SEI Cyber Talk (Episode 11)

Machine and Human Interaction in Aircraft Risk Management
by Elli Kanal and Mike Phillips

Elli Kanal: Hello, this is Elli Kanal. I'm joined today by Mike Phillips. And we want to talk to you today about automation and the related airline crashes that we've been having recently. So, I wanted to actually start with just what's some of your experience with this in the background?

Mike Phillips: Okay, yeah, the reason that I was interested in being part of this discussion was that my history before coming to the Software Engineering Institute was in the Air Force, and I was a test pilot in the Air Force. Now, during those days as a test pilot, I became very interested in human factors and how human factors play in how you control the aircraft. Now that, at the SEI, after having been with the SEI now for twenty-four years, the interactions have increased so dramatically over the years that the amount of computer involvement is just huge. And we've seen some recent examples of things that seem to be worthy of talking about because it's the interaction between the human and the computer in a situation in flight that makes things very tricky.

Elli Kanal: And I don't think most people are aware. To what extent is there automation in an aircraft? When you're driving a car, you have cruise control and that's about it. Modern cars are starting to get automated driving.

Mike Phillips: Right.

Elli Kanal: But that's really only the very high end.

Mike Phillips: Yes.

Elli Kanal: What is it in a typical aircraft?

Mike Phillips: Well, in a typical aircraft, once the pilot manipulates the aircraft-- manipulates-- flies the airplane, pulls the airplane into the sky, very quickly after that, he turns it over to the autopilot because simply the autopilot is more capable than his hands can be of actually navigating the airplane through the air and even down the approach to a landing. But often, the pilot will then take over for that final step of landing the airplane. But in fact, there increasingly isn't a need for that. So, we have a drone aircraft in fact that fly themselves, take themselves off, and land themselves. So, the amount of automation is huge now in there.

The difficulty that I'm expressing is that it's the interaction then between when does a human need to be in the loop and when does he not. When is it better to leave it to the computer? And when is it better that the person takes over. I flash back to those that are old enough to have watched "2001: Space Odyssey" where we have the human out in a pod saying, "Open the pod bay door, HAL." And HAL says, "No, Dave. You are a threat."

Elli Kanal: "I can't do that, Dave."

Mike Phillips: Yes, "You are a threat to the mission." So, this gets to be perilous kinds of considerations.

Elli Kanal: That's very-- I didn't appreciate I think that the full scope of takeoff, fly the thing, landing is all capable-- even handling turbulence or handling reroutes, the autopilot can do that?

Mike Phillips: Correct. It is a matter of getting the correct information for a reroute. But once fed to the computer, the computer then does that better, more accurately, in essence, than a pilot looking at material and trying to translate what he sees into a direction. We've managed to make that a very nicely automated capability.

Elli Kanal: So, we've seen over the past, I'll say, decade a small handful of automation-related problems.

Mike Phillips: Right.

Elli Kanal: Very recently obviously, we had some crashes, but even going back a while, there've been a couple different types. Are these all related? Are these highlighting a variety of problems?

Mike Phillips: It's a variety of problems, and it's also interesting that, from a pilot perspective, you'll hear pilots talk about how much authority they have or don't have. And for a while, there was a difference between the two major makers of airlines as-- airline aircraft as to how much automation was fed in and how much control the computer insisted upon as opposed to the pilot.

So, a quick example, and I think it's one that tells the broader story very well, it also is from the other aircraft producer, being Airbus, was the owner, the creator, of the airplane that many of you will remember from watching "Sully." And if you recall in "Sully," what happened was the airplane was struck by geese. Now, what is not very well portrayed in the movie was that the copilot then spent much of his time trying to get the-- one of the two engines restarted because he had a checklist to go through to try to get power back. The reason this became particularly challenging is because the computers associated with the engine in essence said, "You pilots don't understand this well enough. And we don't want you to do greater damage to the engine by restarting it." So, he was trying to get around the system in order to get some power back to the airplane while Sully was working on let me go ahead and find a place to land the aircraft.

Elli Kanal: And to your point earlier, if you've had all this focus on human factors in the aircraft, you have to take into account that, on the one hand, there are certain things that automation is actually better at--

Mike Phillips: Absolutely.

