July 2022

Flight Test *Safety* Fact

Published for the Flight Test Safety Committee

In This Issue

Risk Matrix Alternatives: Cyber Case-Study

Dr. Brian Mork

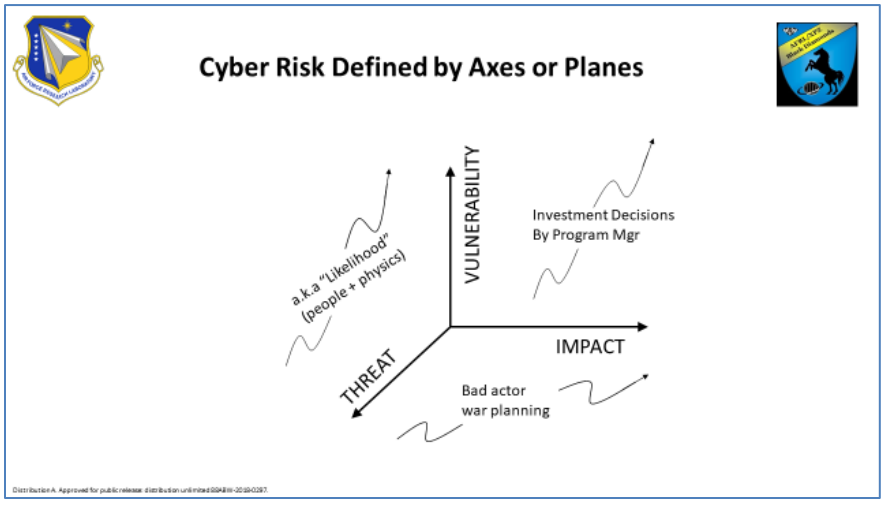
Risk assessment tools should match the underlying reality model they're applied to. Ben Luther's piece in Vol 1 No 5 of Flight Test Safety Fact (issue 19-06) highlighted that the traditional 2D risk matrix represents a certain model. He encouraged testers to consider alternate tools that are useful in other circumstances.

Cyber risk assessment of weapon systems has a different underlying model than traditional test programs, so the 2D model isn't the best fit for risk assessment of cyber test programs. Unlike risk associated with aircraft aero-mechanical or control failures, cyber risk models must include intelligent adversaries. A good cyber risk model is composed of 3 parts – what "we" do, what "they" do, and the impact – concisely, Vulnerability (V), Threat (T), Impact (I). These 3 metrics are sufficient (all is captured), necessary (nothing extra), and orthogonal (each metric can be independently adjusted). For more detail about this model's foundations and usefulness, see "3-Dimensional Cyber Risk Model" in the March 2020 issue of the ITEA Journal.

The 2D tool doesn't work well if force-fit over a 3D reality. Some people roll Threat & Vulnerability together, call it Likelihood, and press with the 2D tool. However the convolution is problematic for acquisition Program Managers because controlling "likelihood" of China, Russia, North Korea, or whoever doing something is way beyond the scope of a weapon acquisition program. As an analogy, if you're changing sizes of spheres, you should work in spherical coordinates where radius is an explicit parameter. You could buy down a sphere's radius by adjusting x, y, z of a Cartesian measurement system, but it's unnecessarily complicated to use the wrong model.

In 3D coordinates, the volume of the box defined by the origin (0, 0, 0) and the point defined by (V, T, I) represents magnitude of risk. This is analogous to the area captured on the 2D matrix: more area defined by your risk point, moves you from green, to yellow, to red. Like the 2D chart, if any of the 3 cyber axes are zero, there is no risk.

And...the 3D model is useful: In 3D space, the projection of the risk vector on each of the three planes introduces management metrics that the 2D matrix does not offer. At least 4 different communities are served.



Projection on the VI "Investment Decisions" plane has no contribution of a threat actor. No matter what the threat is, the risk can be reduced if the vector projected on the VI plan can be shortened. That is the regime of the PM and engineer to design the vulnerabilities out or make the impact innocuous. For example, RMF controls by designers could lessen the vector length.

The TI "War Planning" plane captures the interplay of operators and aggressors – the realm of tactics and procedures used to shorten the projected vector by lessening the impact no matter what the threat brings to bear. RMF procedural controls could also lessen the vector length. It's too late to bake-in lack of Vulnerabilities, so that parameter is not relevant to these actors.

