

WEBVTT

1

00:00:01.360 --> 00:00:04.940

All right, so we're on the downhill stretch. Got a couple hours.

2

00:00:05.110 --> 00:00:08.140

We're gonna go through, uh, the rest of this analysis.

3

00:00:08.150 --> 00:00:11.500

We're obviously not gonna complete the entire analysis in the next couple hours,

4

00:00:11.880 --> 00:00:14.860

but we're gonna, we're gonna just talk through, um, uh,

5

00:00:14.880 --> 00:00:18.820

pieces of it and carry a thread through from where we are now with the safety

6

00:00:18.900 --> 00:00:22.940

control structure, uh, to the scenarios, UCA scenarios and mitigations.

7

00:00:23.000 --> 00:00:25.580

And then I've got a few, uh, final takeaway slides,

8

00:00:25.640 --> 00:00:30.340

and hopefully there's some time at the end for, for questions as well. So,

9

00:00:30.340 --> 00:00:32.780

I think what I'm gonna do, just in the, uh,

10

00:00:32.780 --> 00:00:34.500

just due to the timeframe that we have,

11

00:00:34.930 --> 00:00:37.980

instead of us building our own safety control structure,

12

00:00:38.100 --> 00:00:41.260

I think that's gonna take a hot minute with, with this large of an audience.

13

00:00:41.760 --> 00:00:45.740

I'm just gonna show you what I did and talk through why I did it. And then, uh,

14

00:00:45.770 --> 00:00:50.500

feel free to ask any questions, uh, with that. Alright. I don't know if it'll,

15

00:00:50.960 --> 00:00:55.540

if can make it bigger or go to presentation mode. There we go.

16

00:00:55.970 --> 00:01:00.620

Alright. Um, so on the top there, I've got my ground station,

17

00:01:01.400 --> 00:01:04.740

uh, and which I included the operator and the user interface.

18

00:01:05.040 --> 00:01:07.860

As I mentioned before, the laptop does no, uh,

19

00:01:07.860 --> 00:01:10.380

calculating or anything like that. It's just a pass through,

20

00:01:10.390 --> 00:01:15.300

which is why it's dashed in that way. That was just a convention I chose to use.

21

00:01:15.330 --> 00:01:19.340

There's, there's not a, a formal convention in that way. Um,

22

00:01:19.640 --> 00:01:24.060

and then you see I did not include atc. I very well, I very well could have.

23

00:01:24.100 --> 00:01:27.620

I think that was a good put, uh, from earlier this morning. Uh,

24

00:01:27.620 --> 00:01:32.140

and then there's a variety of commands that the operator is passing, um,

25

00:01:32.240 --> 00:01:34.820

to the, actually before I get to commands, we'll talk about the aircraft.

26

00:01:34.840 --> 00:01:36.980

So I have the, the aircraft there in the big box.

27

00:01:37.250 --> 00:01:39.060

I've got the vehicle management system.

28

00:01:39.400 --> 00:01:44.340

The vehicle management system is turning power on and off to the payload.

Uh,

29

00:01:44.380 --> 00:01:46.740

I kept it simple. It's not doing any control than that.

30

00:01:46.740 --> 00:01:51.700

It's just turning it on and off. Uh, patrol and yaw to the control surfaces. Uh,

31

00:01:51.700 --> 00:01:56.180

throttle start and stop to the engine. Uh, the engine's feeding back some,

32

00:01:56.290 --> 00:01:59.900

some sort of engine parameters back to the vehicle management system.

33

00:02:00.280 --> 00:02:01.460

And then of course you've got your,

34

00:02:01.460 --> 00:02:04.940

your air data system providing air speed and pressure altitude. Uh,

35

00:02:04.940 --> 00:02:06.860

so that's how I, I put this together.

36

00:02:07.040 --> 00:02:10.580

We talked about you could potentially do your ground troops, your,

37

00:02:10.580 --> 00:02:13.860

your customer in here. You could do your atc. Um,

38

00:02:13.860 --> 00:02:18.060

you could break out vehicle management system into your calm, your power,
uh,

39

00:02:18.060 --> 00:02:21.740

navigation. There's, there's a variety of ways that you, you could, uh,

40

00:02:21.800 --> 00:02:25.860

cut this. And as you go through, as I mentioned, start, start high level.
Don't,

41

00:02:25.860 --> 00:02:30.020

don't put a million boxes in there. As you go through. You may choose,
uh,

42

00:02:30.020 --> 00:02:33.020

to break out some of these boxes at a later date.

43

00:02:34.880 --> 00:02:39.020

Um, alright. Any questions on how I set this up?

44

00:02:43.770 --> 00:02:48.550

Yes. Oh, let me get the, ah, thanks.

45

00:02:53.300 --> 00:02:53.590

What

46

00:02:53.590 --> 00:02:55.190

About data link?

47

00:02:55.620 --> 00:02:56.670

What about the data link?

48

00:02:57.010 --> 00:03:01.340

That's something we mentioned probably on the, on the whiteboard, but,
um,

49

00:03:01.520 --> 00:03:03.380

is that something you would, uh, show here?

50

00:03:03.440 --> 00:03:04.273

Or

51

00:03:04.300 --> 00:03:09.100

Y you could, so you could put some kind of data link, uh, within,

52

00:03:09.240 --> 00:03:12.700

within the aircraft or something along those lines. You, you could show that,

53

00:03:13.120 --> 00:03:13.820

um,

54

00:03:13.820 --> 00:03:17.300

I think implicitly there's some kind of data link and that's how the commands

55

00:03:17.300 --> 00:03:20.100

are being provided and, and feedback's going back up to the operator.

56

00:03:20.520 --> 00:03:24.340

So I didn't, I didn't explicitly draw it here, but you could do that,

57

00:03:24.600 --> 00:03:27.460

you could break that out as a subsystem, um,

58

00:03:27.480 --> 00:03:29.780

to the ground station or aircraft if you so chose.

59

00:03:31.970 --> 00:03:34.860

Yeah, I think what would happen is, uh,

60

00:03:35.400 --> 00:03:40.140

if you ended up in a situation where you start writing all your scenarios and

61

00:03:40.200 --> 00:03:43.220

you realize that there's something missing,

62

00:03:43.480 --> 00:03:46.940

or more controls that need to be added to the data link in particular,

63

00:03:47.850 --> 00:03:50.980

then that would give you clarity on where you should add more to your control

64

00:03:51.220 --> 00:03:56.060

structure. But perhaps you could also end up just realizing that

65

00:03:56.640 --> 00:04:01.300

as you write your scenarios, some of those scenarios are, you know,

66

00:04:02.160 --> 00:04:06.740

uh, an unsafe control action because you lost data link and maybe that's enough.

67

00:04:06.740 --> 00:04:10.060

You can write your mitigations to cover that and be okay.

68

00:04:10.760 --> 00:04:12.700

So it could be situational. As you,

69

00:04:13.080 --> 00:04:15.860

as you drill down deeper,

70

00:04:15.860 --> 00:04:19.180

you'll get more clarity on whether you need to come back and update your

71

00:04:19.340 --> 00:04:20.173

structure.

72

00:04:21.200 --> 00:04:23.060

And, um, this is where,

73

00:04:23.170 --> 00:04:27.620

like in our first attempt at doing it in the doctoral initiator is we kind of

74

00:04:27.680 --> 00:04:31.300

did an, an architectural put all the boxes in because this,

75

00:04:31.300 --> 00:04:34.620

that's how the communication goes. But in the end,

76

00:04:34.620 --> 00:04:36.860

you can collapse a lot of those boxes cuz uh,

77

00:04:36.860 --> 00:04:41.060

some of those components aren't making a control action with a feedback, right?

78

00:04:41.060 --> 00:04:43.660

They're just passing data through. And that was the,

79

00:04:43.680 --> 00:04:46.780

that's in my mind right now, the purpose of the data link, right?

80

00:04:46.800 --> 00:04:51.340

Is it actually making a control action based on any feedback it's getting?

81

00:04:51.340 --> 00:04:52.620

Or is it just passing the data through?

82

00:04:52.720 --> 00:04:55.620

And if it's just passing the data through, then it's probably gonna be, uh,

83

00:04:55.660 --> 00:04:59.500

a causal scenario of some sort, but it's not necessarily a, uh, uh,

84

00:04:59.780 --> 00:05:00.613

a control box.

85

00:05:17.780 --> 00:05:20.490

Funny, especially with teams the way it is now,

86

00:05:21.150 --> 00:05:24.650

you tend to get a cast of a thousand instead of, uh, you know,

87

00:05:24.650 --> 00:05:29.050

an effective working group when you do something like this. I mean, uh,

88

00:05:29.140 --> 00:05:31.370

8, 6, 8 people, I mean,

89

00:05:31.370 --> 00:05:35.130

obviously you need a stakeholder from each of the different elements,
but, um,

90

00:05:35.650 --> 00:05:37.810

I, I can see if you have more than that.

91

00:05:37.810 --> 00:05:41.690

This thing is gonna grow almost uncontrollably from the start. Yeah.

92

00:05:41.690 --> 00:05:42.730

Just wanted your opinion on that.

93

00:05:42.920 --> 00:05:44.930

Yeah, no, I, I think that's very true. I think 10,

94

00:05:45.030 --> 00:05:48.850

10 to 12 ish is probably the max that you wanna have. You wanna have the,

95

00:05:49.030 --> 00:05:52.130

the various, uh, disciplines represented, but you don't,

96

00:05:52.130 --> 00:05:55.890

you don't wanna have too many people. And there's a couple different ways
to,

97

00:05:55.950 --> 00:05:59.620

to run this. So, so I've, I've done sprints where, you know,

98

00:05:59.620 --> 00:06:03.060

we're just locked in a room for a week and we go through this. Uh,

99

00:06:03.060 --> 00:06:05.780

sometimes you can make that work with a schedule. Sometimes you can,

100

00:06:05.780 --> 00:06:08.980

especially if you're talking multiple organizations and that type of
thing.

101

00:06:09.240 --> 00:06:13.300

The other thing that I've done as well is if you can get to this point and you

102

00:06:13.300 --> 00:06:16.060

all nod your head and say, yep, I think this is what the,

103

00:06:16.160 --> 00:06:19.300

the functionality of our system is. I've,

104

00:06:19.370 --> 00:06:24.220

I've also sent people away and they'll run through the ucas and scenarios and

105

00:06:24.220 --> 00:06:27.300

mitigations based off of their expertise and their particular background.

106

00:06:27.680 --> 00:06:30.260

And then we come back maybe a week later or something like that,

107

00:06:30.940 --> 00:06:34.020

schedule dependent and, and we'll work through, okay, what did you find?

108

00:06:34.100 --> 00:06:37.060

What did you find? What did you find? We'll talk through it all, uh,

109

00:06:37.060 --> 00:06:40.820

that way we're not just trapped in a room, uh, for, for a while.

110

00:06:41.490 --> 00:06:43.220

There's a few different methodologies of that.

111

00:06:43.530 --> 00:06:47.020

Just a quick question. Uh, most autopilots have a feedback loop,

112

00:06:47.080 --> 00:06:50.940

and I notice where you're showing that there's an output from the VMs to the

113

00:06:51.340 --> 00:06:54.580

elevator, Aron and rudder. Is there a feedback loop there?

114

00:06:54.580 --> 00:06:56.580

So would that actually be a control system and there,

115

00:06:56.640 --> 00:07:00.060

and did you consider that and then not decide not to include it for some reason?

116

00:07:00.560 --> 00:07:04.540

Um, I did not consider it. I was, I was trying to keep it simple. Um,

117

00:07:04.540 --> 00:07:06.900

so I did not include that. But you very well could.

118

00:07:15.820 --> 00:07:19.080

So big question here. Two, two parts of it.

119

00:07:19.900 --> 00:07:22.480

How do you know when you've drilled down enough?

120

00:07:22.540 --> 00:07:25.400

How do you know when you've explored all the things that you have?

121

00:07:25.700 --> 00:07:29.880

Is there a process that helps you say, okay, we're close enough? You know,

122

00:07:29.880 --> 00:07:31.360

the second part of that is,

123

00:07:31.420 --> 00:07:35.040

are there any case studies where TPA missed something?

124

00:07:35.840 --> 00:07:38.720

I know there's, I know we've got the old traditional cases where yeah,

125

00:07:38.720 --> 00:07:41.040

we missed something, but is, is there some,

126

00:07:41.260 --> 00:07:45.320

are there case studies that help us close the loop and show that this is more

127

00:07:45.320 --> 00:07:47.000

effective and we do catch more? Mm-hmm.

128

00:07:47.080 --> 00:07:49.120

And what is the effective stopping point?

129

00:07:49.750 --> 00:07:53.360

There's, there's definitely case studies that talk about how, um,

130

00:07:53.550 --> 00:07:58.320

this catches more than traditional hazard analysis. So that, that does exist.

131

00:07:58.920 --> 00:08:02.440

I think, I think, you know, you've got this, when you go down the,

132

00:08:02.500 --> 00:08:06.800

the lower steps and, and you're not talking about a particular subsystem or,

133

00:08:06.820 --> 00:08:10.440

or the interactions between the two, uh, to the point that was made,

134

00:08:10.670 --> 00:08:15.280

that was made earlier. If you find yourself talking a lot about, you know, uh,

135

00:08:15.350 --> 00:08:19.160

some, some maybe sub component of what I've aggregated as the vehicle management

136

00:08:19.160 --> 00:08:21.760

system, maybe you need to break that out. Um, but,

137

00:08:22.220 --> 00:08:24.280

but if you're not having those conversations when you,

138

00:08:24.280 --> 00:08:27.120

when you get down to the UCAS and the scenarios, um,

139

00:08:27.120 --> 00:08:29.440

you've probably have it at the right level.

140

00:08:32.930 --> 00:08:34.090

I think that, um,

141

00:08:34.720 --> 00:08:39.530

lost link procedures or even to have another block where you have the

142

00:08:39.850 --> 00:08:43.130

transfer from local control to remote control. Mm-hmm.

143

00:08:43.450 --> 00:08:47.050

I think that's significant enough that it needs to have its own block because

144

00:08:47.050 --> 00:08:50.970

there's so many problems that can, can occur there. Mm-hmm. And you,

145

00:08:50.970 --> 00:08:54.770

you lose the whole asset or, uh, lose at least lose, uh, the instrumentation,

146

00:08:55.040 --> 00:08:56.580

The instruments that you need. Mm-hmm.

147

00:08:57.130 --> 00:08:59.980

Yeah. You, you definitely could, you could create another ground station.

148

00:09:00.160 --> 00:09:03.100

You could have grounds, you know, local line of sight, ground station.

149

00:09:03.320 --> 00:09:05.780

You can have an, uh, beyond line of sight ground station,

150

00:09:06.120 --> 00:09:07.820

and then you can talk about the cross control.

151

00:09:07.930 --> 00:09:11.100

There's probably some kind of handoff communication that's going on there.

152

00:09:11.100 --> 00:09:15.020

Right. Um, so you could definitely put that in there and talk about that.

153

00:09:15.140 --> 00:09:19.300

I did come up with, uh, some scenarios associated with that, um,

154

00:09:19.300 --> 00:09:23.180

line of sight to be on line of sight transfer and vice versa. Uh, even,

155

00:09:23.250 --> 00:09:25.180

even without having, having that.

156

00:09:25.200 --> 00:09:29.540

But I think that that would provide value for sure, for the analysis.

157

00:09:34.850 --> 00:09:36.570

I have a question regarding the big picture.

