was extended without looking at the risks of extending the waiver regarding error accumulated over time. It was extended without additional risk analysis. There was also a memo that extended the waiver to all hazards, not just software or human error, and was issued to Scaled.

He also expressed his concerns to Tom Martin, who started in 2012. Tom was part of the waiver but not the original permit.

He participated in the writing to the regulations for the experimental permit and the advisory circular. He was the lead on writing the hazard analysis regulations. He wrote the initial draft of the hazard analysis advisory circular before he left the FAA.

Scaled used a combination of functional hazard analysis and fault trees. Scaled would come up with a catastrophic hazard and then develop a fault tree, and from that fault tree develop a quantitative analysis. If the quantitative analysis showed that for the particular hazard they met their own internal quantitative analysis criteria, then no further work was needed to access the hazard and therefore they did not need to identify mitigation measures. He did not feel that Scaled's approach was acceptable based on the regulations, and told that to the FAA.

Doing a functional analysis combined with a fault tree was totally appropriate. Those tools were fine, it was how Scaled used them and the information they provided that was the issue. When asked if Scaled should done a failure modes and effects analysis (FMEA), he said not necessarily, and with the tools they had they certainly could have done what was intended in the hazard analysis regulations.

To him, it would not have been that big of a step for Scaled to have taken the functional hazard analysis and fill in the blanks, as he suggested in the get-well plan that he wrote, and they could have described what they had done, like procedures used, design standards, safety procedures, and then took each of those and analyzed them to show how each of those were effective.

In the review of Scaled's analysis, he looked at the assumptions that were made. For example, some of the training for the pilots should have come out of the hazard analysis, and it should not

have been an assumption that it had already been done before the procedures are filled in. Also, Scaled's assumption that structure was not an aircraft system invoked a whole lot of deduction. That was a pretty rare situation, and not having structure as part of the hazard analysis was odd. Scaled apparently had done a structural analysis that had satisfied the FAA, but he was not a structures expert and did not analyze that. He knew that one concern was that the structural analysis had not been updated prior to the last flight. Scaled had identified the top level hazards, but more could have been done to describe the scenarios for those hazards.

For documentation of human error and hazard analysis, he would expect the FAA to accept fault trees and/or a separate analysis, but had not seen where the FAA AST had pushed for that. About 2 years ago he was asked to help determine what the FAA should look for since there were broad areas to be covered. He was not a human factors expert, but the FAA had a lot of information regarding human factors that he would hope the FAA would reference.

When he voiced his concerns to Jay Naphas, he did not receive a lot of feedback from him, and assumed Jay took those to his management. He was not sure what management did beyond that. He and Jay and Tom had talked about Scaled's fault trees, and generally agreed that the fault trees were incomplete. Scaled and the FAA had thought that all the mitigations had been included in the fault trees, and he found that not to be true.

For human factors analysis classifications, there were several inputs to consider from a top level. Then it came down to answering a series of questions like; if the personnel had experience, were they properly trained, was the cockpit automated, were the systems demands on the operator compatible with what they could do, system/human interface, what did the pilots need to know and what actions did they need to take. Those were also the concerns back in SpaceShipOne. Some of these items were learned through history, like at NASA where there were certain systems where one operator at a time could control a safety critical function with confirmation for a possible hazardous action.

Through his AST work, he had not seen other applicants use the same methods and assumptions that Scaled used. Many of the mitigations Scaled listed relied on the pilot making the right decision, and he questioned Scaled's reliance on the pilot alone as risk mitigation. In his experience, he had never seen an applicant make the assumption that a pilot would not make a mistake when considering hazard analysis or fault tree construction.

He did have a part in creating the 460 regulation relative to informed consent. He did a white paper on how that worked in other industries to help create that language. He did not have a role in the pilot experience requirements language of part 460.

He was asked to review the updates to the hazard analysis of the second Scaled renewal relative to software under the new fault tree. He sent a memo to FAA in August 2014 with questions for the FAA to ask Scaled, and followed up with his concerns regarding software. This memo went to his point of contact, Tom Martin. To his knowledge his software questions had not been addressed.