Elli Kanal: But, on the other hand, when you have a situation that the pilot's better at, you need to be able to pass that control back to the pilot.

Mike Phillips: Right.

Elli Kanal: And when you don't have that, that's when you seem to get some of these problems.

Mike Phillips: No, exactly right. And so, this is very much about how do the handoffs work back and forth, and how do you make sure there's enough time for the human in the loop to do what the human might need to do to solve a problem that the computer has lost the capability to do better in for whatever reason. So, in fact, the recent crashes had a particular error on one of the sensors. I would go back and note that there's-- for those that become interested in this area, there was a fairly similar kind of accident event in a test vehicle called the X-31 where a probe was malfunctioning, and the pilot of the aircraft fought the system for a while to try to recover it, and then alas, at the end, had to eject from the airplane, which could be done in a-- with a test aircraft, that's very common to have that kind of response, the ability to get out of the airplane. Unfortunately, with airlines, that's not a possibility.

Elli Kanal: Yeah, you really can't do that. So, in going through and thinking about this, when you have automation that's going to be handling the system, there's an awful lot that it's designed really to handle. So, you mentioned take off, piloting, and landing. To the lay observer, that's three things. I'm guessing that when you're-- as a pilot, as someone who's actually dealt with this, that's not three things. That's three thousand things. There's all these tiny little situations.

Mike Phillips: Right.

Elli Kanal: Are there areas even within the, I guess, underneath the greater genre, that here's where the human's good at, and in this specific part of it, though, the pilot's better, or the automation is better.

Mike Phillips: Well, that's absolutely true. I think we're finding, as I mentioned, because of these drone kind of aircraft-- do we lose drone airplanes? Yes, on occasion something happens that they crash. But it doesn't have the same result as when we are aware of an airline actually being lost with people involved at the same time. So, there's not a clear answer here. I think that, in many cases, the notion is that for the everyday operation, the computer is going to be able to do many things better, both quicker and more accurately, than a human possibly can. The issue is then when things don't go quite the way it was intended, how many problems might arise. And if we think about risk management, we often find that we do good risk management for a single event and say if this-- if X happens, this is how we respond.

There was an aircraft accident that I talk about, which was a military airplane where, before anyone-- it turned out there was one fatality in the crash, and there four different issues, all of which had failures. The four failures was what finally resulted in someone being harmed because they had enough safety systems that one would back up the next one etc. But by the fourth one, they had run out of options.

Elli Kanal: So, that actually brings me to something like here at SEI, we have a history with CMMI and other types of maturity models for understanding how well are-- how good are we-- to use improper English, how good are we at managing risk--

Mike Phillips: Yes.

Elli Kanal: And how well do we manage that.

Mike Phillips: Right.

Elli Kanal: So, in a system as complex as this, how would you roll some risk management out?

Mike Phillips: Well, it’s interesting you say that because I just, as we got ready for this event, I discovered an article written by MITRE, a MITRE team with an Air Force research lab person involved as well, released in December of 2018. And it’s titled "Human Machine Teaming." And with that, they go into some-- there’s a great deal of information. If someone’s working int his area and observing this little chat, I recommend that you at least check out that particular article because it talks about ways to wrestle with the risks associated.

And if we put in the notion of risk-- I’ll go back to Sully for another reason and that is that in that, you may recall in the movie if you saw the movie, that the FAA noted that, at the time of the event happening, had Sully immediately gone to the nearest airport to land, they would have been successful. In a simulation, they did this. And he said, “Well, okay, but how about this? We have these checklists that we’re supposed to go through to try to recover the airplane better,” for example, the restart of the engine. So, he said, “Delay thirty seconds for those kinds of interactions to occur between the pilot, the copilot, looking at checklists trying to figure out, resolve what they could do first.” That thirty seconds in the movie was sufficient to eliminate the possibilities of recovering the airplane at a runway and instead made the landing on the Hudson the best thing that could happen.

Elli Kanal: And that’s interesting because you mention human teaming.

Mike Phillips: Yes.

Elli Kanal: Or however it goes. That would be a perfect example where you say Sully and his copilot were trying to restart. You can imagine a scenario, as we continue to mature the technology, where it's Sully, the copilot, and the AI.

Mike Phillips: Yes.