158

00:09:37.110 --> 00:09:39.570

If in the long term I want to replace the FDA

159

00:09:41.390 --> 00:09:43.610

is a mandatory step then to go into details, right?

160

00:09:43.990 --> 00:09:46.370

So this can be iteration zero,

161

00:09:46.550 --> 00:09:51.290

but then in a certain moment I have to be super detailed. Correct?

162

00:09:51.830 --> 00:09:54.570

Or I can't avoid going into details.

163

00:09:55.350 --> 00:09:59.090

You can't avoid going into the details. Yeah. For, for other analyses

164

00:09:59.350 --> 00:10:03.530

Or if I want to replace the fda mm-hmm. With s stpa mm-hmm.

165

00:10:03.610 --> 00:10:07.050

Can I do it by staying high level? Mm-hmm. I, I,

166

00:10:07.430 --> 00:10:11.570

my opinion right now is no, but yeah, I want your, yeah. What's your take?

167

00:10:11.950 --> 00:10:16.930

So, so I think even though this is high level, I came up with 300, uh,

168

00:10:17.130 --> 00:10:20.610

causal scenarios and, and associated mitigations just with this,

169

00:10:20.610 --> 00:10:24.450

with however many seven I think ish elements. Um,

170

00:10:24.550 --> 00:10:28.330

so you can come up with a lot as you go through, as you drill down,

171

00:10:28.440 --> 00:10:32.050

even with the high level analysis. Um, but you can always,

172

00:10:32.110 --> 00:10:36.450

you can always add additional ailments if you feel like this isn't sufficient

173

00:10:36.450 --> 00:10:37.370

for what you're trying to do.

174

00:10:38.840 --> 00:10:42.810

Yeah. I think maybe as we step into the scenario development,

175

00:10:43.580 --> 00:10:47.040

it'll be more clear that, um,

176

00:10:48.340 --> 00:10:49.140

you know, you can,

177

00:10:49.140 --> 00:10:53.360

you can start with something that you think is about right or maybe feels like

178

00:10:53.360 --> 00:10:54.400

it's not quite enough,

179

00:10:55.420 --> 00:10:59.920

and then look at your scenarios and your scenarios will add all this missing

180

00:10:59.920 --> 00:11:02.920

information that I think were feeling the mm-hmm.

181

00:11:03.630 --> 00:11:04.150

Yeah.

182

00:11:04.150 --> 00:11:04.983

Like we're,

183

00:11:05.170 --> 00:11:07.380

Initially I didn't have air data system,

184

00:11:07.380 --> 00:11:11.580

obviously that's a pretty important piece of feedback. So, so I added it on.

185

00:11:12.200 --> 00:11:13.500

Um, if I did this again,

186

00:11:13.580 --> 00:11:16.900

I don't know if I would aggregate elevator aileron and rudder altogether.

187

00:11:17.420 --> 00:11:20.620

I think I might separate those out. Um, so, so there's,

188

00:11:20.770 --> 00:11:24.220

there's learning every time, uh, you do one of these, and again,

189

00:11:24.220 --> 00:11:27.660

there's not one write book answer, which I think as engineers, it's,

190

00:11:27.660 --> 00:11:31.660

that's a difficult thing to admit. All right.

191

00:11:34.660 --> 00:11:39.600

So what we're gonna do is, uh, we're gonna build out some ucas. So,

192

00:11:39.780 --> 00:11:43.640

so we'll throw, um, uh,

193

00:11:43.730 --> 00:11:46.920

we'll throw a command. We'll use that one on the bottom.

194

00:11:47.180 --> 00:11:49.880

So that's an example of, uh, provides.

195

00:11:49.880 --> 00:11:54.740

So the operator provides GPS waypoints when the way points present a conflict

196

00:11:54.740 --> 00:11:59.580

with other aircraft. Um, so, so we'll focus on GPS waypoint.

197

00:11:59.680 --> 00:12:04.020

So what this will look like is in that left box, we,

198

00:12:04.080 --> 00:12:06.940

you would put, uh, you'd write, uh, GPS waypoints,

199

00:12:07.440 --> 00:12:10.420

and then you would go through not providing when,

200

00:12:10.640 --> 00:12:14.860

if the operator doesn't provide GPS waypoints, what's, um,

201

00:12:15.360 --> 00:12:18.500

how does that cause a hazard? If they do provide GPS waypoints,

202

00:12:18.720 --> 00:12:22.940

how does that provide a cause a hazard if they provide in the wrong order too

203

00:12:22.940 --> 00:12:25.940

early, too soon, ex or, uh, too late? Um,

204

00:12:26.660 --> 00:12:29.260

a how does that provide or cause a hazard?

205

00:12:29.680 --> 00:12:33.500

And then same with stop too soon and applied too long. Um, so

206

00:12:35.320 --> 00:12:39.420

go ahead and take some time fi five minutes or so and,

207

00:12:39.520 --> 00:12:43.980

and think on that. Uh, write down some, uh, to fill each of those boxes.

208

00:12:44.530 --> 00:12:48.240

I'll walk around again, and then we'll get back and talk through it.

209

00:12:50.230 --> 00:12:54.860

Sarah, are you asking just for this gps waypoint or all any,

210

00:12:55.000 --> 00:12:59.420

any of the, you guys? Yeah. You want everybody to just do this particular

211

00:13:00.040 --> 00:13:03.260

Yep. Yuca. So, so we've got, I, I didn't, I didn't go through the, uh,

212

00:13:03.260 --> 00:13:07.020

the entire, um, uh, commands there.

213

00:13:07.040 --> 00:13:09.140

But you've got the operator can,

214

00:13:09.520 --> 00:13:12.380

can set up GPS waypoints for the sortie.

215

00:13:12.610 --> 00:13:15.860

They can provide an altitude and air speed, the start engine, uh,

216

00:13:15.860 --> 00:13:19.980

stop engine commands. Uh, there's loss link procedures that they can program in.

217

00:13:20.840 --> 00:13:25.020

Um, and then turn the payload on and off launch. Now they hit the button and,

218

00:13:25.020 --> 00:13:28.540

and it goes through a pre-programmed routine, uh, to take off.

219

00:13:28.560 --> 00:13:32.700

And then a land now where once it gets to a certain, uh, uh,

220

00:13:32.700 --> 00:13:35.740

part of the pattern, they hit the button and it comes back and it lands.

221

00:13:36.160 --> 00:13:40.100

So I chose GPS waypoints, uh, to go forward, uh,

222

00:13:40.100 --> 00:13:42.740

just as to work through this particular problem set.

223

00:13:54.660 --> 00:13:55.493

Okay.

224

00:15:12.350 --> 00:15:13.450

To figure out what's the scenario.

225

00:21:58.920 --> 00:22:03.540

All right. So we'll go,

226

00:22:03.800 --> 00:22:07.820

go to the next slide. I'll show you, um, some examples.

227

00:22:18.150 --> 00:22:20.850

All right. So these are some that I, I came up with and I apologize.

228

00:22:21.010 --> 00:22:24.850

I don't think I gave my instructions, uh, particularly clearly. I think folks,

229

00:22:25.060 --> 00:22:28.770

folks really keyed in on the, you know, uh, presents, uh, uh,

230

00:22:29.010 --> 00:22:31.450

conflict to the aircraft and then working to put,

231

00:22:31.550 --> 00:22:34.370

put things in the bucket that fit that. But, but there's a lot,

232

00:22:34.370 --> 00:22:38.090

there's a lot of different scenarios really focused on that circumstance.

233

00:22:38.090 --> 00:22:42.690

What are the different circumstances? So, so some things I came up with, uh,

234

00:22:42.690 --> 00:22:45.010

for not providing causes a hazard. So in this case,

235

00:22:45.190 --> 00:22:49.090

the operator just never provides GPS waypoints, uh, to,

236

00:22:49.590 --> 00:22:53.330

to the aircraft. Um, if they don't, if they don't provide, uh,

237

00:22:53.590 --> 00:22:58.250

GPS waypoints during pre-launch operations, probably not gonna take off.

238

00:22:58.670 --> 00:23:03.610

So now you've lost the mission, uh, and that's what H three is. Um, maybe,

239

00:23:03.860 --> 00:23:07.610

maybe the mission changes. Again, this is an IR platform of some kind.

240

00:23:07.660 --> 00:23:11.650

Maybe your, maybe your target changes your location. Maybe there's a different,

241

00:23:11.750 --> 00:23:15.810

uh, higher value target or something like that. Uh, so, so, uh,

242

00:23:15.810 --> 00:23:16.643

the mission changes,

243

00:23:16.870 --> 00:23:20.850
but the GPS sway point stay the same as what was originally programmed.
Uh,

244
00:23:20.850 --> 00:23:22.210
so that would also be loss of mission.

245
00:23:22.470 --> 00:23:26.730
Can you think of something else in the not providing causes a hazard

246
00:23:27.310 --> 00:23:28.143
box?

247
00:23:38.160 --> 00:23:38.993
H three,

248
00:23:39.600 --> 00:23:42.120
H three, I believe that was, uh, loss of mission.

249
00:23:46.690 --> 00:23:51.660
What you got? Oh, the mic. Oh,

250
00:23:51.660 --> 00:23:54.820
we've lost the mic. Uhoh. All right. I'll just,

251
00:23:55.090 --> 00:23:59.740
I'll just shout. Uh, the, uh, so if, uh, if a new airplane enters the
airspace,

252
00:24:00.080 --> 00:24:02.660
it was not part of the pre planning mm-hmm.

253
00:24:03.000 --> 00:24:06.940
And do not put in GPS coordinates to void Yep.

254
00:24:06.940 --> 00:24:10.860
Then that could Yeah, that's a good one. So, so an aircraft enters
airspace,

255
00:24:11.440 --> 00:24:14.660
but, um, but you don't change your GPS coordinates provide, uh,

256
00:24:14.660 --> 00:24:19.580
new GPS coordinates, um, that could, that could cause conflict. Yep.

257
00:24:21.990 --> 00:24:26.530
All right. So providing causes a hazard. So you'll see there I had a few,

258
00:24:26.530 --> 00:24:29.250
there's the one in the box that we, we've talked about,

259
00:24:29.270 --> 00:24:33.730
but there's some other ones too. Uh, so the operator provides GPS
waypoint,

260
00:24:34.110 --> 00:24:35.970
uh, when they don't align with the mission.

261
00:24:36.150 --> 00:24:40.130
So you're getting some kind of request from your customer, right? Um,
and, uh,

262
00:24:40.130 --> 00:24:43.290
for whatever reason, the way points that were entered, uh,

263
00:24:43.290 --> 00:24:47.720
didn't in align with what that request is. Uh,

264
00:24:47.720 --> 00:24:48.960
and then the third one there,

265
00:24:49.280 --> 00:24:53.520
operator provides GPS waypoint when the root length exceeds the fuel on
board in

266
00:24:53.520 --> 00:24:58.160
general, that's bad. Uh, so I think H four is, um,

267
00:24:58.390 --> 00:25:02.560
loss of control, I believe is what that one was. Uh, so you run out of
fuel,

268
00:25:02.690 --> 00:25:06.120

can't control the aircraft, uh, the operator, um,

269

00:25:06.350 --> 00:25:10.890

when the route is outside, let me,

270

00:25:11.210 --> 00:25:14.210

I think that's written funky. Um, so, uh,

271

00:25:15.190 --> 00:25:18.450

the route is outside the line of sight radius,

272

00:25:18.470 --> 00:25:23.410

but beyond line of sight is not being used. Uh, so that actually is, is a,

273

00:25:23.470 --> 00:25:27.130

is a test related one. So when this, when this aircraft was being designed,

274

00:25:27.130 --> 00:25:29.090

they would go and, or tested rather,

275

00:25:29.270 --> 00:25:32.290

they'd go fly it and just use a line of sight ground station.

276

00:25:32.670 --> 00:25:36.730

So what happens if it exceeds, uh, the line of sight radius? Uh,

277

00:25:36.830 --> 00:25:41.810

now you've potentially lost your aircraft, uh, incorrect timing and order.

278

00:25:41.990 --> 00:25:46.650

The operator provides GPS waypoints after the line of sight is lost.

279

00:25:46.750 --> 00:25:50.850

But before, beyond, beyond line of sight, radio link is established. Um,

280

00:25:51.470 --> 00:25:56.210

and then operator provides GPS waypoints after the UAV reaches bingo fuel,

281
00:25:56.390 --> 00:26:00.290
so they realize too late. Um, and, and it can't make its way home,

282
00:26:01.510 --> 00:26:04.690
uh, for stop too soon or apply too long. We get kind of,

283
00:26:04.690 --> 00:26:07.410
kind of creative with these. Um, so the first one there,

284
00:26:07.430 --> 00:26:10.970
the operator provides GPS waypoints when the number of waypoint exceeds
the

285
00:26:10.970 --> 00:26:14.490
storage capacity, the autopilot probably not a huge deal in,

286
00:26:14.490 --> 00:26:17.610
in today's modern systems, but, but something to think about.

287
00:26:18.070 --> 00:26:21.490
And then the operator provides GPS way points when the list of way points
is not

288
00:26:21.650 --> 00:26:24.850
complete for the entire mission. So you don't include everything that's
needed,

289
00:26:25.470 --> 00:26:28.050
uh, to, to go to wherever it needs to go, and then,

290
00:26:28.050 --> 00:26:30.370
and then come back to the airfield.

291
00:26:31.070 --> 00:26:34.210
So does this make more sense now that you've actually seen an example,

292
00:26:36.620 --> 00:26:37.570
Sarah? Um,

293
00:26:38.310 --> 00:26:42.850

one thing that I'd like to bring up that caused Darren and I some pain,
um,

294

00:26:43.040 --> 00:26:45.940

so I think Kevin, you mentioned, uh, uh,

295

00:26:46.120 --> 00:26:50.540

not providing GPS waypoints if a, um, there's, uh,

296

00:26:50.880 --> 00:26:54.780

if you're about to have a conflict with another aircraft, and then you
can also,

297

00:26:54.780 --> 00:26:57.980

it's also written here as not providing, uh, a, uh,

298

00:26:58.520 --> 00:27:02.660

GPS waypoints or sorry, providing, uh, GPS provide, uh,

299

00:27:02.660 --> 00:27:06.980

creates a conflict with another aircraft. It's almost the same thing,
just, um,

300

00:27:07.340 --> 00:27:09.620

rewritten. And so we were having a lot of trouble with that.

301

00:27:09.620 --> 00:27:10.980

We were getting wrapped around the axles,

302

00:27:10.980 --> 00:27:13.620

like we could put it in every single category. Um, Dr.

303

00:27:13.620 --> 00:27:16.540

Thomas gave us some advice and talked thought about,

304

00:27:16.910 --> 00:27:21.740

think about the context and if the causal scenarios could be different,
right?

305

00:27:22.120 --> 00:27:26.820

And so in this case, maybe it'd be worthwhile because, um, the,

306
00:27:26.920 --> 00:27:31.820
the causal scenarios for why, uh, you wouldn't provide a GPS point, uh,

307
00:27:31.820 --> 00:27:33.860
waypoint in the case of a, uh,

308
00:27:34.140 --> 00:27:38.380
a imminent conflict or why you would provide something that causes a conflict,

309
00:27:38.670 --> 00:27:40.540
those could be different. Um,

310
00:27:40.560 --> 00:27:42.660
so that was a little hard for me to get my head wrapped around.

