

Flight Test *Safety* Fact



Published for the Flight Test Safety Committee

In This Issue

- EASA issues VTOL Means of Compliance Proposal** – a conversation starter for sure
- vFTSW Trip Report** – You know what a “trip report” is: Pete Donath shares his notes
- Chairman’s Corner** – observations about flight test safety that are out of this world
- Subscribe to our Podcast** – Turbo interviews a special guest in this month’s podcast

EASA issues VTOL Means of Compliance Proposal

On 25 May, EASA published document number MOC SC-VTOL Issue 1, “Proposed Means of Compliance with the Special Condition VTOL” on their [website](#).



European Union Aviation Safety Agency

Comments are due by July 24, and I hope our readers will take time to look it over and, if possible, provide input. The document is 85 pages long, so I know it’s a big ask. At a minimum, reading it will provide you with a grasp of some terms that may begin to make their way into the vernacular, because it begins to provide a shared taxonomy for this evolution of aerospace

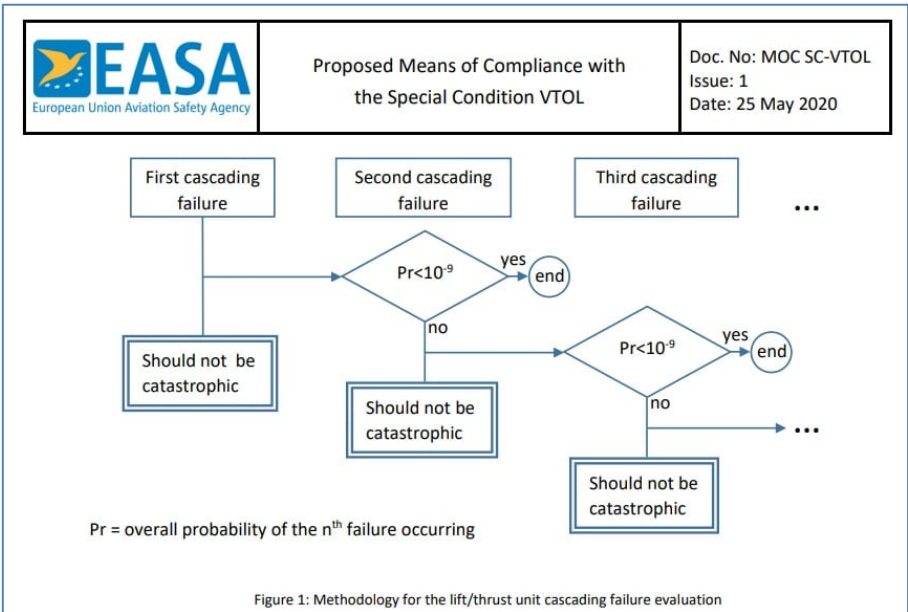


Figure 1: Methodology for the lift/thrust unit cascading failure evaluation

technology. Several things caught my eye—probably because the news article I read published this particular image—and I wanted to discuss them here. **Lift/thrust unit** is the new term that EASA has given to the unique configuration of components that provide thrust and/or lift and/or control. In fact, this MOC completely replaces the terms “engine,” “turbine,” “powerplant,” and “rotor”—whenever referencing the existing rules and regulations—with the new term, *Lift/thrust unit*. This document, the Proposed MOC complements a previous document published by EASA, the Special Condition SC-VTOL-01, but I think you should read the MOC first..

Why are we here?

I can't answer that question in its entirety, but I will explain the purpose of this particular column. The timing of this EASA document was serendipitous. Its publication coincided, loosely with several other things happening in the aerospace community and industry. Therefore, this column has the following three main goals.

1. Alert readers to its publication and recommend review.
2. Inform readers of relevant news at the intersection of flight test safety and VTOL.
3. Investing in the technical development of readers: Specifically, talking about probability and how we *update our beliefs about probability* when accidents happen. So let's see if we can get this conversation off the ground.