The TV "Likelihood" plane is the realm of strategic war planners, and simulations, which can help prioritize blue system vulnerabilities for elimination in the fact of increasing red force threats, or geopolitical landscapes.

Lastly, to the flight certifiers and authorizing officials, the overall program reduction of "risk volume" or the shortening of risk vectors is documented by the changing volume or shape of the cube.

The 3D risk model isn't perfect. Like the 2D matrix, it's a challenge to put engineering units on the axes. However, considering the change from traditional engineering threats of the 1960s, the cyber landscape is different enough that we should consider a 3D alternatives to the 2D risk matrix.

You can contact the author: Dr. Brian Mork, services@increa.com. *Brian spent 12 years teaching at USAF Test Pilot School, and is a life-time member of SFTE. At the Air Force Test Center, he spent years as a civilian involved with flight test before moving to a job at Air Force Material Command. The cyber risk model presented here was first thought of during a tour with the Air Force CROWS (Cyber Resiliency Office for Weapon Systems).*

Flight Test Safety Workshop Recap

Mark Jones Jr., Editor

It was evening when I arrived in Palm Beach Gardens, and the hotel bar already had a crowd of people wearing polo shirts with various logos that suggested their shared purpose. On my way to the elevator, I passed a friend on his way out the door for a workout. We smiled and made a promise to catch up the next day—this is exactly the kind of thing I had hoped would happen and one of the singularly distinctive benefits of the event. The Flight Test Safety Workshop kicked off the next morning, May 3, and it included introductions from the Sikorsky team that organized and hosted the Workshop.

Opening comments also featured the typical annual report from the Chairman of the Flight Test Safety Committee. Turbo conducted a quick poll of the crowd, and we determined that we still need to Reach Everyone. Specifically, there were people in the audience who had never heard of the newsletter or the podcast. This anecdote illustrates not only the meaning of the phrase Reach Everyone but also the kind of ecosystem we intend to cultivate at the Workshop. Those who know about the in-person events have the chance to learn of new media for communication. On the other hand, those who subscribe to the newsletter or find a printed copy in the office break room may learn about the podcast, the in-person events, and the website with its myriad resources.

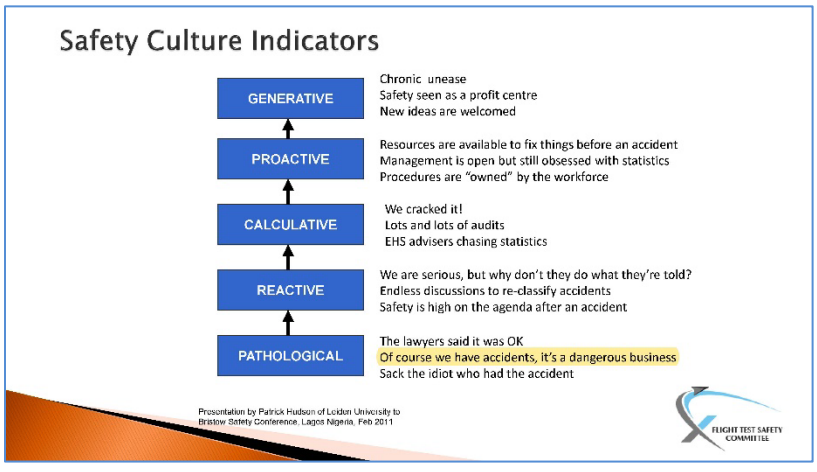
When I found the original column that articulated the specific goal to Reach Everyone (FTSF 19-12), I noticed that it was also the first edition to discuss AI in flight test. It's probably time to bring an update on that particular tech domain, but this workshop focused those in attendance on something timelier and more timeless than tech. It focused us on the humans in the cockpit, control room, and cubicles. The opening session centered on culture, a word that we reap from the agricultural age rather than the current technologically dominated era. Though most of us will not likely remember the definition we heard about culture that day, I would like to suggest that it boils down to two things: 1) what happens when one individual bumps into another and 2) how we describe the aggregate characteristics of a group of such individuals. If you need a formula, I would suggest Attitudes x Behaviors = Culture.