311
00:27:42.700 --> 00:27:44.820
I don't know if you have a better way of phrasing that or not, but

312
00:27:44.920 --> 00:27:48.500
No, I, I think that's right. If, if you're not sure, just put it in both and,

313
00:27:48.500 --> 00:27:51.620
and see how, see how the analysis plays out. Uh,

314
00:27:51.620 --> 00:27:55.740
I wouldn't lose too much sleep over, over where you wanna put it.

315
00:27:55.740 --> 00:27:58.420
Just put it in both and then, and see what happens. And I think you're right.

316
00:27:58.500 --> 00:28:01.100
I think you'll find that your causal scenarios, uh,

317
00:28:01.100 --> 00:28:04.780
tend to be slightly different for that kind of double negative ish thing you got

318
00:28:04.780 --> 00:28:05.613

going on there.

319

00:28:06.050 --> 00:28:09.820

Yeah. I think, like, to build on that specific example, right?

320

00:28:09.940 --> 00:28:14.220

I could see where maybe your system is kind of slow at

321

00:28:15.420 --> 00:28:17.990

inputting way waypoint and accepting waypoint.

322

00:28:18.650 --> 00:28:23.310

And so it might be fine if your scenario is

323

00:28:23.590 --> 00:28:25.350

building waypoint before you take off,

324

00:28:26.170 --> 00:28:30.630

but if you have an emergent conflict while you're flying, it could expose like,

325

00:28:30.930 --> 00:28:35.750

man, maybe your system's just way too slow to put in a waypoint and accept a new

326

00:28:35.750 --> 00:28:39.390

route and get you re-routed before you run into something. Mm-hmm.

327

00:28:40.570 --> 00:28:45.070

So that would be a reason to put both scenarios or both, uh, ucas,

328

00:28:48.080 --> 00:28:52.040

I, I just had one question. I think, uh, we were struggling here with the,

329

00:28:52.420 --> 00:28:55.640

the table, but I think now I think I understand what,

330

00:28:55.830 --> 00:28:59.400

what is the ask or what's the question? So what this does,

331

00:28:59.660 --> 00:29:04.280

it flushes out what you call causal scenarios. What in the,

332

00:29:04.630 --> 00:29:07.280

over here is the circumstance. So what,

333

00:29:07.470 --> 00:29:12.320

what we're trying to do here is answer the question for

334

00:29:12.940 --> 00:29:14.080

the particular command.

335

00:29:15.070 --> 00:29:19.240

What is the circumstance that if this command is not provided,

336

00:29:19.380 --> 00:29:20.680

or if this command is provided,

337

00:29:20.740 --> 00:29:24.280

or if it's provided for too long or too short or too early or too late,

338

00:29:24.750 --> 00:29:27.680

what is the circumstance that could result in a,

339

00:29:28.640 --> 00:29:31.880

a condition that you don't want? Is that the question? Cuz that's what,

340

00:29:31.880 --> 00:29:33.960

That's very good way to state it. Yeah, that's exactly right.

341

00:29:34.620 --> 00:29:37.800

But specifically, uh, uh,

342

00:29:38.450 --> 00:29:42.580

we're not diving into the cause yet. Yeah. So it's just the,

343

00:29:43.120 --> 00:29:46.820

for this specific controller, which I think is just the operator, right?
Mm-hmm.

344

00:29:47.200 --> 00:29:51.140

The, the controller, what are all the control actions that would be undesirable?

345

00:29:51.600 --> 00:29:53.700

Yes. And then we go into the causes later.

346

00:29:53.700 --> 00:29:58.420

Yeah. Yeah. We'll do the scenarios next. Um, so this is just saying this,

347

00:29:58.450 --> 00:30:03.180

this could be a thing that happens, uh, with, with a particular circumstance.

348

00:30:03.400 --> 00:30:06.500

And this often is where people start assuming things away.

349

00:30:06.570 --> 00:30:10.980

That could never happen. We would never, we would never, um, you know,

350

00:30:10.980 --> 00:30:14.060

provide GPS waypoints that exceed, um,

351

00:30:14.280 --> 00:30:16.660

the range of the aircraft or something like that. That could never happen.

352

00:30:17.260 --> 00:30:18.300

Question, go ahead and put it up there.

353

00:30:18.800 --> 00:30:23.620

So, question, uh, uh, so on the horizontal, so not providing, providing,

354

00:30:24.290 --> 00:30:28.580

providing too long, too, too short, too soon, too late. I mean,

355

00:30:28.840 --> 00:30:32.580

you can go on with more columns, can't you? Or, or is that,

356

00:30:32.840 --> 00:30:37.740

is that the end of the possibilities? You could go on the GPS coordinates, uh,

357

00:30:37.740 --> 00:30:41.380

do something else, uh, or another action that is not time related.

358

00:30:42.920 --> 00:30:47.260

So these are the only four buckets that you're gonna have. Um, you can,

359

00:30:47.260 --> 00:30:51.260

you can fit everything into those four buckets, but you can have as many, uh,

360

00:30:52.290 --> 00:30:56.500

ucas within those four buckets as, as you can think of, as you can work through.

361

00:31:01.050 --> 00:31:03.270

All right. Any other questions?

362

00:31:06.770 --> 00:31:08.750

All right. Yep.

363

00:31:15.370 --> 00:31:20.270

Is not my first line, but, um, got a bit confused by that. Uh, when mm-hmm.

364

00:31:20.350 --> 00:31:25.310

What, at the beginning that it would be, so let's take this example.

365

00:31:25.630 --> 00:31:28.150

Actually, the operator provides GPS waypoints.

366

00:31:28.290 --> 00:31:29.123

Oh, thanks.

367

00:31:29.930 --> 00:31:33.590

The operator provides GPS waypoints when the waypoints present a conflict.

368

00:31:33.710 --> 00:31:37.350

I thought that the when would be like a cause, uh, or let's say a condition.

369

00:31:37.530 --> 00:31:41.590

Mm-hmm. So when there is a conflict, I provide the waypoints. Mm-hmm. But it,

370

00:31:42.490 --> 00:31:43.470

Oh, I see what you're saying.

371

00:31:43.910 --> 00:31:44.830

I thought it would be,

372

00:31:44.960 --> 00:31:49.350

let's say like the waypoints which present a conflict with the other aircraft,

373

00:31:49.450 --> 00:31:49.910

or Yeah.

374

00:31:49.910 --> 00:31:54.870

Is there a reason why you used the when or it just came out like this, or,

375

00:31:54.950 --> 00:31:55.950

I think it just came out that way.

376

00:31:56.020 --> 00:31:57.310

Okay. Never mind me.

377

00:31:57.480 --> 00:32:00.510

Maybe my understand, maybe English isn't my first language either. I don't,

378

00:32:02.130 --> 00:32:05.510

but No, it's, it's focused on, uh, you know, what's, what's the result,

379

00:32:05.890 --> 00:32:07.070

the circumstance and the results.

380

00:32:07.530 --> 00:32:11.030

The results of the action, which is uploading the, the way points, obviously,

381

00:32:11.030 --> 00:32:11.863

obviously.

382

00:32:12.050 --> 00:32:13.110

Thanks. That's it.

383

00:32:19.130 --> 00:32:19.963

All right.

384

00:32:23.230 --> 00:32:23.580

Ready

385

00:32:23.580 --> 00:32:24.413

For the next

386

00:32:24.490 --> 00:32:29.220

Yeah, what we got next scenarios. So we're gonna do, we're gonna keep,

387

00:32:29.250 --> 00:32:33.980

keep pulling that thread with the operator provides GPS waypoints when the

388

00:32:33.980 --> 00:32:37.340

waypoints present a conflict, uh, with other aircraft.

389

00:32:37.360 --> 00:32:41.420

So we're gonna come up with some scenarios that could, that could happen.

390

00:32:41.540 --> 00:32:46.100

I think some have already been discussed as we've been going along, but, um,

391

00:32:46.880 --> 00:32:51.740

why, why would an operator do that? Uh, create or provide gps,

392

00:32:52.280 --> 00:32:55.180

gps, waypoints, I can't speak. Uh, when they present a conflict,

393

00:32:59.650 --> 00:33:00.483

I heard something,

394

00:33:07.610 --> 00:33:08.443

sorry, I'm deaf

395

00:33:17.080 --> 00:33:18.920

Aircraft there, they dunno, aircraft positions

396

00:33:19.460 --> 00:33:21.840

Yep. Or something like that. Yep. They're unaware of a conflict.

397

00:33:21.980 --> 00:33:24.960

So they don't know. Maybe they don't know that another aircraft has,

398

00:33:25.020 --> 00:33:29.680

has violated the airspace or something like that. Yep. That's one.

399

00:33:30.780 --> 00:33:31.613

What other ones?

400

00:33:38.140 --> 00:33:40.080

Yep. Wrong file. Previous mission planning.

401

00:33:46.970 --> 00:33:51.300

What are other, other scenarios? Typo.

402

00:33:51.980 --> 00:33:56.180

A typo. Yeah. They, they typed it in wrong.

403

00:33:57.440 --> 00:33:58.340

The vehicles that way.

404

00:33:58.690 --> 00:34:02.380

Yeah. Yeah. Yep. I has definitely gotten,

405

00:34:02.520 --> 00:34:03.780

gotten some folks before.

406

00:34:09.050 --> 00:34:13.340

What if, um, maybe there's some submission changes or something like that.

407

00:34:13.340 --> 00:34:16.700

They were, they were given information they thought was good. Uh,

408
00:34:16.790 --> 00:34:20.860
maybe now there's some other aircraft that are gonna be flying that have flight

409
00:34:20.860 --> 00:34:23.220
plans, et cetera, that they're unaware of

410
00:34:32.800 --> 00:34:36.020
Flying where there will not be.

411
00:34:36.570 --> 00:34:39.740
Yeah. They think they have altitude deconfliction and they don't.

412
00:34:43.480 --> 00:34:47.820
So the other thing that helps when you're trying to come up with scenarios is,

413
00:34:48.080 --> 00:34:48.913
uh,

414
00:34:49.040 --> 00:34:53.780
you can look at what existing feedback is there and

415
00:34:53.780 --> 00:34:58.540
look for sometimes a scenario might be that feedback is erroneous,

416
00:34:59.790 --> 00:35:03.250
or the other to look for is maybe there's feedback that's missing that would

417
00:35:03.250 --> 00:35:08.130
lead an operator to a, into a scenario. Mm-hmm.

418
00:35:09.040 --> 00:35:10.210
Yeah. I Go ahead.

419
00:35:10.760 --> 00:35:13.970
Include something like, uh, incomplete transmission,

420
00:35:14.440 --> 00:35:19.200

like a lack of error checking on the, on the vehicle for, you know,

421

00:35:19.200 --> 00:35:21.840

a complete transmission and it only gets the first couple of digits

422

00:35:21.840 --> 00:35:23.480

Or something. Yeah, definitely.

423

00:35:23.580 --> 00:35:27.240

So incomplete transition or transmission so it doesn't get the entire message.

424

00:35:27.740 --> 00:35:31.120

Um, that's absolutely one. So we talked about, um,

425

00:35:31.120 --> 00:35:34.080

different types of scenarios early on. I can't remember if I put it,

426

00:35:34.320 --> 00:35:38.380

I think maybe it's on your sheet. Yeah. Yeah. The, so,

427

00:35:38.400 --> 00:35:40.220

so you can kind of go through, uh,

428

00:35:40.220 --> 00:35:43.980

either I think it's very important that you go look at your safety control, uh,

429

00:35:44.100 --> 00:35:46.540

structure that you created, but you can also go through these different types.

430

00:35:47.160 --> 00:35:51.660

So, so if, uh, if it, if, um, a command was not transmitted fully,

431

00:35:51.670 --> 00:35:56.540

there was some kind of, some kind of issue, um, that might follow, uh,

432

00:35:56.540 --> 00:36:00.180

somewhere in, in kind of the, that type two or something along those lines.

433

00:36:05.540 --> 00:36:06.373

What else?

434

00:36:15.180 --> 00:36:18.320

All right. So we can go on to, uh,

435

00:36:18.340 --> 00:36:23.320

to mitigations on the, on the right side, or if you go back up, um,

436

00:36:23.620 --> 00:36:25.680

to talk mitigations. So,

437

00:36:25.860 --> 00:36:30.200

so the operator is unaware of other aircraft in their airspace.

438

00:36:31.380 --> 00:36:33.280

What's a, a mitigation for that one?

439

00:36:36.900 --> 00:36:38.670

Monitor the correct frequencies.

440

00:36:39.730 --> 00:36:43.070

Yep. Yep. Maybe he's not on the, the right frequencies for,

441

00:36:43.370 --> 00:36:47.550

for whoever's controlling the airspace. Yep.

442

00:36:47.570 --> 00:36:48.950

At attc.

443

00:36:50.290 --> 00:36:51.123

Mm-hmm.

444

00:36:51.410 --> 00:36:53.750

Yep. Mission planning.

445

00:36:55.290 --> 00:36:59.270

Mm-hmm. Two independent information,

446

00:36:59.930 --> 00:37:04.830

Two independent sources of traffic information. Create some redundancy.

447

00:37:09.890 --> 00:37:10.723

D

448

00:37:16.430 --> 00:37:19.490

So perhaps you have a requirement or mitigation, uh,

449

00:37:19.490 --> 00:37:23.570

your system has an audible or feedback for,

450

00:37:24.390 --> 00:37:26.850

uh, if a GPS waypoint is about to cause a conflict.

451

00:37:28.030 --> 00:37:28.863

Mm-hmm.

452

00:37:29.550 --> 00:37:33.690

Yep. So some kind of, some kind of feedback. The, that ui uh,

453

00:37:33.830 --> 00:37:37.770

the laptop provides some kind of feedback to the operator.

454

00:37:44.970 --> 00:37:48.300

Yeah. And then we talked about ATC as part of the safety control structure.

455

00:37:48.410 --> 00:37:51.540

This would be why, why, right. Uh, they're gonna,

456

00:37:51.540 --> 00:37:54.060

they're gonna play a role in this part.

457

00:37:56.960 --> 00:38:01.300

All right. So, uh, a prior mission file was used

458

00:38:04.450 --> 00:38:05.340

Loading procedures,

459

00:38:05.890 --> 00:38:07.580

Loading procedures, wipe the

460
00:38:07.580 --> 00:38:08.413
Old one before you

461
00:38:08.680 --> 00:38:10.940
Yep. Clear, clear the, uh,

462
00:38:10.960 --> 00:38:15.100
old file as part of your pre-flight checklist. And then, uh,

463
00:38:15.100 --> 00:38:17.060
before you load the next one,

464
00:38:28.940 --> 00:38:30.560
and you can maybe have some kind of, uh,

465
00:38:31.340 --> 00:38:36.060
double check too that what's in the system actually matches what you think it

466
00:38:36.060 --> 00:38:36.893
ought to.

467
00:38:37.280 --> 00:38:39.260
Visual representation of route.

468
00:38:40.640 --> 00:38:45.410
Yep. Yep. Visual representation of the route.

469
00:38:45.750 --> 00:38:50.010
So that could be part of the UI design. Just making sure that's, that's there.

470
00:38:53.100 --> 00:38:53.933
Mission brief.

471
00:38:54.740 --> 00:38:55.573
Okay.

472
00:38:57.250 --> 00:38:59.830
All right. Typo on the waypoint.

473

00:39:03.640 --> 00:39:04.473

What you got

474

00:39:15.390 --> 00:39:18.610

second set of eyes verifying that it's good. Yep.