Two Categories of VTOL

EASA has defined two distinct categories for VTOL certification: Category Basic and Category Enhanced. (See Special Condition [SC-VTOL-01] for a precise definition.) Loosely speaking, there is strong correlation between Part 23 and Category Basic, with a similar analogy between Part 25 and Category Enhanced. Certainly, we can conclude that they intend a higher standard of design safety for commercial operations. I mention this because the flow chart above applies to failure of a lift/thrust unit for Category Enhanced VTOLs.

The Flow Chart

The flow chart in Figure 1 above states: **A failure of any Lift/thrust unit should not be catastrophic.** That seems fair. It's the second column, “Second Cascading Failure,” that probably means something different to the average reader, something we should pause to truly consider. EASA explains their reasoning for the flow chart this way: “Due to the distributed propulsion, the failure of a lift/thrust unit may, for some architectures, potentially cause other lift/thrust failures in a chain reaction” (page 25). According to this chart, if the first failure is the beginning of a cascade, then the second failure should have a probability of less than 10^{-9} per flight hour (or not be catastrophic). It's important to really consider what this means.

What is $Pr < 10^{-9}$?

Most of us have a hard time comprehending, really understanding at a visceral level, what this means. Let me try to describe it in a more meaningful way: There are 60

seconds in a minute. Likewise, there are 60 minutes in an hour, or 3600 seconds. If we continue multiplying in this way, we find that there are 3×10^9 seconds in *one hundred years*. When I first sat down to perform this estimation, my intuition suggested that I would get to the desired order of magnitude in a single year. I was waaay off. This demonstrates, I think, how our intuition is ill-equipped to consider problems of this magnitude (and their inverse). The probability in question, from the flow chart, means that the chance of this failure is 1 in 10^9 flight hours. That's more than 100,000 years worth of flight hours. Our first goal is to understand how enormous this number is, or how very small the probability is, and I think this illustration helps.

The reader may object immediately to the illustration above, with the caveat that the probability should hold for the whole fleet. This is true, but it does not change the sheer magnitude of the number, which was the first goal of the illustration. As Pete Donath pointed out, "Yes, even if they make 8,000 VTOLs, that's still a lotta' flying hours per frame, and these don't do the 14 hour flights like the long haul jets. My sarcastic FTE remark is: 'When a design engineer tells me it's ten to the minus nine, I'm only going to see it happen three times in the first thousand hours of test.' But the good news behind that is we (Flight Test) help find deficiencies, and the design gets better." I laughed out loud when I read his sarcastic comment, but I think he hit the nail on the head—there's some truth in that statement that we may not have time to discuss. (The ambitious reader should consider reading up on exponential and Weibull distributions.)

What is a Catastrophic Failure?

The second way to exit the flow chart is to assess that the failure is not catastrophic. I don't want to spend a lot of time discussing definitions of these terms, but my question is this: How well do we imagine the outcomes of these failure modes? For example, were you aware that Kitty Hawk had a software "timing error" with their Heaviside VTOL? That sounds innocent enough. The operator had failed to disable a battery charging script at the ground control station prior to flight. Neither one of those things sounds catastrophic, but the aircraft did, in fact, crash. The [NTSB determined that software was the cause](#).



Kitty Hawk photo

On the subject of software, one editor said this: "One central challenge is that software is embedded in many elements of the complex system making up the control system of any modern air vehicle. But, here's the big hitch: Software doesn't fail. It always does exactly what the compiled code tells it to do." I will happily admit that this is not my area of

expertise, and furthermore, I may not know the precise way to parse my language on this topic. Nevertheless, I think we agree that software, and its bugs, may contribute to the failures described in the flow chart.