In March 2013, he and Tom Martin and Jay Naphas put together a set of recommendations on where the AST office should be going and what they should be doing. One of the recommendations was for the FAA to be involved earlier in the development process and have more hands on discussions with the applicant. While the FAA did have AST 500 folks on site, during the pre-application consultation process, the FAA would get the "biggest bang of for their buck" getting more involved in the development process with the applicant, otherwise it simply became a "paper exercise."

He said there was frustration with the FAA offices to define what was AST's role in evaluating these applications. Some people in AST felt the FAA's role was simply administrative and making sure the paperwork was done, while most believed AST should be more involved in the engineering evaluation to evaluate the risks to the public. That had never been made clear to those in the AST office. He also believed there should be a real evaluation on the culture at FAA to determine what safety means to them. Before he left the FAA, he wrote a safety management system document that mirrored what the safety system management system was at the FAA and recommendations for AST, but he believed that was never implemented.

He also said there were clear lines defined between AST 300 and 400 and 500, and in his opinion the communication lines between those departments seemed to have broken down.

The interview concluded at 1020.

## 3.0 Interview: Bob Withrow, Scaled Composites

**Date: January 28, 2015**
**Location: Mojave Airport conference room**
**Time: 1000 PST**
Present: David Lawrence, Katherine Wilson, Mike Hauf, Lorenda Ward – National Transportation Safety Board (NTSB); Brett Vance, Christy Helgeson (via phone) – FAA; Niki Dugue – Scaled Composites; Michael Masucci – Virgin Galactic.
Representative: Gary Halbert

During the interview, Mr. Withrow stated the following:

His name was Robert Warren Withrow, and he was 61 years old. His title was Project Engineer at Scaled Composites. He worked on several things at Scaled, and currently was the project engineer responsible for the aircraft called "old school" and was responsible for transitioning all the Tier1B assets to the customer, and was helping out with engine control on yet another project. He was also supporting the NTSB investigation into the SpaceShipTwo (SS2) mishap. He held a BSEE (Bachelors of Science Electrical Engineering). His background included working a number of years in the IT industry, eventually working for the chief technology officer at Nortel as a "technologist." He then came to Scaled about 5 years ago. He had a commercial pilot's license, single engine land, and was building a composite aircraft (Cozy MarkIV).

His roles and responsibilities as a Scaled Project Engineer varied depending on what project he was working on. On the "old school" project, he was responsible for all the engineering and flight test activities, and directed the engineering talent that worked on the project, along with the shop personnel and with the Crew Chief. He also interfaced with the customer and managed the budget. Other programs had different requirements.

Specific to the Tier1b program, over the course of the program he worked on various items. He started by working on transferring technical information to the customer. He then was responsible for the rocket motor control (RMC) on the SS2, and then became responsible for the Scaled experimental permit. He was later assigned the role of transitioning all the assets to the customer. He then became the Flight Test Project Engineer (FTPE) for the remaining flight tests on SS2.

On the day of the accident, he was an observer in the control room, and to take notes for things that could be addressed in the future. He remembered that the mission was nominal with a few nuisance items like the DAU that came up. There was a delay related to the nitrous temperature, but on the whole it was a nominal evolution leading up to the launch. The L-10, -4 and -30 checks were all nominal, and nothing stood out. There was a clean release and he remembered a nominal ignition. He remembered a call of "unlock" that came at an unexpected time. At that

time he was looking at the video display on the "big board," and saw the feather system move. He then saw the decomposition of the vehicle.

When asked what his role was in the waiver process, he said "I had no role in the waiver" and that "Scaled had not applied for a waiver." Scaled did not believe they needed a waiver in that area. His primary interactions with AST were through Michelle Murray, and a few days before the waiver was to be issued she called him to tell him the wavier would be issued. He did not know who wrote the waiver. No one at Scaled helped write the waiver, and it was his understanding the waiver originated within the FAA. He thought he got to see a draft of the waiver a few days before it was issued. He did not have any concerns about the language in the waiver since "it did not affect anything we were doing."