475

00:39:19.950 --> 00:39:23.450

And what's interesting is that would also potentially solve the prior mission

476

00:39:23.450 --> 00:39:27.290

profile as well. Right? And that goes back to the point that, um,

477

00:39:27.520 --> 00:39:29.770

that Darren and Dunes met talked about during their,

478

00:39:29.820 --> 00:39:33.610

their piece is that sometimes you can have a mitigation that,

479

00:39:33.640 --> 00:39:35.650

that solves more than one scenario.

480

00:39:37.830 --> 00:39:38.270

Any

481

00:39:38.270 --> 00:39:38.500

Say

482

00:39:38.500 --> 00:39:40.050

Legal feedback also solve

483

00:39:44.000 --> 00:39:44.833

Yeah.

484

00:39:45.670 --> 00:39:46.080

Yep.

485

00:39:46.080 --> 00:39:46.913

Very true.

486

00:39:47.480 --> 00:39:47.770

What

487

00:39:47.770 --> 00:39:49.410

About incomplete transmission?

488

00:39:56.340 --> 00:39:59.110

Read back? Yep.

489

00:39:59.110 --> 00:40:01.990

Some kind of feedback or read back function from the aircraft.

490

00:40:18.200 --> 00:40:21.860

So it's what's interesting, we talked about the, uh, order of precedence.

491

00:40:22.320 --> 00:40:25.420

So there's some things we could do to, to design this out, right? If you,

492

00:40:25.420 --> 00:40:28.940

if you put a DSB or TCA or something like that onto the aircraft,

493

00:40:28.940 --> 00:40:33.700

you could potentially design out some of this risk. Um, and then you have,

494

00:40:34.010 --> 00:40:37.620

okay, maybe, maybe we don't have that ability for whatever reason. Um,

495

00:40:37.640 --> 00:40:41.580

so now we're doing, you know, the, the two person checks or, or other, uh,

496

00:40:41.580 --> 00:40:45.020

visualization techniques that leaves room for the operators to goof it up,

497

00:40:45.020 --> 00:40:49.500

right? So, um, so, so that's something to think about.

498

00:40:49.520 --> 00:40:50.700

If you can design it out,

499

00:40:51.080 --> 00:40:53.780

that's gonna be a more successful mitigation in the long run.

500

00:40:57.940 --> 00:41:02.400

All right. If you go to the next slide. So these are some of the ones that I,

501

00:41:02.520 --> 00:41:05.680

I came up with. They're a little wordy.

502

00:41:05.680 --> 00:41:09.480

I could probably cut back on this a little bit. Um, but the operator provides,

503

00:41:10.140 --> 00:41:13.400

uh, GPS way points that don't conflict with other aircraft,

504

00:41:13.420 --> 00:41:16.480

but there's some interference along the route. Um, they're not received.

505

00:41:16.700 --> 00:41:18.640

It uses waypoint from a previous sorting,

506

00:41:18.690 --> 00:41:21.760

which conflict with the present traffic. So we kind of had some,

507

00:41:21.830 --> 00:41:26.160

some scenarios along those lines, uh, that y'all created. Uh,

508

00:41:26.200 --> 00:41:30.200

the operator provides way points to the uav. Um, uh,

509

00:41:30.200 --> 00:41:34.980

but they use an old flight plan, um, not as opposed to,

510

00:41:35.240 --> 00:41:39.500

uh, the current mission. Um, and they don't match the approved route. So we,

511

00:41:39.680 --> 00:41:44.460

we came up with that one as well. Old mission, the operator provides waypoints,

512

00:41:44.800 --> 00:41:45.980

uh, which don't conflict,

513

00:41:46.240 --> 00:41:49.900

but they're far apart from each other and travel between the waypoints do

514

00:41:50.050 --> 00:41:53.220

present a complex, maybe they're not close enough, uh, to,

515

00:41:53.240 --> 00:41:56.220

to really control the route of that aircraft.

516

00:41:57.900 --> 00:42:01.920

And then the operator provides way points which don't conflict. Um,

517

00:42:01.920 --> 00:42:04.720

however the aircraft air traffic changes, um,

518

00:42:04.720 --> 00:42:08.120

and they don't receive the updated information. We got that one as well.

519

00:42:09.820 --> 00:42:14.400

And then, um, they weren't saved. So older way points were,

520

00:42:14.550 --> 00:42:19.520

were not overwritten. I think we talked about that one as well. So you guys,

521

00:42:19.540 --> 00:42:23.040

you guys hit pretty much everything, um, that I thought of.

522

00:42:23.040 --> 00:42:27.760

And then you can see some of my mitigations over there. Um, uh, be aware of em.

523

00:42:27.760 --> 00:42:31.200

Usage, deconflict operations, um,

524

00:42:31.300 --> 00:42:35.480

verify the mission plan with a customer request and the, and, um,

525

00:42:36.000 --> 00:42:38.800

approved ATC route, um,

526

00:42:39.190 --> 00:42:42.600

must be sufficiently closed together to control the behavior of the UAV
and

527

00:42:42.600 --> 00:42:45.840

prevent it from conflicting with other aircraft. Um,

528

00:42:46.600 --> 00:42:49.000

operator must be provided with, uh, air traffic,

529

00:42:49.020 --> 00:42:52.920

any air traffic changes to ensure the UAV is properly de conflicting from
other

530

00:42:53.120 --> 00:42:54.480

aircraft. Um,

531

00:42:55.260 --> 00:42:59.960

and it must aircraft or autopilot must say the GPS waypoint received by
the uav.

532

00:43:01.650 --> 00:43:02.483

Okay.

533

00:43:02.520 --> 00:43:05.100

So there should be some kind of check to make sure that that happens.

534

00:43:06.100 --> 00:43:11.070

So we pretty much hit all the ones I was, uh, I thought of for this one.

535

00:43:11.650 --> 00:43:15.850

Any questions on that? What you got

536

00:43:25.220 --> 00:43:27.950

test unique and credible? Um,

537

00:43:27.950 --> 00:43:30.630
so I think part of it is scoping,

538

00:43:30.860 --> 00:43:34.870
scoping your safety control structure correctly. Uh, so,

539

00:43:35.170 --> 00:43:37.670
so focus it on the,

540

00:43:37.770 --> 00:43:41.910
the actual system that's under test and the test procedures and all that
type of

541

00:43:41.910 --> 00:43:46.510
stuff. You saw what Murph did with, with his loyal Wingman case where he,

542

00:43:46.730 --> 00:43:48.670
he had all the test, um,

543

00:43:48.670 --> 00:43:52.030
test elements that were orange and the system on our test was purple,

544

00:43:52.300 --> 00:43:56.310
just to make it very easily understandable what the system is

545

00:43:59.450 --> 00:44:00.283
Process.

546

00:44:04.440 --> 00:44:05.273
Say again?

547

00:44:05.730 --> 00:44:08.540
Like, as you're coming up with the bosses hazards and,

548

00:44:08.870 --> 00:44:10.990
cause they're not tracing,

549

00:44:13.450 --> 00:44:17.950
So they, they are. So your, your ucas, uh, are commands.

550

00:44:18.410 --> 00:44:22.910

Uh, so the question was, uh, the ucas and, and, uh,

551

00:44:23.630 --> 00:44:27.230

scenarios not traceable to the safety control structure. So, um,

552

00:44:27.970 --> 00:44:30.470

all the commands there that are on the safety control structure,

553

00:44:30.920 --> 00:44:33.060

you're gonna have a row in the,

554

00:44:33.610 --> 00:44:37.660

your UCA table for each single one of those. Um, so,

555

00:44:38.320 --> 00:44:41.660

so that's how it's traceable back to the safety control structure.

556

00:44:45.400 --> 00:44:48.490

Does that answer your question? I don't think it did. Kind of.

557

00:44:51.860 --> 00:44:52.693

All right.

558

00:44:55.140 --> 00:44:59.310

Yeah. And just to re reiterate what she said is that you're,

559

00:45:00.090 --> 00:45:03.550

you're not going through the yuca sort of at random, you're starting with this,

560

00:45:04.370 --> 00:45:07.080

right? And then you're generating your yukas cuz you're,

561

00:45:07.080 --> 00:45:10.360

you're looking at your controller, in this case, the operator,

562

00:45:11.020 --> 00:45:12.000

and then the command,

563

00:45:12.660 --> 00:45:16.160

and then you're generating your yuassas and then you're gonna go on to your next

564

00:45:16.220 --> 00:45:18.680

one. So you, you do it methodically.

565

00:45:18.980 --> 00:45:19.813

Mm-hmm.

566

00:45:21.640 --> 00:45:23.020

So I think what might be useful,

567

00:45:23.240 --> 00:45:27.540

so I have a table in the slides for the vehicle management system. Um,

568

00:45:28.720 --> 00:45:31.900

do you guys like to, to run through, if you go back, sorry,

569

00:45:31.900 --> 00:45:33.380

go back to the safety control structure.

570

00:45:34.190 --> 00:45:38.220

Let's pick one of the vehicle management system control actions and run through

571

00:45:38.570 --> 00:45:42.980

some ucas now that I think, uh, it's better explained. Better understood.

572

00:45:46.980 --> 00:45:51.080

How about the vehicle management system powering on the payload?

573

00:45:55.220 --> 00:45:57.680

All right, so if you go back to the,

574

00:45:59.930 --> 00:46:02.140

back to the UCA table, one more.

575

00:46:04.970 --> 00:46:08.150

All right. So if you type in there,

576

00:46:08.190 --> 00:46:12.950

you have to bring it outta presentation mode, put in, um,

577

00:46:14.550 --> 00:46:17.050

um, down below, put a

578

00:46:18.790 --> 00:46:21.140

power on or payload power on.

579

00:46:27.330 --> 00:46:27.800

There

580

00:46:27.800 --> 00:46:29.800

We go. All right.

581

00:46:29.860 --> 00:46:33.880

So when would not providing the payload power on

582

00:46:34.730 --> 00:46:35.563

cause a hazard

583

00:46:40.500 --> 00:46:44.360

Yep. Mission failure. So that's H three. Yep.

584

00:47:03.210 --> 00:47:05.070

Yep. You can say leading to mission failure,

585

00:47:05.250 --> 00:47:07.870

you could also say something to the effect of, you know, the,

586

00:47:07.870 --> 00:47:09.470

the ground troops don't get the data they need,

587

00:47:09.610 --> 00:47:14.390

or something along those lines as well. I think it all says the same thing.

588

00:47:14.860 --> 00:47:18.150

What about providing, when would, um,

589

00:47:19.500 --> 00:47:22.550

providing payload power on, cause a hazard

590
00:47:24.300 --> 00:47:25.133
That,

591
00:47:25.370 --> 00:47:26.550
Oh, go ahead. It sends

592
00:47:26.550 --> 00:47:27.510
A jettison signal to the

593
00:47:27.510 --> 00:47:29.860
Payload. It sends a jettison signal to the payload

594
00:47:31.180 --> 00:47:31.810
Parts

595
00:47:31.810 --> 00:47:36.730
Aircraft. Yep. Parts the aircraft. You one, two.

596
00:47:37.150 --> 00:47:37.470
Uh,

597
00:47:37.470 --> 00:47:39.450
No, I actually later.

598
00:47:39.840 --> 00:47:40.673
Okay.

599
00:47:42.900 --> 00:47:43.733
Condit,

600
00:47:45.190 --> 00:47:49.000
When there's an unsafe unsafe Yep. The payload's in unsafe condition.

601
00:47:51.940 --> 00:47:52.773
Mm-hmm.

602
00:47:52.820 --> 00:47:57.640
Yep. This, uh, another one. This, this particular aircraft had,

603

00:47:57.740 --> 00:48:02.640

uh, some power issues. Um, they actually added the, the second alternator to it.

604

00:48:03.140 --> 00:48:07.640

So, so maybe you, maybe you're having, uh, maybe the second alternator fails,

605

00:48:07.640 --> 00:48:11.920

you don't have enough power to power the payload and power the VMs.

606

00:48:12.630 --> 00:48:13.840

Something along those lines.

607

00:48:24.960 --> 00:48:25.650

Uh, I,

608

00:48:25.650 --> 00:48:30.620

I'll just point out that what will help I think with the causal scenarios is to

609

00:48:30.690 --> 00:48:34.380

have, uh, uh, the clear context or the circumstance.

610

00:48:35.200 --> 00:48:38.100

So for example, not providing, uh,

611

00:48:39.050 --> 00:48:43.860

results in mission failure would be missing the context of, of that,

612

00:48:44.280 --> 00:48:47.660

um, undesirable control action. So, uh,

613

00:48:47.800 --> 00:48:52.340

not powering on the payload when the troops need the data, you know,

614

00:48:52.500 --> 00:48:53.340

whatever the scenario is,

615

00:48:53.340 --> 00:48:57.260

that's the context that would help guide what the causal scenarios would be.

616
00:49:00.490 --> 00:49:01.323
Yeah.

617
00:49:02.090 --> 00:49:03.750
And we didn't talk about the hazards.

618
00:49:03.750 --> 00:49:08.470
So the VMs system provides a payload power on while the aircraft is in an

619
00:49:08.470 --> 00:49:09.910
unsafe condition for the payload.

620
00:49:10.410 --> 00:49:13.670
So what might be the hazards that trace to that one?

621
00:49:23.480 --> 00:49:24.380
The pain explode.

622
00:49:25.650 --> 00:49:29.700
Yeah. If the payloads explode, you lose the plane. Yep.

623
00:49:31.180 --> 00:49:35.560
Or the other one where the, uh, there's an electrical issue and it
departs,

624
00:49:35.950 --> 00:49:40.480
departs controlled flight. Say again? Yep.

625
00:49:42.000 --> 00:49:46.780
So you could do probably H four would probably be the good one.

626
00:49:53.080 --> 00:49:56.060
All right. Incorrect timing slash order.

627
00:49:56.760 --> 00:50:01.340
So the payloads provided payload power on command is provided too soon.

628
00:50:02.160 --> 00:50:03.580
Too late or out of order

629
00:50:07.550 --> 00:50:09.210
Too soon. Could overheat the payload

630
00:50:09.710 --> 00:50:12.530
Too soon. You could overheat the overheat, the payload. Yep.

631
00:50:12.530 --> 00:50:14.650
Maybe you can only be turned on for a certain amount of time

632
00:50:17.920 --> 00:50:19.370
Over overpower your generat.

633
00:50:19.710 --> 00:50:21.330
You could overpower your generator.

634
00:50:27.020 --> 00:50:27.853
The payload,

635
00:50:27.910 --> 00:50:32.420
Early release of the payload. Yeah. Maybe you're not over the target yet,

636
00:50:33.880 --> 00:50:37.460
so, or you've already passed the target, now you turn your payload on.

637
00:50:37.800 --> 00:50:38.780
So that could be too late.

638
00:50:44.440 --> 00:50:45.273
Any others?

639
00:50:48.120 --> 00:50:50.020
Too late? Your groups don't get the, uh,

640
00:50:50.880 --> 00:50:53.860
Yep. Too late. You're, they don't get the data. So that'd be H three.

641
00:51:00.120 --> 00:51:04.820
Say again? Yeah, yeah. Injure your support team,

642
00:51:04.970 --> 00:51:06.900

depending on what that payload is.

643

00:51:06.900 --> 00:51:10.740

Some kind of radar or something you expose people to, to RF on the ground.

644

00:51:10.740 --> 00:51:15.740

Something along those lines. Yep. That was a big one when I was working. Awax

645

00:51:27.690 --> 00:51:28.523

Multiple.