I did some research, in an attempt to answer some questions about software reliability, but I came up mostly empty. I did find some academic/instructional material on the topic but nothing practical. The closest I came to something we might recognize is the NASA Software Assurance program and supporting documentation. They have very specific and thorough requirements for a Software Assurance program, especially in the case of manned spacecraft. They do not publish probabilities or reliability requirements—at least none that I could find. Boeing’s recent Starliner flight test should remind us that software bugs are a very real possibility. One reporter suggested that they [narrowly missed catastrophic failure](#). In any case, to complete my investigation into software failure rates, I appeal to the readers—do you know of any experts or authoritative references on the topic? One reader suggested DO-178C may have the answers, but at press time, I hadn’t found a way to access the document.

Minimum Acceptable Handling Qualities Rating (MAHQR)

The second item that really caught my attention, was the computation of probabilities related to MAHQR. The document’s Table 2 illustrates the discussion about the Flight Conditions required for Handling Qualities assessments. They define a method for computing the probability of a given flight condition as $X_{FE} \times X_{FC} \times X_{AD}$. This is mostly jargon, but the important point is this: Multiply the probability of a Flight Envelope (FE) times the probability of a Failure Condition (FC) times the probability of a Atmospheric Disturbance (AD). For those who have forgotten, they are saying $P(A \text{ and } B) = P(A) \times P(B)$, but this is *only* true when the events are independent. It is unfortunate that “independence” is such a nuanced topic, but let me try to illustrate.

Consider, for example, the [flight of a business jet into severe turbulence](#) (which is what EASA means by Atmospheric Disturbance [AD]). Do we believe that an aircraft in severe turbulence is more likely to suffer damage or other failure modes? I recommend the article above, because it will inform your intuition and help you answer the question. The simple fact that an Atmospheric Disturbance (AD) like severe turbulence may increase the chance of a Failure Condition means they are *not* independent. I believe that EASA knows this, but the ensuing discussion about how to “adjust” seems too vague. I’m not certain that a manager who has to approve the risk could understand it. It is, however, a technical nuance that we need to remember with sufficient familiarity, enough to make us ask someone to explain it, when necessary. I would also point the reader to the pilot’s description of Handling Qualities in the report of the Heaviside crash as relevant to this portion of the description as well. That crash and the wake turbulence event above should also inform our ideas about the frequency (or probability) of these kinds of events, and they might even give us a way to update our beliefs about probability assessments.

Updating our Beliefs

As we close, I want to plant the seed of discussion with one more question. How do we update our beliefs about probability when we gather new data, learn something new, or witness an accident? Knowing how to properly assess the information in that event is the subject of an entirely different column, but it is an equally important one.

We haven't covered much of the EASA Proposal, but I believe that what we have covered should make us all pause before we gloss over exponents and quantitative criteria for safe system design and lead us to the following conclusions.

Conclusions and Recommendations

Every good flight test document has a section with conclusions and sometimes a recommendation or two, so I provide mine here. I recommend that you read the document in order to:

1. Learn about an approach to VTOL certification.
2. Review the proposal and provide input by July 24.
3. Familiarize yourself with the growing vocabulary.
4. Grow as a flight test safety professional.
5. Brush the dust off your probability knowledge and skills.

I hope you will glance over the document and reflect thoughtfully on your intuitions about chance and statistics. I believe the short discussion here will dovetail nicely with Animal Javorsek's paper (next time) which references Brownian motion and its analogy to accident investigation and safety management. I also hope this column helps you sharpen the saw of our quantitative reasoning, a task we must return to regularly and humbly as we gain in qualitative experience in our careers. *Mark Jones Jr.*

Trip Report – the vFTSW

Pete Donath

The 2020 Flight Test Safety Workshop, planned for Denver, Colorado, was derailed by the 2020 COVID-19 pandemic lockdowns. The Flight Test Safety Committee shifted to a smaller, shorter two-day webinar format, hosted online with Zoom on May 6 & 7, 2020. It was far from “workshop-lite.” Instead the subject matter was hard hitting and engaging.

FTSC Chairman Tom Huff led off with a review of Flight Test accidents and incidents in the recent past, and then set the stage for the STPA and STAMP presenters. They were honest and upfront: STPA is not going to replace some of the valuable safety processes we've come to love (or hate): STPA is another tool in our kit, and it has the potential to make us safer and better at what we do.