The language in the waiver relieved Scaled from conducting hazard analysis in two areas required by 437.55; human and software error. Scaled believed the hazard analysis they performed already covered those areas. Scaled spent a lot of time focusing on human error and software error in the program. When asked about the mitigation of using WhiteKnightTwo (WK2) discussed in the waiver and whether WK2 was actually used as an additional chase airplane on the accident flight, he said they had used it as a chase airplane. He went back and looked at their original permit application to see if there was language that discussed the use of chase airplanes, and he could not find any representation about chase airplanes. In the context of the waiver, the FAA never came to Scaled to ask them if they were using two chase airplanes. Regarding the simulator being run at 1.4 times speed, he said that they did "sometimes" run it at 1.4 times. The application stated that they would sometimes run it at 1.4. Asked when the last time he knew the simulator to be run at 1.4 times speed, he could not specifically recall. He did not believe they did that leading up to PF04, at least not when he was the flight test project engineer.

He was only involved in the development of the pilot procedures to ensure they were updated frequently. He was not involved in the content of the procedures. During simulator sessions, the Director of Flight Operations, pilots and flight test engineers could decide to update procedures. There were updated procedures between PF03 and PF04, but he would have to go back and verify what they were.

There were procedural changes for PF04 related to the new rocket motor, and they had to do with the new (b) (4) There was a rocket motor model for the simulator that was updated based on the most current data. He did not know when that was last updated. The rocket motor modeled in the simulator did model the rocket motor flown on the accident flight, he just did not know when that was last updated. He did not know the details or specifics of the updates. Scaled pilots did not ask him about the differences in the new rocket motor for either training or

the actual boost flight. He was not involved in the 0.8Mach callout, or the feather unlock procedure.

He knew that the feather locks were scheduled to be unlocked around 1.4Mach, and there was some margin built around that number as far as the forces on the feather system, and there was a 1.5Mach caution if the feathers were not unlocked. The history of the forces involved on the feather system went back to SpaceShipOne (SS1). There were documents submitted to the NTSB that showed briefings regarding the aerodynamic forces trying to open the feather system were greater than the forces trying to close them. That information was used in the design of the feather system and used in the requirements for the locks. It was well known and briefed in the FRRs. Test pilots were included in those discussions, and at least one pilot was a board member on the flight readiness review. They were required to attend and to sign off on the FRR. He did not recall who the pilot was for the FRR leading up to PF04.

He did not know if Scaled participated in data entry in the FAA/NASA Flight Test Safety Database. He did not know what that database was.

When asked if Scaled factored in pilot error in its hazard analysis, he said yes, in two ways; in their fault trees and in the methodology section of the hazard analysis, they discussed the means of reducing human error through training and procedures, and the simulator, training and procedures.

When asked for an example of a fault tree that included pilot error, he could not recall a specific function number or specific fault tree. In general, there would be a case where a pilot would be involved in responding to an action, and the probability of that pilot's action being correct would be estimated based on the workload. Different numbers were used for different workloads. None of the fault trees began with the pilot error leading to subsequent errors. The analytical tools they used started with a functional hazard assessment (FHA), and they started with the functions of the airplane and thought of all the ways that "function could fail to provide the function." For hazards considered catastrophic, a fault tree analysis was done with all the hazards that could lead to that particular hazard to assert itself. That included human error, software error, human components and so forth. They were all treated the same way.

Scaled did not make a formal response to the waiver. They certainly did not change anything they were doing. They recognized that there was a waiver and continued about their business. Scaled did not view any of the things identified in the supplemental portion of the waiver as "requirements" on their own. Scaled viewed them as things the FAA was extracting from the application materials. On the day of the accident, they had two chase airplanes; one was the Extra and the other was WK2. Scaled did not use three chase airplanes, and the FAA inspectors were the ones who ensured regulatory compliance. Scaled did not see the waiver as regulatory in

any way, but rather as a way to relieve responsibilities; they did not apply additional responsibilities. Scaled did not believe there was a requirement to use up to three chase aircraft, and it was difficult to find chase aircraft that could do so up to 50,000 feet.

There was a letter from the FAA in May 2014 from Ken Wong concerning the waiver, but it did not purport to actually be a waiver. There was no additional waiver issued that he was aware of.