646

00:51:31.110 --> 00:51:35.050

So I typically have one row for,

647

00:51:35.230 --> 00:51:39.450

for a single command, but then I'll have multiple ucas in each box.

648

00:51:39.450 --> 00:51:44.130

So I think you saw that on, uh, the slide 67 there. Where,

649

00:51:44.260 --> 00:51:49.250

where I broke it out kind of in paragraphs within the same, um, I think,

650

00:51:49.370 --> 00:51:52.090

I think it, it's clean for me. Um,

651

00:51:52.110 --> 00:51:55.850

so then you'd have another box underneath for, um,

652

00:51:56.550 --> 00:51:59.770

one of the other launch now or some whatever the next command is down

653

00:52:03.660 --> 00:52:04.493

Cameo.

654

00:52:05.130 --> 00:52:09.190

I do not know. Never used cameo. No

655

00:52:09.680 --> 00:52:10.513

Cameo.

656

00:52:12.170 --> 00:52:16.510

Um, I think cameo had a separate line for each one. Uh,

657

00:52:16.510 --> 00:52:21.350

but because it was all connected, you could then sort and show, uh,

658

00:52:21.470 --> 00:52:23.950

okay, for this command, what are all the ucas you had? Mm-hmm.

659

00:52:24.580 --> 00:52:28.910

Yeah. I used Fancy Excel. So if you're using something better than that,

660

00:52:28.980 --> 00:52:32.910

that has some, some built in traceability, it'd make more sense to do each line.

661

00:52:33.170 --> 00:52:35.870

You know, anecdotally, we actually, on our next attempt,

662

00:52:35.920 --> 00:52:39.630

we're actually going back to Excel because there's a big learning curve,

663

00:52:40.130 --> 00:52:44.350

and we wanted to just work on the actual analysis and, uh,

664

00:52:44.410 --> 00:52:45.750

so we we're just doing it in Excel.

665

00:52:47.380 --> 00:52:52.350

Good feedback. All right. So if you go back to the, uh, VMs slide,

666

00:52:55.370 --> 00:52:59.550

all right. Stop too soon or applied too long, what are some,

667

00:52:59.740 --> 00:53:00.870

some ucas for that

668

00:53:11.940 --> 00:53:14.480

hit on? A couple already talked about the overheating.

669
00:53:14.480 --> 00:53:19.400
Maybe if you keep it on too long or if you turn it off before you've,

670
00:53:19.500 --> 00:53:23.360
uh, you've gotten all the, whatever the data is that needs to be
collected

671
00:53:30.010 --> 00:53:30.870
Too long, I guess.

672
00:53:33.530 --> 00:53:38.510
Yep. Too long you admit, uh, admit some rf. So it should be part of,

673
00:53:38.730 --> 00:53:43.270
you know, a, a whatever the pre pre landing checklist list looks like,

674
00:53:43.350 --> 00:53:44.183
something like that

675
00:53:45.520 --> 00:53:47.420
Too long. You could, uh, overwrite,

676
00:53:49.000 --> 00:53:50.020
Say again, too

677
00:53:50.020 --> 00:53:51.460
Long, you could overwrite your, uh,

678
00:53:51.460 --> 00:53:51.660
Data

679
00:53:51.660 --> 00:53:56.090
Storage. Oh, yeah. Overwrite your data storage. Yep. Definitely.

680
00:54:00.330 --> 00:54:02.510
Was this helpful? The second time going around?

681
00:54:11.130 --> 00:54:11.963
All right.

682
00:54:13.690 --> 00:54:15.110
So on this,

683
00:54:16.410 --> 00:54:19.670
it seems like overheating could be order,

684
00:54:22.160 --> 00:54:23.460
you're saying doesn't matter.

685
00:54:26.440 --> 00:54:30.660
So, um, you can put it in one, you can put it in both. Uh, uh,

686
00:54:30.790 --> 00:54:33.260
dunes made the, made the point that there may be,

687
00:54:33.560 --> 00:54:37.380
may be a scenario that's different and keeping it on too long versus,

688
00:54:37.480 --> 00:54:41.300
versus some of the others. So you may wanna just put it in, in all the,

689
00:54:41.880 --> 00:54:43.700
all the buckets where you think it could belong.

690
00:54:47.220 --> 00:54:51.760
And so at this point, there's several hazards that we haven't traced to yet. Um,

691
00:54:51.860 --> 00:54:54.560
so obviously if we went through this full analysis, we,

692
00:54:54.630 --> 00:54:59.120
we'd likely trace back to those hazards. But, uh, keep in mind this is,

693
00:54:59.120 --> 00:55:02.800
is that part of that iteration? So, so if, if you go through,

694
00:55:02.820 --> 00:55:05.040
you build out your UCA table and you,

695

00:55:05.060 --> 00:55:09.240

and you go back to your hazards and you have, you have not, um,

696

00:55:09.240 --> 00:55:10.080

addressed a hazard,

697

00:55:11.270 --> 00:55:14.960

that means that either maybe you're missing some ucas that you haven't thought

698

00:55:14.960 --> 00:55:18.760

about yet, or maybe that hazard, uh, shouldn't be considered.

699

00:55:18.760 --> 00:55:21.480

Maybe it's not really part of your system. So those are the,

700

00:55:21.480 --> 00:55:24.960

the two things that can happen there. Um, so,

701

00:55:24.980 --> 00:55:28.240

so that helps with the completeness as well. So if you go back and you're like,

702

00:55:28.240 --> 00:55:30.640

oh, I didn't, I didn't think about that hazard. How could,

703

00:55:30.700 --> 00:55:34.360

how could this command result in that? So it helps you, uh,

704

00:55:34.360 --> 00:55:36.040

make sure that you have a thorough analysis.

705

00:55:41.360 --> 00:55:46.100

All right. Any, any questions on that? Yes.

706

00:55:47.860 --> 00:55:52.020

I just asked Jeff the feeling that this is very brainstorming based.

707

00:55:52.490 --> 00:55:54.100

Yeah, it's kind of structured, brainstorming,

708

00:55:54.840 --> 00:55:55.673

Um,

709

00:55:55.720 --> 00:56:00.580

how I would end up with a feeling that I might not have had everything and

710

00:56:01.120 --> 00:56:04.740

be kind of incomplete. Is there a approach to, um,

711

00:56:05.520 --> 00:56:09.900

get more satisfaction of feeling having done a complete job?

712

00:56:10.200 --> 00:56:11.033

Mm-hmm.

713

00:56:11.440 --> 00:56:14.860

So, so the question was, uh, he feels like he may not have, uh,

714

00:56:15.490 --> 00:56:19.220

have a complete look with the analysis. So, so that,

715

00:56:19.570 --> 00:56:23.620

that iteration and going back and looking at the previous steps helps a lot with

716

00:56:23.620 --> 00:56:26.420

that. Um, the buckets help a lot with that.

717

00:56:26.420 --> 00:56:31.060

It helps you walk through all the different ucas that, that you could possibly,

718

00:56:31.640 --> 00:56:34.980

uh, you know, potentially come up with. And then for the scenarios,

719

00:56:35.160 --> 00:56:36.820

you have the different type 1, 2, 3,

720

00:56:36.820 --> 00:56:40.420

and four scenarios to help you walk through that safety control structure.

721
00:56:40.800 --> 00:56:45.740
So that gives you a decent idea. Um, I've yet to meet a perfect human,
so,

722
00:56:45.800 --> 00:56:49.500
so you're not gonna get this analysis perfect. Um, and,

723
00:56:49.880 --> 00:56:52.460
but I think you're gonna get something that's a pretty good product.

724
00:56:53.280 --> 00:56:55.740
And what's nice is because you have this traceability,

725
00:56:55.740 --> 00:56:58.620
because you have this set up, let's say, let's say you,

726
00:56:58.880 --> 00:57:02.660
you go out and test and you have some kind of unexpected test event,

727
00:57:03.840 --> 00:57:06.940
you have a really good analysis that can help you understand how that
occurred,

728
00:57:08.000 --> 00:57:09.140
uh, to, in order to,

729
00:57:09.240 --> 00:57:12.660
to build that into your system and prevent and understand the system
behavior

730
00:57:12.660 --> 00:57:14.380
that occurred, and then be able to,

731
00:57:14.800 --> 00:57:17.780
to get yourself back into a safe place to keep testing or,

732
00:57:17.840 --> 00:57:19.540
or make adjustments however you need to.

733
00:57:20.490 --> 00:57:25.020

Does the facilitator still in people who may not think of some of the things

734

00:57:25.020 --> 00:57:26.860

that they shoulda, is it,

735

00:57:27.240 --> 00:57:30.500

is it the role the facilitator keep pinging people?

736

00:57:31.240 --> 00:57:33.460

Uh, so the question was, is it the role of the facilitator to,

737

00:57:33.640 --> 00:57:36.420

to keep pinging people if folks aren't thinking about things?

738

00:57:36.680 --> 00:57:38.980

So the facilitator definitely can, uh,

739

00:57:38.980 --> 00:57:42.140

what's kind of nice is sometimes when you have a facilitator who's not

740

00:57:42.140 --> 00:57:45.220

necessarily an expert in that particular system, so they can,

741

00:57:45.220 --> 00:57:49.740

they can ask questions that, that you may not think about because you have your,

742

00:57:49.740 --> 00:57:53.180

your understanding of the system. Uh, so sometimes that helps. You'll say, Hey,

743

00:57:53.330 --> 00:57:56.820

what if this happened? You go, I never would've thought about that, but here's,

744

00:57:56.820 --> 00:57:58.620

here's how I think that might affect the system.

745

00:57:59.450 --> 00:58:03.220

Yeah, that was definitely my experience of the, our facilitator, you know,

746

00:58:04.030 --> 00:58:07.740

being from a completely different part of the company and not understanding what

747

00:58:07.740 --> 00:58:12.660

we were doing was able to keep kind of poking at us and making us think a little

748

00:58:12.660 --> 00:58:17.460

bit broader than we would've. Um, but, you know,

749

00:58:17.500 --> 00:58:20.460

I compare that to ths, which are

750

00:58:22.350 --> 00:58:25.130

by and large unstructured brainstorming. Um,

751

00:58:25.350 --> 00:58:27.090

and you compare that to this and the,

752

00:58:27.630 --> 00:58:32.450

the level of detail you're gonna end up at is just far greater because of this

753

00:58:33.170 --> 00:58:37.930

structure and focusing in on a single control. First off, defining what are,

754

00:58:37.990 --> 00:58:41.050

are all your controls? That's not something we normally do.

755

00:58:42.150 --> 00:58:46.570

You've so convincing yourself that you've covered every possible control action

756

00:58:46.570 --> 00:58:49.250

throughout the whole system that you're interested in.

757

00:58:49.790 --> 00:58:53.770

And then taking each control one at a time and spending

758

00:58:54.720 --> 00:58:57.570

however long it takes to convince yourself,

759

00:58:57.570 --> 00:59:01.850

you've covered all four different types of ways that it could turn into an

760

00:59:01.850 --> 00:59:06.460

unsafe control action, visa safe control action. Um,

761

00:59:08.280 --> 00:59:11.060

so I can tell you one of the things we learned was,

762

00:59:11.600 --> 00:59:13.340

and other people maybe,

763

00:59:14.870 --> 00:59:18.820

maybe it changes some too as you get more used to the process,

764

00:59:19.200 --> 00:59:24.020

but two hours was about our limit. Like two hours of doing this. Like,

765

00:59:24.080 --> 00:59:25.060

all right, we're done.

766

00:59:25.120 --> 00:59:29.060

You're not gonna do an eight hour workshop and pound this out. Um,

767

00:59:29.700 --> 00:59:34.430

it's a lot of thinking. Um, but that structure is what gives me the confidence.

768

00:59:34.460 --> 00:59:35.070

It's like, yeah,

769

00:59:35.070 --> 00:59:38.990

I think we turned over certainly a lot more rocks than I've ever turned over

770

00:59:38.990 --> 00:59:42.030

before and trying to do something like this. And it,

771
00:59:42.030 --> 00:59:44.950
so it just gives you a lot of confidence coming out of it. It's like,
yeah,

772
00:59:45.320 --> 00:59:48.030
maybe there's something that you might not uncovered,

773
00:59:48.770 --> 00:59:52.990
but you probably uncovered something very similar to it. Um,

774
00:59:53.010 --> 00:59:55.750
and you certainly uncovered a lot of things you wouldn't have thought of
if you

775
00:59:55.830 --> 00:59:59.430
hadn't been confronted with this rigid structure

776
01:00:00.770 --> 01:00:01.603
or detailed

777
01:00:01.710 --> 01:00:06.110
Structure. And, and kind of back to your experience, uh, question.

778
01:00:06.810 --> 01:00:09.990
Um, one of the smart sdpa people at our company,

779
01:00:10.650 --> 01:00:13.070
we were looking at this for another project, kind of mentioned how,

780
01:00:13.300 --> 01:00:16.510
what we need to make it a good experience. And I think what,

781
01:00:16.510 --> 01:00:19.430
what she was getting at, and Dr. Thomas said just as much, like,

782
01:00:19.610 --> 01:00:23.990
you're not gonna be able to do this after a, a one day workshop. Right?
Um,

783
01:00:24.090 --> 01:00:27.550

so the worst thing in his mind is that somebody tries to go and do an analysis

784

01:00:27.600 --> 01:00:31.510

using s stpa by themselves, uh, uh, and,

785

01:00:31.810 --> 01:00:34.670

and it goes horribly wrong, or they don't get anything out of it, and like,

786

01:00:34.670 --> 01:00:37.070

this is garbage, right? Um, uh,

787

01:00:37.090 --> 01:00:41.590

so having the facilitators there helped to guide us and actually come up with a

788

01:00:41.590 --> 01:00:45.190

good experience was important in my mind. And I think that's what Dr.

789

01:00:45.190 --> 01:00:46.070

Thomas was getting at.

790

01:00:48.340 --> 01:00:49.390

Yeah, I think there's,

791

01:00:49.390 --> 01:00:52.350

there's nuances with this that you may not pick up the first time,

792

01:00:52.490 --> 01:00:55.750

the second time. So it takes a few times to,

793

01:00:56.050 --> 01:00:59.310

to understand all of that and be able to be able to apply it.

794

01:00:59.310 --> 01:01:02.190

So having a facilitator is definitely a good thing.

795

01:01:05.290 --> 01:01:08.470

One question here. Um,

796

01:01:09.290 --> 01:01:12.550
the structure of the UCA table is this, um,

797
01:01:12.760 --> 01:01:17.190
let's say hard coded in how you do s stpa, these four,

798
01:01:17.800 --> 01:01:20.030
let's say columns, let's call them. Mm-hmm.

799
01:01:20.130 --> 01:01:24.350
Or is this based on your experience and do you think, uh, there could be,

800
01:01:24.710 --> 01:01:29.390
I don't know, reasons to deviate or expand or change these columns?

801
01:01:29.810 --> 01:01:34.750
So, uh, so this is part of the STPA methodology, and Dr.

802
01:01:34.860 --> 01:01:36.870
Levison, again, computer scientist, super,

803
01:01:37.160 --> 01:01:40.990
super theoretical math background has done,

804
01:01:41.380 --> 01:01:45.310
done work to show that, that if you, if you fill these buckets in,

805
01:01:45.310 --> 01:01:49.270
there's not gonna be anything, um, outside of that.

806
01:01:52.100 --> 01:01:53.590
Yeah. I looked at it the first time,

807
01:01:53.620 --> 01:01:57.270
read in the STPA handbook that there's only four ways you can screw something

808
01:01:57.270 --> 01:02:00.270
up. And my first thought was like, I gotta show this to my ex.