Col. Wickert acknowledged that many Flight Test Organizations are “pressured” into accepting greater risk. He pointed to STPA as looking for ways we could experience

“loss of function,” be it performance, control or other aspects of flight test. Some organizations are using the STPA process model for scenario planning, and catching more ways that things can “go wrong” in flight test.

Several presenters acknowledged the “business” resistance to adopting STPA and STAMP – our organizations have already invested in the 2-D risk matrix, Fault Hazard Analyses and Fault Tree Analyses...why should they pay for training and standing up a new system? Clear examples were given as to why FHA’s & FTA’s are not really well suited for flight test – especially with the recent explosion of complexity to our systems and the various system interactions. My takeaway is that applying the STPA analyses (especially well thought out “control structures”) will help us reveal more ways our systems can break down and this may help us (flight test) flush out more failure scenarios. While it’s good to be aware, it adds burden to the flight test function, already overtaxed and behind schedule.

Ideally, design organizations would add these analyses to their system safety analysis processes; it was observed that flight test organizations put systems through extreme and unusual scenarios, and as such we have ways of looking at use of systems a bit different from the designers. As presenters commented that design should invite flight test to “the table” earlier and more often, I added my \$0.02 saying we flight testers need to invite designers to our world a little more often, so they get a better appreciation of what and how we do our work, build goodwill and a track record that shows we ADD value to the program, in contrast with the program manager’s typical view that Flight Test is a cost sink at the end of a program. We agree, getting testers involved earlier helps flush out problems earlier and more cost effectively.

We had homework, trying our hand at the STPA process for an event we’ve experienced: Dr. Thomas walked through a good example on the second day. Major Summers provided some more STPA background and pointed out that we could use STPA to inform our traditional Safety Risk Assessments (e.g., Test Hazard Assessments).

FTSC Chairman Tom Huff wrapped up the workshop with an excellent reminder that what we do applies well beyond our job titles: “It’s not just about testing safer, it’s about making safer products.”

Chairman’s Corner *Tom Huff*

Testers, I hope this June edition finds you healthy as we begin summer and hopefully some level of normalcy. Just a reminder, we continue to add COVID-19 guidance material to the website: <http://flighttestsafety.org/web-links>. We welcome resource documents that might aid in developing or refining SOP or CONOPS for resumption and sustainment of safe operations. As I pen this, I was hoping to highlight that we had successfully launched two of our test brothers to the space station, resuming space

exploration from American soil. I can only imagine the pressure to hold the line on acceptable launch weather which will only increase for the next attempt. The live feed images were captivating. The professionalism was evident with the precision and cadence of the team, yielding an “all systems go” just minutes prior to the abort due to uncooperative atmospheric conditions including lightning proximity. I’m proud to know two extraordinary flight test engineers for SpaceX that I’m sure are unwavering on safety. Although lots of disappointment in not “lighting the candle” on this first attempt, it was a positive for test discipline and safety!

I was also pleased to see Virgin Orbit test: successful LauncherOne carriage, release and ignition prior to booster shutdown following an anomaly. Despite this test failure, it appears the team succeeded in proving the safe mating of the LauncherOne vehicle to Cosmic Girl, the effective liquid oxygen fueling/containment system, and an executable launch profile. Media reports suggest that the extensive data acquisition system functioned well and captured significant data to enable root cause determination. Unique high-risk testing done safely...check.