The pre-application consultation was a mechanism for an applicant and the FAA can resolve issues that could impede the application process, and allowed the FAA to become familiar with the applicant, and allowed the applicant to become familiar with the FAA application process. It was a way to get a lot of those things out of the way before the formal application process began. This began in 2010 for Scaled. He and Niki Dugue worked on the process for Scaled, and on the FAA side they worked with Glenn Rizner, Michelle Murray, Ray Jenkins and other people in AST. It was a 2 year process, so there were a lot of people involved. The hazard analysis was discussed with the FAA. The assumptions in the fault trees were also discussed. He did not recall any disagreements from the FAA during those conversations. The FAA had questions about their methodologies and how they arrived at hazard probabilities, and how their hazard analysis protected the public safety. There were questions on how their analysis reported the likelihood of hazards before mitigations and how systems were being analyzed.

The tools they used were described in the advisory circular (AC) as an acceptable means of compliance. They did a preliminary hazard analysis, and the AC had a 4-step process to follow, and all their steps could be mapped into those steps. The AC stated that the functional hazard assessment tool they used was an acceptable means of compliance. It also cited other aviation references they used, like AC 23.1309 for system safety analysis.

When he referred to "the customer" he was referring to TSC, The Spaceship Company. They started with a functional hazard assessment, and looked at how those functions could fail to be achieved. For certain ones of those that were sufficiently severe, they used fault tree analysis, and those included human error and software error. They used the fault tree analysis to determine the severity of all the causative ways that function could fail as described in the hazard analysis. He was familiar with AC 437.55-1 and had read it several times. They addressed the human errors identified in the AC through the analysis in the fault trees, and also through the hazard analysis where they used more general mitigations like training, simulation and procedures. He could not remember any specific human errors identified in the fault trees. Regarding the hazard analysis capturing a pilot action at the wrong time, he did not know there would be a statement that mirrored the example in the AC. He was not aware if Scaled had used any outside source references for human error modeling.

The hazard analysis included a pilot failure of a task through the fault tree. His belief was that the tools Scaled used met the requirements in the regulation, and was covered in the hazard analysis and their mitigations.

He was involved in the AST inspections prior to the PF04. The inspectors attended simulator sessions and briefings. They inspected pilot and vehicle maintenance records. That started about a week before launch. He never saw the FAA's inspection checklist, and only facilitated the FAA in completing their checklist items. He did not know if the waiver items were included in their checklist, and there was nothing in Scaled's checklists related specifically to the waiver. In his role as FTPE, he just made sure that the Director of Flight Operations said the crew was ready. He could not recall if there were any details regarding 460 in the pre-application process.

He did not know the chase airplane they used for PF01. For the permit part of the application, there was a series of 460 requirements that needed to be ensured were complete. His role was to verify that those things had been done. For PF04, the timeline was based on completion of those requirements. He did not recall the specifics of the delay due to the nitrous temperature or DAU issue.

For the simulator sessions, they would have a briefing prior to the simulation covering checklists, simulator status, and general areas. They would then debrief after the simulator sessions. For use of the 1.4 simulator speed, he could not recall what phase that would occur in.

He was the project engineer on another airplane. He was appointed in 2012 and had conducted 166 test flights and 400 hours on that airplane. An experimental permit was to conduct testing on a new craft, conducting new crew training, and to show compliance to obtain a launch license.

AST never "tolled" their application, and Scaled never asked for one. Early in the process, they delivered to AST a draft of their application. There were questions and answers covering a variety of issues including containment area, and part 460. He did not recall the FAA telling Scaled there were unresolved issues during that process.

In their terms and conditions, Order A covered basic conditions Scaled was allowed to exercise their permit like safety zones, pilot flying etc. Order B was a financial aspect that required them to carry insurance. The terms and conditions did not mention the waiver. The terms and conditions changed after the 1st application and the 1st renewal, and then they basically stayed the same. Scaled had renewed their permit twice, and there were three modifications, two of which were concurrent with the renewals. There were a lot of questions from the FAA for the 1st renewal, as with the 2nd renewal. There was no expressions from AST of deficiencies.

Scaled did not have any input into the AST waiver process at all.

The goal of the hazard analysis as required by the regulation was to protect public health, safety and property. The hazard analysis process focused on the safety of the vehicle and the safety of the crew, based on their background as an aviation company.