809
01:02:02.250 --> 01:02:05.630

But, and then I was like, I'm gonna prove this wrong. I was gotta be more ways.

810
01:02:06.090 --> 01:02:08.470
And yeah, she's right.

811
01:02:09.650 --> 01:02:13.270
So if you can find another way that it can be wrong with Dr. Levison,

812
01:02:13.310 --> 01:02:16.030
I sure like to hear about it, but it, it, it's amazing.

813
01:02:16.290 --> 01:02:17.230
The first thought is like,

814
01:02:17.230 --> 01:02:20.980
there's gotta be more ways to mess something up than just four categories,

815
01:02:21.160 --> 01:02:22.620
but it really fits.

816
01:02:25.850 --> 01:02:30.310
It seems like maybe this would lend itself to a curated list of

817
01:02:30.500 --> 01:02:31.333
prompts.

818
01:02:31.770 --> 01:02:32.790
Of prompts Yeah.

819
01:02:32.900 --> 01:02:35.470
That to get you thinking about something like mm-hmm. You know,

820
01:02:35.470 --> 01:02:40.230
it could use the HVAC nano codes for operator errors and work

821
01:02:40.230 --> 01:02:42.550
backwards from those. How would that manifest in,

822
01:02:42.970 --> 01:02:47.510

in this or overheating over cooling, stuff like that. Mm-hmm.

823

01:02:47.590 --> 01:02:49.070

So does such a thing exist?

824

01:02:49.850 --> 01:02:54.430

Uh, so, so no, not really. Uh, uh, I, I think,

825

01:02:54.910 --> 01:02:57.550

I think prompts are good, especially if you're doing this for the first time.

826

01:02:57.570 --> 01:03:00.910

The first time you do this and you have this, you know, white blanket, uh,

827

01:03:00.910 --> 01:03:03.790

piece of paper with, with these columns, it's,

828

01:03:03.820 --> 01:03:06.870

it's difficult to come up with things. It does help to have people.

829

01:03:06.870 --> 01:03:08.950

When I did this, I was, you know, I was a grad student,

830

01:03:09.070 --> 01:03:11.110

I was all on my own trying to, trying to come up with these,

831

01:03:11.250 --> 01:03:13.750

so I'm brainstorming with myself. Um,

832

01:03:13.820 --> 01:03:16.670

it's helpful when you have ideas that you can, you know,

833

01:03:16.670 --> 01:03:20.430

bounce off of folks and, and talk through things. Um, I, I think you can,

834

01:03:20.550 --> 01:03:25.110

I think you can also, um, uh, you can also use, uh,

835

01:03:25.110 --> 01:03:28.270

like for the scenarios, like I said, the, the different types. And,

836

01:03:28.410 --> 01:03:31.950

and going back to that control structure, I think is really helpful.

837

01:03:32.130 --> 01:03:33.790

You can kind of use it as a checklist,

838

01:03:34.250 --> 01:03:37.030

but you also wanna be careful with that because, uh, you know,

839

01:03:37.030 --> 01:03:40.270

if you have a set of prompts and you, okay, well, I went through these prompts,

840

01:03:40.330 --> 01:03:44.830

I'm now done. Maybe there were some other things out there. So, so, uh,

841

01:03:45.220 --> 01:03:46.630

just have to be careful with that,

842

01:03:46.630 --> 01:03:50.270

that you don't turn your brain off to some other, um, other things that,

843

01:03:50.270 --> 01:03:51.103

that could happen.

844

01:03:53.170 --> 01:03:57.190

How complex a system do you think can be analyzed with this tpa?

845

01:03:57.700 --> 01:04:02.470

I'll give you an example. We talked, uh, earlier today about a car and breaking,

846

01:04:02.870 --> 01:04:05.150

breaking too soon, breaking too hard, uh,

847

01:04:05.150 --> 01:04:07.390

beginning to move and the light changes. Uh,

848

01:04:07.630 --> 01:04:11.510

recently was a passenger in a Tesla with the autopilot function,

849

01:04:12.090 --> 01:04:14.830

and it was really amazing what it would do in traffic.

850

01:04:15.010 --> 01:04:19.070

It knew where the stoplights were, what they were. It could make left turns, um,

851

01:04:19.070 --> 01:04:22.630

waiting for traffic to clear, um, you know, how,

852

01:04:22.810 --> 01:04:27.510

how complex the system can we analyze and still do it reasonably

853

01:04:27.700 --> 01:04:31.550

efficiently without taking, you know, hours and days, et cetera. Mm-hmm.

854

01:04:31.970 --> 01:04:33.350

So you can get pretty complex.

855

01:04:33.490 --> 01:04:38.110

And actually this is really built for highly complex automated

856

01:04:38.160 --> 01:04:41.670

human integrated systems. So, so if,

857

01:04:41.730 --> 01:04:46.150

if it's too simple breaking in a car, breaking a car, I mean, we all have,

858

01:04:46.340 --> 01:04:49.550

have driven enough cars that we can probably come up with something,

859

01:04:49.780 --> 01:04:52.270

come up with some, some ideas of how that can,

860

01:04:52.380 --> 01:04:55.750

that can be dangerous without going through this rigorous process.

861

01:04:56.130 --> 01:04:58.590

So that was one thing that we were talking about during one of the breaks.

862

01:04:58.890 --> 01:05:03.110

If it's too simple of a program or, or, uh, or a system under test,

863

01:05:03.690 --> 01:05:07.750

you're probably gonna spend more time than you need. Your ROI is,

864

01:05:07.770 --> 01:05:12.510

is not very good, but the, the more complex a system is, that's,

865

01:05:12.510 --> 01:05:13.670

that's when you start to,

866

01:05:13.850 --> 01:05:17.410

you don't have a good mental model of what that looks like because it's beyond,

867

01:05:17.960 --> 01:05:22.100

uh, our understanding. Um, so, so that's when this actually becomes very,

868

01:05:22.100 --> 01:05:22.933

very useful.

869

01:05:23.160 --> 01:05:25.500

So I have a question. Um, so,

870

01:05:25.600 --> 01:05:30.100

so we're trying to get a buy-in of s stpa for flight test. So I,

871

01:05:30.540 --> 01:05:34.620

I think we all accept that it's good for system safety development for

872

01:05:35.580 --> 01:05:40.340

hardware or processes that are not flight test, but for flight test.

873

01:05:40.360 --> 01:05:44.660

So my question is, so you're teaching this at test, at the test pilot schools.

874

01:05:45.040 --> 01:05:46.700
Mm-hmm. At at least the Air Force.

875
01:05:47.180 --> 01:05:51.980
I don't know about the Navy or the other test pilot school. Uh, so,

876
01:05:53.640 --> 01:05:56.420
so what, what are you teaching at the test pilot school and,

877
01:05:56.880 --> 01:06:01.620
and are you getting some buy-in from the students?

878
01:06:01.760 --> 01:06:03.700
Are they coming out of the test pilot school saying,

879
01:06:04.010 --> 01:06:08.220
this is the way of the future, and I'm gonna do this when I graduate by,
gosh,

880
01:06:08.760 --> 01:06:13.220
you know, I, every test, uh, program that I'm gonna do, I'm gonna use
cpa,

881
01:06:13.280 --> 01:06:18.020
forget the ths, uh, the way they're structured right now. Mm-hmm.

882
01:06:19.000 --> 01:06:21.420
Uh, I'm just gonna, and then, then that's one question.

883
01:06:22.480 --> 01:06:27.100
And then how do you get from s TPA to get a, an approval from the, uh,

884
01:06:27.130 --> 01:06:31.820
authority from the person in charge? Mm-hmm. Uh, so how do you take,

885
01:06:31.850 --> 01:06:36.500
okay, we did, we've did, we've done the research, we did the s tpa, we
have,

886
01:06:36.640 --> 01:06:39.620
uh, the, the proper, uh, answers and mitigations.

887

01:06:40.240 --> 01:06:44.340

And now don't you have to go back to the, is it,

888

01:06:44.400 --> 01:06:46.660

is it low risk, high risk, or you don't have to do that?

889

01:06:46.680 --> 01:06:50.540

And then how do you get a buy-in from the guy who's gonna sign off on the test?

890

01:06:51.290 --> 01:06:53.900

Yeah. So, so this,

891

01:06:53.900 --> 01:06:58.180

this is not a probabilistic risk assessment, right? Um, so,

892

01:06:58.960 --> 01:07:02.860

but we're gonna have to wedge it into a risk matrix because that's what,

893

01:07:02.880 --> 01:07:06.620

that's what's expected. Um, so, so at some point,

894

01:07:07.160 --> 01:07:09.220

you're gonna have to, you know,

895

01:07:09.220 --> 01:07:12.420

take whatever data you have or take whatever background you have and,

896

01:07:12.680 --> 01:07:16.620

and put it on that risk matrix, unfortunately, because that's how our,

897

01:07:16.800 --> 01:07:21.140

our organizations are set up. Um, but, but that also,

898

01:07:21.600 --> 01:07:25.140

um, leads to the issue that we have with risk matrices, right?

899

01:07:25.140 --> 01:07:29.660

Like you go back to that Fukushima example that, that Murph talked about.
Um,

900
01:07:29.760 --> 01:07:33.140
the, the fact that, that you can have this low probability, well,

901
01:07:33.520 --> 01:07:35.580
what's the probability if you have, you know,

902
01:07:35.650 --> 01:07:40.220
your one in one in a thousand years tsunami, but it's gonna flood the basement.

903
01:07:40.220 --> 01:07:43.340
It's one, you know, so, so that's,

904
01:07:43.480 --> 01:07:47.220
that's the issue unfortunately with that. But unfortunately,

905
01:07:47.280 --> 01:07:50.180
I'm not gonna change that. No question was

906
01:07:51.160 --> 01:07:55.020
That's why you getting outta Yeah. Outta this, the students,

907
01:07:55.130 --> 01:07:58.900
what is the outcome? Are they coming out, they buying and are they gonna

908
01:07:58.920 --> 01:08:02.460
Use it? Yes. I think, I think students are coming out, uh,

909
01:08:02.720 --> 01:08:07.100
un understanding that this is, is a powerful method. Um, they're,

910
01:08:07.100 --> 01:08:10.820
they're going into organizations where sometimes they have leeway to,

911
01:08:10.820 --> 01:08:14.940
to do this type of thing. Sometimes they don't. It depends on, depends on,

912
01:08:15.060 --> 01:08:17.820
you know, their supervisors, their leadership they have and their particular,

913

01:08:18.320 --> 01:08:21.900

uh, you know, test squadron. Um, so, so, but I,

914

01:08:22.020 --> 01:08:26.180

I think they do see the power of it. One of the things that we've talked about,

915

01:08:26.480 --> 01:08:28.620

and I think I've mentioned this before, lunch too, is,

916

01:08:28.800 --> 01:08:30.940

is if you do that safety control structure,

917

01:08:31.450 --> 01:08:33.780

just that in and of itself is powerful.

918

01:08:33.970 --> 01:08:37.820

Just getting us on the same mental model of understanding the system is

919

01:08:38.100 --> 01:08:41.420

powerful. So that's, that's one of the big things we, we talk about is just,

920

01:08:41.690 --> 01:08:45.860

just to change your mindset and be able to create a functional diagram of your

921

01:08:45.860 --> 01:08:49.620

system and be able to have conversations, even if you don't go through the rest,

922

01:08:49.890 --> 01:08:52.420

even if you don't go through the UCAS and the,

923

01:08:52.420 --> 01:08:53.700

the scenarios and the mitigations,

924

01:08:54.130 --> 01:08:57.540

that in and of itself can provide a lot of value to an organization,

925

01:08:57.680 --> 01:08:58.513
to a test program.

926
01:09:01.910 --> 01:09:03.160
Another question over here,

927
01:09:06.700 --> 01:09:07.533
I'm not sure

928
01:09:08.780 --> 01:09:09.840
The mic is on the move

929
01:09:13.090 --> 01:09:14.600
Dunes is getting us steps in today.

930
01:09:20.980 --> 01:09:21.813
Mm-hmm.

931
01:09:22.990 --> 01:09:27.360
Yeah. So, uh, my question is, um, there, there are two questions. So first, um,

932
01:09:27.720 --> 01:09:32.560
I remember from the early morning slides that we had that, um,

933
01:09:32.850 --> 01:09:36.720
there was a chart that showed like there is complexity mm-hmm.

934
01:09:36.980 --> 01:09:41.560
But systems are organized complexity, right? It, it's not completely chaotic,

935
01:09:41.780 --> 01:09:46.120
and thereby statistical methods are not best suited. So mm-hmm.

936
01:09:46.590 --> 01:09:51.520
With, with, with the stpa philosophy and stamp, are I, is the,

937
01:09:51.820 --> 01:09:56.040
is it recommended that, you know, probabilistic methods are not right for, uh,

938

01:09:56.040 --> 01:09:58.840

system safety? Or would you say that's not the case?

939

01:09:59.380 --> 01:10:03.200

So I, I think, I think some,

940

01:10:03.200 --> 01:10:06.240

sometimes probabilistic assessments are good if you,

941

01:10:06.300 --> 01:10:10.600

if you have the data and, and, uh, they can be helpful.

942

01:10:11.460 --> 01:10:13.440

Um, but what you don't wanna say is,

943

01:10:13.560 --> 01:10:16.200

I multiplied all of these things and I got a really small number.

944

01:10:16.280 --> 01:10:19.440

I don't have to think about anything else. I can assume it away. What,

945

01:10:19.440 --> 01:10:24.120

what I think this shows you is that, uh, one, um, uh,

946

01:10:24.260 --> 01:10:28.600

you know, if, if something does happen, it's no longer a teeny tiny, you know,

947

01:10:28.660 --> 01:10:33.240

10 to the negative 26th number. Um, and then I think the,

948

01:10:33.340 --> 01:10:36.520

the other aspect is there's a lot, when you talk about human behavior,

949

01:10:36.630 --> 01:10:40.520

when you talk about software integration, you cannot put probabilities on that.

950

01:10:40.860 --> 01:10:43.880

What's the probability that I'm gonna accidentally hit the wrong button?

951
01:10:44.700 --> 01:10:48.600
You know, I do or I don't. Um, there there's no probability and there's,

952
01:10:48.600 --> 01:10:52.640
there's been attempts to try to, to try to create, um, uh,

953
01:10:52.640 --> 01:10:55.600
probabilities for human behavior. Um, and it's,

954
01:10:55.630 --> 01:11:00.080
it's largely not been super effective because how you're gonna react in the

955
01:11:00.280 --> 01:11:01.120
situation is different than you,

956
01:11:01.120 --> 01:11:04.720
is different than me based off of our training and experience and knowledge and

957
01:11:04.720 --> 01:11:05.553
all that type of stuff.

958
01:11:06.070 --> 01:11:10.400
Okay, thanks. And the other thing is, we are talking about, um, commands, right?

959
01:11:10.420 --> 01:11:14.580
Mm-hmm. Like it's more like a controlled centric, um, way of doing it.

960
01:11:15.320 --> 01:11:16.153
Um,

961
01:11:16.320 --> 01:11:21.140
but there are cases where like the responding system or whatever it is that

962
01:11:21.140 --> 01:11:24.500
they're receiving, and it doesn't do its job. Like, for example,

963
01:11:25.160 --> 01:11:29.980

you send a command to an AOR on to deflect and it jams. Mm-hmm. Um,

964

01:11:30.480 --> 01:11:33.060

how does that get captured, would you say?

