**Question:** That is a false statement. The SAE 4761 process includes flight crew identification and reaction to failures and abnormal conditions, and includes Human Error Analysis. Western civil airplanes have been designed to preclude the Moscow scenario for decades because current methods DO find those cases.

**Response:** Sorry, but I think the A320 is a western aircraft. So are the defense aircraft that have had the same thing happen. It is not just a Russian problem. And these types of problems are causing accidents in Western civil aircraft. Note that there were no failures and the crew could not have done anything in this case (or in the others where there is no ability built in to override the software).

I am very surprised by this statement about SAE 4761 including a Human Error Analysis. I am on S-18, but I attend less than my colleague Dr. John Thomas. I checked this response with him and he agrees with me along with both the authors of 4761 and the FAA. 4761 does not include a human factors analysis. The closest it comes is a column labelled "effect on crew" in the FHAs (where they write down best-case outcomes) and a box for "pilot error" in the fault trees. So one could say that it technically doesn't completely ignore humans, but even the authors agree that it does not provide an analysis of human factors. In the FHA, the effects on the human are only used to mitigate any potential safety effect.

In an FHA example provided in the 4761 standard itself, if the brakes fail while in taxi mode and the brake failure is annunciated to the crew, it is assumed that the crew will be able to safety steer the aircraft onto grass and stop it safely. That assumption leads to a result that says that annunciated brake failure has "no safety effect" and can be ignored in the airworthiness certification. That's what I mean by a "best case analysis." However, it seems easy to imagine a (worse case) where the pilots cannot "save the day," for example, if the aircraft is headed toward the ramp, there are baggage and other cars and people on either side of it (so the pilots cannot steer it away from the ramp), and the brakes fail. There is not much the pilot can do in that case (and it actually has happened, e.g., a Continental aircraft plowing into and through the terminal wall).

And putting "Pilot Error" in a fault tree box is also not a human factors analysis. So even the authors of the standard, the committee charged with maintaining it, and the FAA all agree that it does not provide an analysis of human factors. A human factors analysis is accomplished by a different FAA-approved standard and concentrates only on the humans (and their controls and displays) but not the total integrated human-physical system. It is not in 4761.

**Question:** In the Warsaw Accident of Reverse Thrust Case, how was 'Landed' defined for the Process Model? Was wrong definition the causal factor?

**Response:** The problem was a “missing case,” which is a standard problem in system and software engineering. The weather factors at the time were very unusual. There was a heavy rain, leading to a lot of water on the runway and hydroplaning of the wheels. There had been a windshear warning from the pilots landing earlier, so the pilots followed the directions provided by the manufacturer for landing with windshear, etc. Taken together, the “cues” provided to the software for being on the ground (e.g., rate of wheel turning, weight on wheels, etc.) did not hold in that landing. In the Moscow case, there was a crosswind. I would describe the problem as a system design error or a requirements flaw, where the design did not account for cases that either were thought to be too unusual (low probability) and thus ignored or simply forgotten in the analysis. But it could also be described in the way you did, because the design of the process model is part of the design of the aircraft.

Note that I only mentioned two cases of this happening (Warsaw and Moscow). In fact, we found quite a few when looking for them on the internet. The real problem is twofold: (1) our certification and
analysis methods concentrate on failures and miss design errors where no components fail, (2) we may think of the really odd cases, but decide they are too unlikely (low probability) and therefore they can be ignored. I have lots of other examples of these types of accidents (having nothing to do with deceleration), but didn’t have time in the talk to present more than just this one example.

**Question:** How does STPA inform flight test to enable testing of the integration cases?

**Response:** STPA is a system analysis; it analyzes the system working as a whole and not just individual component failures or errors. So the scenarios identified are the integration cases. The analysis should ideally be used during development. Flight tests can then be identified both by the analysis itself but also by how effectively the developers were able to eliminate or mitigate the scenarios leading to the hazardous state. Using it only during flight test is not the most efficient way potentially to use it, but is what usually must be done today if STPA is not used during development. I understand that it is being used in planning flight test at Edwards AFB and taught at the TPS. There are so many users of STPA around the world today that I don’t know everyone that is using it.

**Question:**

1. **Are there any established methods to tailor STPA for an organization that is severely resource-limited?**

**Response:** We now have hundreds of evaluations and comparisons with the standard hazard analysis techniques and STPA requires orders of magnitude fewer resources (e.g., days vs. months or weeks vs. years). For the reason why this saving is true, see the response to a question below. So it is naturally the way to go for resource-limited organizations.

2. **The FAA, especially for Part 23, is comfortable using the methods from ARP4754/4761. Is there an established method to systematically ‘translate’ between STPA and the ARP processes that could be used in demonstrating the efficacy of STPA for compliance demonstrations?**

**Response:** ARPs 4754 and 4761 are very expensive to apply for small aircraft manufacturers. Because of that, STPA will probably be approved for Part 23 aircraft before Part 25 (there is more enthusiasm for it by small manufacturers, who have fewer resources). In fact, the ASTM has created an STPA standard to be used for certification of Part 23 aircraft. This standard effort was initiated and is being pushed by Embraer. I understand that the standard is written, has gotten comments, but the final vote has not been done. Part of the reason is that each person from Embraer who has spearheaded this effort has been hired away by other companies because they know STPA and the effort ends up not having someone to head it. I was told last week by the head of system engineering at Embraer that they are looking for a replacement to lead the ASTM standard effort. I cannot imagine any reason why it would be useful to translate the STPA results to a process, such as the one described in 4761, that only finds a portion of them and is very expensive. The hangup right now is not the FAA.