The topic sparked a healthy conversation that was both enthusiastic and surprising. One of the things that surprised me most was the stark contrast in opinions about how to measure safety culture. One group insisted on numerical metrics or quantitative analysis of the culture. Another group insisted that numbers were not helpful here. Even more surprising was the discovery that someone who ascribed to quantitative metrics for something fuzzy like culture was just as adamant about subjective probability.

As I tried to soak it all in, I made a note that we were talking about people, not planes, and teams not tech. This shouldn't be a surprise. Jerry Weinberg, who was a computer scientist in the early days of the space race, said this about the nature of technology and humanity:

> Back then, our failures all seemed to be programming problems, technical errors in code. So, that's what I wrote about. As time went by, we had more programmers, more and bigger projects, and though the technical problems remained, we could usually find a large number of people who could solve them. But, with bigger and more complex projects, we began to see that human failures were increasingly frequent, and more serious. At the same time, none of us technically trained people had much training or instinct for solving those human problems.

No matter the era, humans and how they interact is important. That's also true about the information shared from this workshop. We need to interact with it, and we believe you will benefit if you interact with it. To that end, videos of the sessions and slides from the workshop are available for your use on the FTSC webpage, http://flighttestsafety.org/2022-palm-beach-gardens-fl.



While you are there, I highly recommend the presentation by Dr. Rob Niewoehner, USNA: Intellectual Virtue Grounds Sound Organizational Culture. Within just a few moments, he had captivated the crowd, and he quickly established his thesis: "Intellectual virtue provides the greatest leverage we have over intellectual performance." I only wrote down five of the Intellectual Virtues, but beside everyone was a phrase that cut to the heart of the matter. Who among us doesn't need to be reminded that "I might be wrong," the hallmark of Intellectual Humility. Niewoehner delivered the talk with the expertise of a seasoned professor and the humility of your next door neighbor. Perhaps that's what made the challenge so profound, so powerful. I highly recommend it (again).

Turbo Talk – Chairman's Corner

Art "Turbo" Tomassetti

This is our first newsletter since meeting in Palm Beach for the Flight Test Safety Workshop. It was great to see familiar faces and new faces attending. I want to thank everyone who contributed to making it a success which includes those who attended.

One key to success of the workshop is having meaningful content, but more important is having people there to hear it, to share their thoughts and to engage in discussion, because those people go back to their teams and share that experience and that knowledge. That dynamic is *kinda* what our mission is all about.

To promote flight test safety and continually improve the profession's communication and coordination.

The world of Aerospace continues to expand, presenting new opportunities, new concepts, and of course new challenges. We need to do what we can to keep pace with those changes. To ensure that we make our tools and resources available to those who might benefit from them. To seek out new tools and resource relevant to these new developments, new technologies, and new frontiers. And "TO BOLDLY GO WHERE NO ONE HAS GONE BEFORE" imagine that in a booming echoing voice followed by theremin music. (Trekkies know what that is). Sorry couldn't resist that.

As the chairman and with the help of the Committee, we will continue to look for opportunities to do more, but we need your help. We have a lot of experience, knowledge, and talent, on the FTSC, but there is more knowledge and expertise out there. We want you to share your lessons, your successes, and even your failures. From those we all can learn, we all can improve, we all can succeed, and of course, we all can be a little safer. A great example can be found in the June podcast where you can hear how flying club in Oregon does safety.

Until next time: Be Safe, Be Smart and Be Ready. **Turbo**

Subscribe to our Podcast

Flight Test Safety Committee Podcast Channel - EP31 - How Do You Do Safety?

This month I spoke with Steve Bush and Stan Swan from the Columbia Aviation Association (CAA) and talked about one of the approaches they have to improving flight safety. You can learn more about the CAA here:

Home - Columbia Aviation Association (caapilots.com) https://www.caapilots.com/content.aspx?page_id=0&club_id=63452

Available on iTunes, Spotify, Podbean, Google Play, and Amazon Music: FTSCChannel
Podcast: flighttestsafety.org/ftsc-news/flight-test-safety-podcast-channel

Contact Flight Test Safety Committee

Art "Turbo" Tomassetti, 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

Connect with us by joining the LinkedIn Group: "Flight Test Safety Committee."