965

01:11:33.400 --> 01:11:35.900

We throw it in the providing causes hazard bucket?

966

01:11:36.840 --> 01:11:41.700

So, so what I would do is, um, in that case, so,

967

01:11:41.920 --> 01:11:45.300

so the, the UCA would be something like, uh, you know, the,

968

01:11:45.320 --> 01:11:48.940

the pilot does not provide, um, uh,

969

01:11:48.940 --> 01:11:52.780

the aileron command when it needed to be, you know, needed to bank or whatever.

970

01:11:53.560 --> 01:11:56.060

Um, and then, and then when you do the scenarios,

971

01:11:56.640 --> 01:12:00.020

you can say back to the type one, two, and three, and four, you can say, well,

972

01:12:00.020 --> 01:12:04.500

what if, what if the pilot did provide that command, but something happened,

973

01:12:05.000 --> 01:12:09.060

uh, either either in the communication route or there's a mechanical failure or

974

01:12:09.060 --> 01:12:11.540

something like that. So that's where you get to that level of detail.

975

01:12:12.570 --> 01:12:13.660

Okay. Thanks. Mm-hmm.

976

01:12:15.440 --> 01:12:16.273

All right.

977

01:12:22.760 --> 01:12:26.060

So I think, Darren, you said earlier this morning here, um,

978

01:12:26.800 --> 01:12:31.700

one of the benefits out this, uh, is it helps work past the, you know, the, the,

979

01:12:32.160 --> 01:12:35.540

the, the mental breakdown, so to speak, or the mental model breakdown here.

980

01:12:35.540 --> 01:12:38.460

And so I wanna go ahead and use this example that I think we used this morning

981

01:12:38.460 --> 01:12:42.060

again in the Fukushima thing. And I think, uh, where,

982

01:12:42.070 --> 01:12:45.940

where I'm having a problem connecting the dots is when you get to the causal

983

01:12:46.500 --> 01:12:50.780

scenarios kind of thing. And in particular, that example where the switch, uh,

984

01:12:50.880 --> 01:12:53.860

was co-located with the generator in the basement that flooded.

985

01:12:54.640 --> 01:12:56.100

And while you can say, Hey,

986

01:12:56.280 --> 01:12:59.660

the switch fails to operate when you're doing your ucas kind of thing there,

987

01:12:59.720 --> 01:13:02.060

in this case, that's, you know, I think what one of the,

988
01:13:02.060 --> 01:13:05.260
one of the issues was there. And then you get to the causal scenario,
well,

989
01:13:05.260 --> 01:13:07.420
why would this switch fail to operate? And you say, well,

990
01:13:07.420 --> 01:13:09.540
maybe there was a fire. You say, Hey,

991
01:13:09.540 --> 01:13:12.660
well okay then we can put a fire suppression system in there.

992
01:13:12.660 --> 01:13:16.740
Maybe a mitigator for it kind of thing there. But, you know, that may be,

993
01:13:16.800 --> 01:13:18.420
you know, that's a mental model kind of thing there.

994
01:13:18.560 --> 01:13:21.180
But who would think in the causal scenario, Hey,

995
01:13:21.180 --> 01:13:24.580
we're gonna get a one in a million flood kind of thing there that's gonna
flood

996
01:13:24.580 --> 01:13:26.900
both the generator out and then,

997
01:13:26.900 --> 01:13:30.380
and cause a switch to not operate kind of thing there. So it gets me back
to,

998
01:13:30.380 --> 01:13:33.700
aren't we still going back where we have to have these mental models kind
of

999
01:13:33.700 --> 01:13:36.300
thing there and someone has to come up with the idea, Hey,

1000
01:13:36.300 --> 01:13:39.500

we're gonna get a one in a million flood that would cause a switch not to

1001

01:13:39.500 --> 01:13:40.420
operate. I,

1002

01:13:40.460 --> 01:13:44.580
I just wonder if anybody actually presuppose that and how this would get
us to

1003

01:13:44.580 --> 01:13:48.540
that point. Where had we had done this analysis, you know,

1004

01:13:48.540 --> 01:13:49.620
when Fukushima was built,

1005

01:13:50.150 --> 01:13:53.500
would someone have come to the conclusion as a causal scenario, Hey,

1006

01:13:53.500 --> 01:13:55.100
this room could flood mm-hmm.

1007

01:13:55.210 --> 01:13:58.420
When there was no history ever have it happened before, perhaps. And,

1008

01:13:58.520 --> 01:14:00.540
and they would've come to the same conclusion and said, Hey,

1009

01:14:00.540 --> 01:14:02.940
we've gotta locate the switch somewhere else.

1010

01:14:05.400 --> 01:14:05.940
So I,

1011

01:14:05.940 --> 01:14:09.340
I think you would find it in the Fukushima case because they had a sea
wall.

1012

01:14:09.340 --> 01:14:14.060
They knew that that flooding due to, due to a tsunami, was a, was a
threat,

1013

01:14:14.640 --> 01:14:18.420

um, to that particular power station. So that was, that was a, that was a known,

1014

01:14:19.320 --> 01:14:20.980

um, a known situation.

1015

01:14:21.520 --> 01:14:24.900

So I think what what would happen is you'd have a command is you,

1016

01:14:24.900 --> 01:14:27.260

as you went through this, you'd have a command that says something like,

1017

01:14:27.560 --> 01:14:31.740

you know, switch, you know, switch from onsite generators to,

1018

01:14:31.920 --> 01:14:35.220

to offsite generators or something like that. And then you'd be like, well,

1019

01:14:35.360 --> 01:14:37.940

why wouldn't that happen? And you'd be like, oh crap, we put,

1020

01:14:38.320 --> 01:14:41.740

we put the switches in the basement where it's gonna flood. And so,

1021

01:14:41.800 --> 01:14:42.660

so I think it would,

1022

01:14:42.780 --> 01:14:47.660

I think it would come out because you would be talking about the tsunami and the

1023

01:14:47.660 --> 01:14:48.360

flood risk.

1024

01:14:48.360 --> 01:14:49.100

But, but I,

1025

01:14:49.100 --> 01:14:52.620

I think the disconnect that I have is they say we already mitigated that by

1026

01:14:52.740 --> 01:14:55.500

building the sea wall. Mm-hmm. You see what I'm saying? So they said, Hey,

1027

01:14:55.500 --> 01:14:59.260

you know, that's done. We, we mitigated that one by building the seawall.

1028

01:14:59.260 --> 01:15:01.820

Mm-hmm. So the basement won't get flood, kinda thing. Mm-hmm.

1029

01:15:01.940 --> 01:15:04.380

So then they had to presuppose then that, Hey,

1030

01:15:04.380 --> 01:15:07.700

what happens if the sea wall breaks down kinda thing? It seems like you struck,

1031

01:15:07.700 --> 01:15:10.060

ended up going down a rabbit hole that could probably last forever,

1032

01:15:10.110 --> 01:15:12.500

Kinda thing. Well, I think I, I,

1033

01:15:13.330 --> 01:15:18.020

what my hope would be is that by using this kind of structured approach

1034

01:15:18.680 --> 01:15:20.180

at some point Yeah.

1035

01:15:20.180 --> 01:15:23.100

Whether they realized it was going to be because of flooding or not,

1036

01:15:23.610 --> 01:15:25.380

they might not catch that. Yeah.

1037

01:15:25.520 --> 01:15:29.020

But I would hope that when they've ran numbers that says we're 10 to the minus

1038

01:15:29.040 --> 01:15:32.380

27, and then they realize we've got one switch,

1039

01:15:33.550 --> 01:15:36.280

that they would've figured out a way to have more switches involved.

1040

01:15:36.980 --> 01:15:39.680

And as they start down that and kind of get zeroed in on,

1041

01:15:39.770 --> 01:15:43.560

we've got a single point failure on the 10 to the minus 27 probability event,

1042

01:15:45.070 --> 01:15:48.840

that part of that would be that realization that like, hey,

1043

01:15:48.840 --> 01:15:51.320

we already decided we need a generator way up the hill.

1044

01:15:51.850 --> 01:15:55.440

Maybe we should have three switches and one of those switches should be way up

1045

01:15:55.440 --> 01:15:58.120

the hill. And so that you don't necessarily have to,

1046

01:15:58.120 --> 01:15:59.840

because that's one of the things that always haunts,

1047

01:16:00.510 --> 01:16:04.440

certainly myself when we talk about flight test, right. Of like,

1048

01:16:04.500 --> 01:16:06.920

what's the Fukushima event for us? And,

1049

01:16:07.340 --> 01:16:11.600

and especially when it comes to our higher risk tests,

1050

01:16:11.810 --> 01:16:15.480

which a lot of those are ones that we might fly every three years or every 10

1051

01:16:15.480 --> 01:16:20.200
years, or, you know, the higher the risk tests and what least likely we
are to,

1052
01:16:20.260 --> 01:16:24.720
to fly it on a regular basis. And so if we think that it's a,

1053
01:16:25.140 --> 01:16:25.973
you know, a,

1054
01:16:26.160 --> 01:16:30.600
a medium probability and or a low probability and catastrophic

1055
01:16:31.220 --> 01:16:32.720
in the history of our organization,

1056
01:16:32.780 --> 01:16:34.680
we don't have enough data to prove that we're right.

1057
01:16:36.020 --> 01:16:37.520
And so are we fooling ourselves?

1058
01:16:37.540 --> 01:16:41.600
Are we missing something and getting lucky in the 20 times we've flown
that

1059
01:16:41.600 --> 01:16:42.960
condition? Um,

1060
01:16:43.220 --> 01:16:47.240
or do we have it right and have we covered everything or do we have a
single

1061
01:16:47.240 --> 01:16:50.080
switch somewhere that we just haven't flooded yet?

1062
01:16:50.420 --> 01:16:54.040
And it comes down to that, uh, don't, you know,

1063
01:16:54.780 --> 01:16:58.160
not not having the priest conceived notions, right? Like, oh yeah,

1064
01:16:58.740 --> 01:17:03.200
that's not a problem. The switch is behind a sea wall, you know, we're good. Uh,

1065
01:17:03.460 --> 01:17:07.560
low probability of it's failing, right? But the going through the process,

1066
01:17:08.830 --> 01:17:12.660
okay, well, there's a control action. The switch has to switch, um,

1067
01:17:12.660 --> 01:17:15.620
the power in the case of, uh, of the generators failing in the basement.

1068
01:17:16.290 --> 01:17:20.060
What are the causal scenarios that would cause that it asks a question where,

1069
01:17:20.060 --> 01:17:22.660
whereas before you just may not even ask it, right? Yeah.

1070
01:17:23.130 --> 01:17:26.620
Yeah. I, and I think, I think to your point, I mean, again, no,

1071
01:17:27.240 --> 01:17:30.820
no analysis that, that we ever do will be a hundred percent complete.

1072
01:17:30.840 --> 01:17:33.780
That's just, that's just not possible. Um,

1073
01:17:33.780 --> 01:17:36.940
unless we find a way to become perfect. So, um,

1074
01:17:37.110 --> 01:17:42.060
which apparently according to your ex, you're not, I don't, uh, but, uh,

1075
01:17:42.280 --> 01:17:45.380
but, but I think it gives you a good shot of,

1076
01:17:45.560 --> 01:17:49.980
of being pretty close to, to as, as good as we humanly can.

1077

01:17:50.560 --> 01:17:53.700

So, so sometimes I think I'm a, I'm a hope, I'm a,

1078

01:17:54.600 --> 01:17:57.340

I'm very much an optimistic person, and sometimes I think I,

1079

01:17:57.420 --> 01:18:00.740

I talk about this like it's a panacea. There's no such thing as a panacea.

1080

01:18:00.960 --> 01:18:04.740

But I think, I think it is a, it is fair, very thorough,

1081

01:18:04.800 --> 01:18:07.540

and it's gonna get you to think about things that you may not have thought of

1082

01:18:08.300 --> 01:18:10.620

previously. Get a

1083

01:18:10.900 --> 01:18:13.540

Question. Yeah, I was just gonna add that if you go with a purely, uh,

1084

01:18:13.540 --> 01:18:14.940

statistical approach, right?

1085

01:18:15.250 --> 01:18:18.260

It's easy to fall into the trap of thinking that all of your probabilities are

1086

01:18:18.260 --> 01:18:21.900

independent of each other. But going through this exercise,

1087

01:18:22.060 --> 01:18:24.100

I think will help you realize that like,

1088

01:18:24.100 --> 01:18:27.860

if a single causal event could knock down three of my probabilities,

1089

01:18:28.130 --> 01:18:31.860

then it's not really three probabilities, right? It's really one probability.

1090

01:18:32.320 --> 01:18:36.580

And so then that may spur you to put some extra mitigations in place. So I,

1091

01:18:36.580 --> 01:18:39.060

I don't know if it, it may not necessarily be a flood. I mean,

1092

01:18:39.060 --> 01:18:41.100

you mentioned maybe the, maybe the basement would be on fire,

1093

01:18:41.400 --> 01:18:43.820

but going through that, that similar exercise, just with the fire,

1094

01:18:43.920 --> 01:18:44.700

you would say, okay,

1095

01:18:44.700 --> 01:18:47.020

so that turns out we have generators in the basement and the switch in the

1096

01:18:47.140 --> 01:18:49.780

basement, and it's not, they're not two separate probabilities,

1097

01:18:50.400 --> 01:18:52.140

so it may still lead you down that path.

1098

01:18:53.130 --> 01:18:55.140

Yeah, that's, that's a very good point. When you're,

1099

01:18:55.140 --> 01:18:57.060

when you're doing that assessment, you're assuming,

1100

01:18:57.480 --> 01:19:00.580

you're assuming that these are not interdependent on each other.

1101

01:19:00.580 --> 01:19:04.420

They're completely independent, uh, systems or subsystems.

1102

01:19:05.080 --> 01:19:07.260

And sometimes that assumption is, is not correct.

1103

01:19:07.320 --> 01:19:10.180

And especially as you go more and more complex, uh, there,

1104

01:19:10.180 --> 01:19:14.820

there are tons of inter interdependencies between our subsystems and that

1105

01:19:14.820 --> 01:19:19.260

becomes less and less of a reality. Is there another question?

1106

01:19:20.520 --> 01:19:21.290

If not,

1107

01:19:21.290 --> 01:19:26.180

I've got a few takeaway slides and then we'll see if we've got some,

1108

01:19:26.400 --> 01:19:27.940

uh, time for some more questions.

1109

01:19:34.450 --> 01:19:34.880

Yeah,

1110

01:19:34.880 --> 01:19:38.900

Go for it. All right. So, um, hopefully what you,

1111

01:19:38.900 --> 01:19:43.580

what you got out of this is you focus on, on system behavior. And,

1112

01:19:43.760 --> 01:19:47.260

uh, we've talked, we've talked a lot offline with different folks about, okay,

1113

01:19:47.260 --> 01:19:49.700

well this is great for flight tests, but you know,

1114

01:19:49.700 --> 01:19:51.700

we're dumped a system and now we gotta build this.

1115

01:19:51.700 --> 01:19:55.220

And this is a lot of work to put this safety control structure together and

1116

01:19:55.220 --> 01:19:59.380

everything else. And so really, uh, in ideal Sarah land, uh,

1117

01:19:59.380 --> 01:20:01.780

the designers would start this. And so this is,

1118

01:20:01.780 --> 01:20:03.700

this is one way to to think about that.