S-18 also has a formal description of STPA being developed that could be used by the FAA for certification, but it will likely take longer to finish than the ASTM STPA standard. Several people at the FAA have told me they need a formal specification of STPA before they can allow certification using it.

3. **For a design that has not been flown, or for which there is not accident evidence (such as eVTOL), is CAST usable?**
Response: No, CAST is used to investigate an accident or incident that has already occurred to identify the causal factors.

Question: Are you anticipating that STPA will become a formal requirement for FAA a/c certification? If yes, do you have any idea of when this could happen?

Response: As I understand it, the FAA does not require anything specific for certification. They allow the use of ARPs 4754 and 4761 for certification of aircraft. They can also allow alternative methods of certification. We have been told, informally, that the FAA is likely to do something this year to allow STPA as an alternative method.

Question: If STPA captures all of the existing interactions, how can it be that the resource requirements are fewer? It seems that touching all of those interactions takes substantial time.

Response: I must admit when we started seeing the data, I also was very puzzled. Intuitively, it seems that if it finds everything that other methods do plus things they cannot find, it should be more expensive. The reason, I figured out, is that STPA works in a very different way than the traditional methods. For example, FMEA examines all failures to see if they can lead to an accident. STPA starts with the accident and works backward so the only paths examined are critical ones. That makes STPA much more efficient. The difference is in the way STPA is performed.

Question: Would STPA analysis techniques be able to find errors or missing scenarios in models used to evaluate systems for example, terrain models used to evaluate a terrain following or terrain avoidance system?

Response: I’m not quite sure what you mean by a “model,” but yes STPA could find errors and missing scenarios for functions like terrain following or terrain avoidance. In fact, I’ve used it for that.

Question: Just wanted to highlight that many STPA resources are available on flight test safety.org as well as the tutorials from the virtual 2020 Flight Test Safety Workshop.

Response: Thank you.

Question: What's the authorities' (EASA, FAA, etc) stance towards STPA?

Response: There is no official stance that I know about. The FAA has asked Dr. John Thomas to teach classes on STPA to FAA certification personnel—which he has been doing for several years now—so I assume that is a positive sign. What we are told informally is not really appropriate for me to disclose publicly. I have less contact with EASA although someone at Embraer told me that EASA has allowed a small aircraft to be certified using STPA. I have no idea if that is true.

Question: Are you anticipating that STPA will become a formal requirement for FAA a/c certification? If yes, do you have any idea of when this could happen?

Response: As I said above, there are no formal FAA requirements that specific methods be used for certification. They allow some methods to be used. We have been told it will be approved as an alternative method, although I have no knowledge of a date. I hear rumors but prefer not to pass them on.
**Question**: Thank you Nancy for the outstanding brief. Which tools currently exist, and are certified for STPA? Are they integrated with current UML/SysML modeling tools such as Cameo? Thank you.

**Response**: The problem with using SysML is that it does not provide the right type of model for a hazard analysis (although I think a failure analysis might be possible). STPA is an analysis method that is performed on a particular type of model, a hierarchical control structure. See the answer to a similar question below.

**Question**: Was STPA methodology applied by Boeing or contributed for return of the 737 Max to service?

**Response**: I am not privy to what goes on internally at Boeing. Boeing Defense and Space (BDS) has been using STPA for many years. I was told by an executive in BDS that he (and others) recommended that BCA use it for the 737 MAX return to service, but I have no idea if they did.

**Question**: I understand the power of STPA to identify causal scenarios for losses. Can STPA contribute to assessing the relative likelihood of the scenarios or does that require more traditional methods?

**Response**: STPA identifies the safety-related requirements and scenarios that can lead to a loss. Once they have been identified, the proper and ethical response is to eliminate those scenarios and implement the requirements. For example, in the Warsaw case, if STPA identified the missing case related to the reverse thrusters, then the software should be changed to allow the reverse thrusters to be activated in that case. I don’t know how one can accurately find the probability of such a case occurring. In fact, every accident report I have seen and the accidents where I helped to write the report (such as Deepwater Horizon and the Columbia Space Shuttle) had done a probabilistic risk assessment that showed the accident could not happen (although it did). There have been two scientific evaluations of probabilistic risk assessment that I know about in the past 50 years. Both were failures, i.e., the estimates of the risk by experts for the same system were 3 to 4 orders of magnitude different. There is a big difference between $10^{-3}$ and $10^{-7}$. Again, see answer to the next question.

**Question**: If STPA encompasses normal system safety, is that part still mechanized via the same way, through FTAs, or is it now done through the control model w/o FTAs? How are probabilities then calculated?