Elli Kanal: And those thirty seconds, all of a sudden, are reduced to four.

Mike Phillips: Yes.

Elli Kanal: Go down the checklist, boom, boom, boom, boom, boom. They're both watching, monitoring--

Mike Phillips: Right.

Elli Kanal: Kicking off different events, and it still is recoverable in the future.

Mike Phillips: Exactly right. And that takes us to things like "Star Wars" with R2D2 being (beeping) in the backseat, in essence. The other pilot that, in essence, for whatever craft they were in at the time, that he was doing his thing. But it's a good model to say in our future state, we are not going to be going back to human only at all.

Elli Kanal: Right.

Mike Phillips: We will not. It just simply is not going to occur. Now, how do we make those interactions work better? How do we make sure that we don't go down a path that precludes the human being able to intervene in a way, perhaps not as adroitly as the computer would do, but save a situation from being catastrophic?

Elli Kanal: Very cool, alright, yeah that's definitely pretty neat. While we're not flying X-Wings any time soon, you can see that the potential for this is really-- it's not a joke. There are automated fire suppression systems kind of like you see in R2D2. There are automated steering and increase the power. So, it's not that far-fetched as it sounds, minus the sound effects. So, what kind of-- as we're going to build more of these systems-- and this is something which you've been thinking about a lot, what kind of message would you say here's how you have to think about this in the development?

Mike Phillips: Yes, part of the issue that I wanted to try to elaborate on a little bit, it actually goes back to another fascinating movie of the Russians were ahead of us. This was a Clint

Eastwood movie. And the Russians were ahead of us in the design of one particular vehicle. Clint Eastwood gets assigned to go steal it. And he gets in the airplane, and then he has to remember what the Russian word is that will enable him to command the vehicle to do the right thing. And that, in itself, is part of the issue that we've got to be very cognizant of. Often, we assume that if we design a system so that let's say the pilot pushes a particular button in order for something to happen, that, of course, that will be easily done. Well, will the pilot remember which button? Will he remember that he has to hold the button down for three seconds for it to work to avoid just an inadvertent operation etc.? There's too many things that are involved in the interactions that often get-- a particular designer thinks that someone is going to understand, but, at the end of the day, they won't.

I had a particular situation myself, in my very young flying days, where we were starting down the runway, and there was a problem on my side, and the word that I needed to tell the pilot to do was abort. That's the word that he will then pull back the throttle. I couldn't remember the word. So, we went faster than we needed to until finally the word came, "Abort," and he did, and we got the brakes hotter than we wish we had because of that simple delay. So, time delays are one of the ways that we can see this. Inadvertent operation of the wrong situation, and those that drive know the phenomenon of gee, I thought I was hitting the windshield wipers, but instead, in this car, this rental car that I'm in, it's positioned differently, and I hit the light switch instead, and that's worse and etc.

Elli Kanal: When I was first starting to drive, I remember I was on the highway parked in a line of traffic, and I meant to merge out, slammed on the gas instead of the brakes, smashed into the car in front of me, and that cost my parents quite a lot of money when I as a kid.

Mike Phillips: Yes.

Elli Kanal: And it's exactly that. You mean to do this. You do that.

Mike Phillips: Yes.

Elli Kanal: And it's just a momentary issue. In that case, thank god, no one was hurt.

Mike Phillips: Yes.

Elli Kanal: But it's the exact kind of mistake that you-- that people, especially folks who are brand new to whatever the situation is, very frequently make.

Mike Phillips: Right.

Elli Kanal: Well, cool, go ahead.

Mike Phillips: No, it was just that that's the part of design that's very difficult is to make sure that you're considering what the individual that you're trying to help is going to do. And in the MITRE study, as an example, they said get groups of three or four because no one is going to be sufficient to give an answer that everyone is going to do it the way that that person says.

Elli Kanal: The way that person is going to think it through. Cool, thank you very much. Well, thank you very much for joining us. For more information, please check out the links in the description. This has been Mike and Elli. Thank you for watching.

Related Resources

Crash of an Airbus A320 in New York

X-31: Breaking the Chain: Lessons Learned

X-31 Final Test Flight and Crash

Human-Machine Teaming Systems Engineering Guide (Mitre)

CMMI

SEI Mission Assurance