Virgin Orbit photo: <https://virginorbit.com/mission-recap-our-first-launch-demo/>

The virtual Flight Test Safety Workshop is in the books. I was thrilled to see the interest in Systems Theoretic Process Analysis (STPA) with well over 500 registered. The high watermark was 407 attendees joining the webinar, and we maintained at least 300 through conclusion on day 2. Thanks to all those that tuned-in and engaged in active learning with our august group of expert presenters including Dr John Thomas, Col Doug Wickert, Maj Sarah Summers, Fred George, Ben Luther, and Capt Shem Malmquist. Our very own Susan Bennett earns major props for her tireless coordination and management of the webinar platform. We are finalizing the recordings from both days so in case you missed the live program, you will be able to view the sessions soon at flighttestsafety.org. The preponderance of the feedback was very positive, and there appeared to be high interest in further tutorials on STPA. The Committee is investigating opportunities later this fall. In the meantime, I recommend checking out the Flight Test Safety Committee podcast channel for an upcoming episode that includes an interview with Dr Nancy Leveson of MIT. She is the mastermind behind

STAMP/STPA and shares some great insight into the history, effectiveness and adaptability of these frameworks.

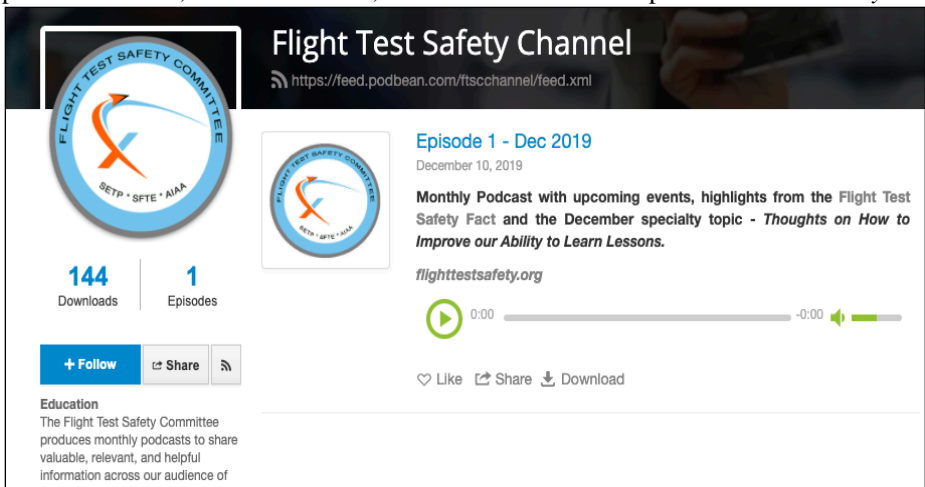
As always, we seek your suggestions and feedback on the newsletters, podcasts and workshops. We build the programs based on interest and needs expressed by the community. Please help us by sharing and discussing/debating the topics. Launch an air mail to chairman@flighttestsafety.org.

In your service,

Tom Huff

Subscribe to our Podcast

This month you will hear Turbo interview Nancy Leveson, the brains behind STPA. If you still don't know what STPA is, listen in. While you are there, please subscribe to the Flight Test Safety Podcast on the [Apple](#) or [Google podcast app](#). You can also navigate directly to the recording in [a web browser](#). You can leave comments on these platforms. Last, but not least, tell a friend: Help us *Reach Everyone*.



Flight Test Safety Channel
<https://feed.podbean.com/ftscchannel/feed.xml>

Episode 1 - Dec 2019
 December 10, 2019

Monthly Podcast with upcoming events, highlights from the Flight Test Safety Fact and the December specialty topic - *Thoughts on How to Improve our Ability to Learn Lessons.*

flighttestsafety.org

0:00 ————— -0:00

Like Share Download

Education
 The Flight Test Safety Committee produces monthly podcasts to share valuable, relevant, and helpful information across our audience of

Contact Flight Test Safety Committee

Tom Huff, Chairman

chairman@flighttestsafety.org

Susan Bennett, FTSC Administrator

susan@setp.org

Society of Flight Test Engineers

edir@sfte.org

Society of Experimental Test Pilots

setp@setp.org

AIAA Flight Test Group

derek.spear@gmail.com

Contact *Flight Test Safety Fact*

Mark Jones Jr, Editor

mark@flighttestfact.com

Website: flighttestsafety.org

Podcast: ftscchannel.podbean.com/

Connect with us by joining the LinkedIn Group: “Flight Test Safety Committee”