**Response**: STPA is more powerful than FTA because it uses a different approach to finding causal scenarios. There would be no reason to revert to using FTA after doing STPA. It would be a waste of resources. STPA uses a different process.

There are now probably about a hundred comparisons between STPA and the traditional hazard analysis techniques. Some were carefully designed comparisons and some were informal comparisons done in industry. All showed that STPA is more powerful and finds things not found by the other methods. In some cases where there had been an accident but the analysts were not told about it, only STPA found the accident scenario. In another case (a defense system), the standard DOD required process was followed by the company developing the system. STPA was applied experimentally after the two vehicles ran into each other twice during test (because of a software problem). We did a CAST analysis of the two test accidents and also an STPA on the system as a whole. We found lots of software-related scenarios that were not in the official MIL-STD-882 analysis but the program manager told us that they had done a probabilistic risk assessment and did not need all this new fancy stuff. He put the
vehicle into operation and within two months there was another serious accident. It was one of the scenarios we had told them about but they decided they did not have to fix.

Every probabilistic risk assessment starts with identifying the qualitative scenarios that can occur. Then probabilities are assigned to the events. This used to work when systems were made up of almost all standard hardware components, which have failure probabilities. But aircraft (and other systems) are not just hardware today. Probabilities make no sense for software design errors. Even ARP 4761 admits this fact. So software and human errors are usually omitted from the fault trees, one of the reasons the probabilities are not accurate.

STPA identifies the scenarios, but those scenarios include software behavior and pilot (operator) behavior for which no probabilities are known or could be known (e.g., software is not stochastic). So the greater power to find all the scenarios leading to an accident means that it will not be possible to identify probabilities for these scenarios. But we can eliminate or mitigate them.

**Question:** Dr. Leveson, Some STPA doubters have countered that traditional tools e.g. FMEA with the help of subject matter experts can be used to identify hazards. Can you expound more on the specific characteristics STPA provides. Thank you!

**Response:** FMEA can identify hazards by starting with failures and identifying what those failures can lead to, but it cannot identify all the scenarios leading to the hazards. By the way, FMEA is a reliability analysis method, not a hazard analysis method. STPA starts from the hazards (e.g., loss of control over the aircraft, loss of thrust, inadequate lift) and finds the paths that can lead to those hazards. That is traditionally what a hazard analysis method does. Fault tree analysis does this too, but it again only identifies failures. It cannot find things where the system worked as it was designed, such as the Warsaw example. That’s, of course, why this scenario has happened in multiple types of aircraft (including Western aircraft 😊). I have dozens of other examples (not related to thrust reversers or deceleration), but had no time to present them in the hour I had to talk.

**Question:** How does this method draw on or complement other constraints-based methods such as cognitive work analysis?

**Response:** I have not looked at cognitive work analysis for a long time. It is usually used in human factors analysis, right? It can include the human operators and organizational entities, but does it include detailed hardware and software analysis? One of the problems I have worked on is mode confusion. To identify potential mode confusion, it is necessary to look in detail at the software logic and the human task. I don’t know if CWA does this. But as I said, I only looked briefly at it a while ago.

**Question:** In the example where the thrust reverser failed to deploy, the hazard was "Inadequate Deceleration on Landing". This is something that would be identified in a traditional Aircraft Functional Hazard Assessment. How is the STPA process different in identifying the Aircraft level hazards?

**Response:** Inadequate deceleration on landing is trivial to identify. It’s obvious and where the STPA an analysis starts, not where it ends. Knowing that inadequate acceleration is a hazard provides no guidance to the engineer in terms of preventing that hazard. 4761 identifies the component failures that can lead to it, but not the system design errors. In fact, as in the example in 4761 mentioned earlier, the FHA assumes that an annunciated brake failure cannot lead to a hazard because the pilot will always be able to do something about it without any accident resulting.

**Question:** TELL all... “Wherever there is a human in the loop there will be a problem.” : )
Response: I would add that if there is software in the loop, there will be a problem. We blame the human when something goes wrong but not the software when it does the wrong thing, or more commonly confuses the pilot and induces a human error. In future systems, we are going to need both humans and software and they will need to be understood as they affect each other. The belief that we are going to eliminate humans (including human pilots on the ground) is not realistic. Our systems are becoming incredibly complex. We can either forgo all this complexity (and the greater functionality it bestows) or start using and creating more powerful hazard analysis techniques. The traditional techniques used today (such as FTA or FMEA) are all 50-70 years old. We were building very different and much simpler systems at that time. And there was no software control.

Question: Thank you for your presentation, Dr. Leveson. Do you think it is feasible and beneficial to integrate STPA with MBSE methods that are currently in use?

Response: MBSE simply means that models are used in system engineering activities and analyses. That is true for STPA. One of the reasons MBSE has been limited in its impact is that engineers assume that only one model (view) of a complex system is necessary to perform all useful analyses. This assumption is untrue, but it does benefit the companies building tools (they only have to provide the tools to use one model, which increases their profits) and those using MBSE in terms of only having to learn to use one model and one tool. But it does not benefit our goal of improving system engineering.