When a fault tree was initially created, Scaled would use a conservative number, 1/1000, for the components in the system. That number was picked because it represented the worse that could be imagined. By using the conservative number, if the system met that criteria it would be considered "robust" and it did not rely on the failure probabilities of the things you were analyzing. If the system met the requirements, you were done. Otherwise you would look further at the system and redo the analysis. Scaled used a database of components, and matched as closely to the component on the SS2 and used that probability number.

The Scaled fault tree analysis had software error in it, and the body of the hazard analysis described how the software was developed and the mitigations used. The rocket motor controller was a safety critical item on the vehicle. The fault tree analysis showed the rocket motor controller software as a point of failure.

Scaled considered structure as safety critical. They had a separate means to analyze a structure different than a system. In the AC 23.1309, it described the techniques to identify what was structure and what was a system. That AC was also mentioned as guidance in AC 437.55-1.

Scaled cooperated with AST. There was never a timeline given to him to answer AST questions by AST, though during the application process they had a week goal to answer AST questions. Most of the questions from AST came either as formal written questions or during technical interchange sessions, which were essentially free-form information exchanges. Those meetings were on a weekly or bi-weekly basis. Technical meetings were topic specific and scheduled with AST. Scaled provided formal written answers to the formal written questions. He was not aware of any issues not resolved or heard of questions posed to Scaled from AST that were filtered.

In his opinion, all piloted vehicles had human error as a single point failure. The tools they used for a specific scenario with a human action applied probabilities to the action. Challenge-response protocol was not a risk elimination means.

He never worked as a flight test engineer prior to Scaled. He came to Scaled in November of 2009.

During the initial application process they received 25 question packages from AST. He did not know the exact number for the renewals, but it was not as many.

He thought the pre-application process worked well, and had no recommendations for improvements.

His role differed depending on the project. On Tier1B, he was new to the role. As a flight test project engineer for Tier1B, he focused on "all the stuff that had to get done, got done." He conducted flight test planning meetings to discuss contents for the flight test card. He recalled that they held a flight test planning meeting for PF04, and did not recall a discussion of why the feathers would be unlocked.

When asked about his physical reaction, in the control room for the accident, he heard the unlock call being made, then saw the feather begin to move, and knew the outcome would not be good.

He did not recall the details of the fault tree for the uncommanded feathering. He recalled a note gate that said "feathers are unlocked" and the intent was that the feathers had been unlocked on schedule during the boost phase. It did not mention specifically during the transonic region, and that was based on the assumption that the feathers were already locked, and did not consider an unintentional unlocking of the feathers. It was always known that you did not unlock the feathers during transonic.

He said the best thing to say about the fault tree was that it was incomplete, and there were other fault trees that were similar. Part of the fault tree should consider flight phase after 1.4Mach, and another that should consider transonic. When asked if he had any mitigation recommendations for the early unlocking of the feathers, he said it was an interesting discussion since, early in the glide flight program, they had a situation that required the pilot to unlock early to recover the vehicle. It was something that should be looked at, but he was worried about the consequences of any mitigations.

He was part of most of the simulator sessions for PF04. The transonic unlocking of the feather system in the simulator was not modeled, and it never happened in any simulator sessions he attended.

He thought they had a cordial working relationship with the FAA.

The unlocking of the feather system was derived from the SS1 program. The issue of the transonic region was discussed in meetings, and was covered in the POH (pilot operating handbook), Emergency Procedures (Eps), Normal Procedures (NPs), and Cards. There was also the normal expectation that pilots would be very familiar with the vehicle, and would discuss these things with other pilots.
He did not remember who came in to do safety inspections prior to PF04. It used to be Dave Gerlach.

A single point failure would be a failure that alone would cause an outcome. When asked if there was time to recover from an action, would that action be considered a single point failure, he said he would have to think about that.

He thought the POH said something in the EP section about feathering above 200KEAS could be catastrophic.

His percentage of time he worked on Tier1B would vary based on the various projects he had. If they were between powered flights, the majority of his time would be on other projects not related to Tier1B. Over the course of the past year, his workload varied a lot.

He did not recall any discussion about changing the waiver. The letter from Ken Wong in May 2014 he received from the FAA simply said there was a waiver, but the letter did not purport to be a waiver, so they did not make any interpretation of the letter at all. There was an October 2014 letter addressing the modification.

The interview concluded at 1135.