1119

01:20:03.960 --> 01:20:07.220

So you can use it very early on in the design phase, uh,

1120

01:20:07.220 --> 01:20:11.460

to understand the functionality and the concept of operations of whatever system

1121

01:20:11.460 --> 01:20:15.300

that's trying to be developed. So I, I did a lot of AR testing,

1122

01:20:15.600 --> 01:20:17.740

so I go back to that a lot. Um,

1123

01:20:17.740 --> 01:20:21.660

so imagine we've never had aerial refueling before. We wanna create the first,

1124

01:20:22.040 --> 01:20:26.940

the first tinker aircraft. Um, so we've got a refuel aircraft of some kind.

1125

01:20:27.190 --> 01:20:32.060

We've got a receiver aircraft of some kind. And then if you hit next,

1126

01:20:33.720 --> 01:20:36.740

you can do an STPA analysis on that, hit next again.

1127

01:20:37.360 --> 01:20:40.620

And then what you're gonna get is mission assurance requirements associated with

1128

01:20:40.620 --> 01:20:44.340

that, that are gonna f that are gonna then flow through, uh,

1129

01:20:44.380 --> 01:20:48.060

the rest of your design analysis. So if you hit next, again,

1130

01:20:48.680 --> 01:20:51.420

so some things you might think about is, uh,

1131

01:20:51.420 --> 01:20:54.620

how is receiver communicating that it's ready to take on fuel?

1132

01:20:54.880 --> 01:20:57.820

How does it communicate if there's some kind of abnormal issue, condition,

1133

01:20:57.820 --> 01:21:01.140

that type of thing. Uh, how does it disconnect from the refuel?

1134

01:21:01.240 --> 01:21:06.100

So physical disconnect of some kind, and then, uh, with the refuel,

1135

01:21:06.100 --> 01:21:09.060

or how does it connect, disconnect, how does it feel flow, fuel?

1136

01:21:09.520 --> 01:21:10.900

How does it communicate position?

1137

01:21:11.320 --> 01:21:14.020

So one of the things to think about with this is right now we are,

1138

01:21:14.020 --> 01:21:16.820

we are form agnostic. This is purely function.

1139

01:21:17.000 --> 01:21:19.780

We don't know how it's gonna communicate. Is it voice?

1140

01:21:20.000 --> 01:21:23.580

Is it some kind of physical electrical connection there, some kind of wifi land?

1141
01:21:23.800 --> 01:21:25.700
We don't know. We haven't made that decision yet,

1142
01:21:26.120 --> 01:21:30.500
but we know that this is probably how something like this ought to look.

1143
01:21:30.960 --> 01:21:35.460
And you can actually go through this and do, do that s STP analysis. So,

1144
01:21:35.600 --> 01:21:39.460
so what happens if the receiver, um, you know,

1145
01:21:39.670 --> 01:21:43.660
isn't able to disconnect? And you can go through that analysis, um,

1146
01:21:43.960 --> 01:21:48.180
and get some really good information that then you can, you can plug into
your,

1147
01:21:48.330 --> 01:21:52.060
into your design requirements. So I think this is pretty powerful. You,

1148
01:21:52.120 --> 01:21:54.180
you can't, there's very little, uh,

1149
01:21:55.410 --> 01:21:59.060
ability with other hazard analysis, um, to,

1150
01:21:59.060 --> 01:22:02.180
to do that before you even have designed a system. Um,

1151
01:22:02.200 --> 01:22:06.780
but s stpa allows you to do that. Um,

1152
01:22:07.000 --> 01:22:11.780
so few of you guys probably know what the UTA loop is. Um,

1153
01:22:11.880 --> 01:22:16.500
so, uh, this is my version of that design safety loop. So,

1154
01:22:16.560 --> 01:22:20.300
so you design, you have some kind of design, you know, the previous
slide,

1155
01:22:20.330 --> 01:22:23.220
it's just two elements, right? Uh, you analyze that,

1156
01:22:23.440 --> 01:22:27.300
you input your mitigations in your system, and then as you design,

1157
01:22:27.320 --> 01:22:30.180
as you get to a more detailed design, you can flow that through,

1158
01:22:30.180 --> 01:22:34.780
which you'll see in the next slide. Uh, so we're all very familiar with,

1159
01:22:34.850 --> 01:22:38.060
with the v the systems engineering V. Um,

1160
01:22:38.230 --> 01:22:42.700
often the, the requirements, if you got your requirements wrong,

1161
01:22:43.400 --> 01:22:45.660
uh, which is the basis of anything that we do,

1162
01:22:45.960 --> 01:22:48.780
you're not gonna notice it until you get to the right side of the,

1163
01:22:48.780 --> 01:22:52.220
of the V When you start to realize, you start to integrate, you start to
test,

1164
01:22:52.760 --> 01:22:55.340
uh, what this allows you to do is,

1165
01:22:55.440 --> 01:22:59.460
is look to see if those requirements are right through an s t P analysis
of your

1166
01:22:59.560 --> 01:23:03.980

conops early, early on in the requirements development. As you go through,

1167

01:23:04.400 --> 01:23:09.230

you refine that. And then,

1168

01:23:09.730 --> 01:23:12.110

uh, once, once you have those requirements developed,

1169

01:23:12.280 --> 01:23:16.150

those TPA requirements can be tested just like any other technical requirement

1170

01:23:16.150 --> 01:23:16.983

that you might have.

1171

01:23:17.170 --> 01:23:20.150

Do you have some kind of endurance requirement or anything else? Uh, you can,

1172

01:23:20.150 --> 01:23:24.590

you can test those. And then what happens if your system behavior, um,

1173

01:23:24.650 --> 01:23:28.470

is not as expected? Um, so maybe,

1174

01:23:28.560 --> 01:23:32.950

maybe your design was flawed or maybe the operation of the system wasn't within

1175

01:23:33.130 --> 01:23:35.910

the bounds, the design bounds, uh, that,

1176

01:23:36.020 --> 01:23:38.150

that unfortunately happens often as well.

1177

01:23:38.150 --> 01:23:40.230

There's probably a couple others in there as well.

1178

01:23:40.890 --> 01:23:44.710

But now you can go back in your analysis and try to understand, uh,

1179

01:23:44.810 --> 01:23:46.310

was that there's an issue with the design.

1180

01:23:46.530 --> 01:23:50.670

Did it operate in a way that we didn't intend it, uh, when we did the design?

1181

01:23:51.690 --> 01:23:56.390

Um, and those vmv, uh, results can be fed back into your TPA analysis. So you,

1182

01:23:56.390 --> 01:23:58.990

you already have the functional behavior model, uh,

1183

01:23:59.010 --> 01:24:02.710

so you can feed that back in. And what's nice about that is that you're getting,

1184

01:24:02.730 --> 01:24:03.710

you're getting a,

1185

01:24:04.150 --> 01:24:08.710

a holistic systems approach to solving whatever those deficiencies are that were

1186

01:24:08.710 --> 01:24:13.470

found and test. Uh, so leading indicators,

1187

01:24:14.370 --> 01:24:18.630

um, this is a big one. We wanna know that we're about to step off a cliff, uh,

1188

01:24:18.630 --> 01:24:23.230

before we step off the cliff typically. Um, so, so sociotechnical systems,

1189

01:24:23.970 --> 01:24:28.590

uh, trends towards unsafe or unsecure scenarios. Let's imagine we had,

1190

01:24:28.810 --> 01:24:32.150

we created the, the safest aircraft you could come up with.

1191
01:24:32.490 --> 01:24:35.470
All the operators are well trained. All the maintainers know what they're doing.

1192
01:24:35.700 --> 01:24:37.790
They all have the right tools and equipment,

1193
01:24:37.790 --> 01:24:42.110
everything that they need to be successful. As soon as you hit go, uh,

1194
01:24:42.120 --> 01:24:44.510
we're trending towards an unsafe environment. You've got,

1195
01:24:44.510 --> 01:24:49.270
you've got personnel changes, uh, you change your procedures, um,

1196
01:24:49.270 --> 01:24:53.910
you make, uh, updates and modifications to, to whatever that system is, um,

1197
01:24:54.210 --> 01:24:57.830
et cetera. You list a a few there. Um, and so there's,

1198
01:24:57.830 --> 01:25:02.270
there's been a lot of research into, into how, um,

1199
01:25:02.410 --> 01:25:06.310
you trend into, uh, unsafe environments. If anyone knows beaker, wicker,

1200
01:25:06.620 --> 01:25:08.870
he's done some, some good papers on that.

1201
01:25:09.900 --> 01:25:13.960
But you can come up with some leading indicators to be aware out of your STP

1202
01:25:14.160 --> 01:25:17.040
analysis to be aware that you're heading down on safe path.

1203
01:25:17.420 --> 01:25:21.400
So one is documented assumptions. I foot stomped that a lot today. So,

1204

01:25:21.460 --> 01:25:26.360

so if you say, Hey, I don't think this is gonna be an issue because, uh,

1205

01:25:26.360 --> 01:25:28.200

it's already, um, you know,

1206

01:25:28.200 --> 01:25:30.480

there's already a regulation that tells me I have to do this thing,

1207

01:25:31.200 --> 01:25:33.560

document that. Cuz what happens if that regulation changes?

1208

01:25:34.060 --> 01:25:37.520

You have no traceability if you haven't documented it to understand that that's

1209

01:25:37.520 --> 01:25:40.120

gonna affect your safety analysis. Uh,

1210

01:25:40.120 --> 01:25:43.560

and then safety constraints and mitigations. So, um,

1211

01:25:43.700 --> 01:25:47.960

so if you have constraints and mitigations in place and then in the,

1212

01:25:47.980 --> 01:25:49.760

in the test or the operation of your vehicle,

1213

01:25:50.020 --> 01:25:53.960

you start to find that you're violating those safety constraints or safety

1214

01:25:53.960 --> 01:25:57.480

mitigations, you're trending to an unsafe, uh, situation.

1215

01:25:58.980 --> 01:26:03.740

And, uh, you know, we talk a lot about incidents often proceed mishaps. So,

1216

01:26:03.880 --> 01:26:08.580

so from an TPA perspective, what that means is you've, you've,

1217

01:26:08.880 --> 01:26:12.380

um, realized a hazard but you did not realize the loss.

1218

01:26:12.380 --> 01:26:14.980

That's really what an incident is. So that gives,

1219

01:26:14.980 --> 01:26:18.660

that gives you the opportunity to go back and look at your analysis and,

1220

01:26:18.760 --> 01:26:23.140

and see, see what occurred to try to prevent a future mishap.

1221

01:26:26.050 --> 01:26:29.420

Alright, so I talked about this at the, at the beginning of the day.

1222

01:26:29.780 --> 01:26:34.420

I talked about how I did KC 1 35 testing and then I did KC 46 testing.

1223

01:26:35.160 --> 01:26:39.060

So, uh, some of the major differences between between them are, uh,

1224

01:26:39.060 --> 01:26:41.580

the boom operator has a direct view of the receiver.

1225

01:26:41.580 --> 01:26:46.180

They're looking out the window. Um, they also have a lot of non-visual cues.

1226

01:26:46.290 --> 01:26:50.340

They use, they use the, um, bow wave as the aircraft comes up closer.

1227

01:26:50.370 --> 01:26:52.300

They can feel that, um,

1228

01:26:52.300 --> 01:26:55.780

they also have feedback through the boom cuz it's a hydro mechanical system.

1229

01:26:56.000 --> 01:26:59.300

So they can feel when they're pushing through, uh, or when they've, with,

1230

01:26:59.300 --> 01:27:03.220

when they've made contact or when they disconnect in the KC 46,

1231

01:27:03.370 --> 01:27:06.780

they're using cameras, they're using 3D glasses. Uh,

1232

01:27:06.780 --> 01:27:10.260

so it's different visual feedback and they're non-visual cues.

1233

01:27:10.260 --> 01:27:11.540

They're up in the front of the aircraft.

1234

01:27:11.540 --> 01:27:13.860

They're no longer feeling that bow wave. Uh,

1235

01:27:13.930 --> 01:27:17.940

they don't get the tactile feedback, uh, from, from their stick.

1236

01:27:18.200 --> 01:27:22.380

So those non-visual cues are gone. So the, the losses,

1237

01:27:23.440 --> 01:27:26.500

um, damage to or loss of receiver or tanker are,

1238

01:27:26.520 --> 01:27:31.020

are the same for both for what the 1 35 and the KC 46 and the hazards are the

1239

01:27:31.020 --> 01:27:34.540

same. Emitter, collision, boom, strike fuel system, incompatibility,

1240

01:27:34.540 --> 01:27:38.140

those are the three main things you're looking for. Um, but,

1241

01:27:38.160 --> 01:27:41.020

but now that you've had a chances chance to go through ucas,

1242

01:27:41.020 --> 01:27:43.540

you've had a chance to go through scenarios, uh,

1243
01:27:43.540 --> 01:27:47.100
do you think that they're gonna be the same for those two two particular?

1244
01:27:47.910 --> 01:27:52.210
All right, I'm seeing some, some left and right nos that's good. Um,
yeah,

1245
01:27:52.210 --> 01:27:53.850
they're gonna be different. They're gonna be different.

1246
01:27:54.360 --> 01:27:57.890
UCAS will probably be roughly the same, but,

1247
01:27:58.110 --> 01:28:02.130
but the scenarios and the mitigations for those scenarios are absolutely
gonna

1248
01:28:02.130 --> 01:28:04.170
be different. Um,

1249
01:28:04.390 --> 01:28:07.210
do you think the probability of a hazard will be greater or smaller?

1250
01:28:10.550 --> 01:28:15.130
Who knows? That's, that's kind of the point. Uh, we don't,

1251
01:28:15.130 --> 01:28:17.650
we don't know necessarily what the probability of,

1252
01:28:17.650 --> 01:28:19.770
of that human system interaction is gonna be.

1253
01:28:22.380 --> 01:28:26.440
All right, so we've talked about risk a little bit already. Um, so again,

1254
01:28:26.440 --> 01:28:30.480
it's a, you don't get risk out of this right's, a hazard identification
tool.

1255
01:28:30.900 --> 01:28:33.000

Um, but it does,

1256

01:28:33.000 --> 01:28:35.920

what it does really well is it identifies some of the unknowns.

1257

01:28:35.920 --> 01:28:38.200

It helps you walk through this, this process,

1258

01:28:38.270 --> 01:28:41.680

this very structured process to make you think about things that you may not

1259

01:28:41.680 --> 01:28:45.840

have thought about otherwise. Um, and, um,

1260

01:28:46.140 --> 01:28:50.520

you get a lot, you get this traceable, these traceable, um, mitigations,

1261

01:28:50.520 --> 01:28:53.880

these recommendations, whatever you'd like to call them, um, that,

1262

01:28:53.880 --> 01:28:57.000

that feed back up, uh, to your hazard analysis. So,

1263

01:28:57.380 --> 01:29:01.980

so depending on the hazards, like for example, the, the test case,

1264

01:29:02.720 --> 01:29:06.980

um, that, uh, uh, dunes and Darren talked about, they had,

1265

01:29:06.980 --> 01:29:08.420

they had essentially like a,

1266

01:29:08.660 --> 01:29:12.380

a test efficiency hazard and then they had some more serious hazards.

1267

01:29:12.800 --> 01:29:15.460

So one way that you can look at this again cuz we're,

1268

01:29:15.460 --> 01:29:17.820

we have resource constraints, um,

1269

01:29:18.040 --> 01:29:22.900

is maybe you accept a scenario that traces back to a

1270

01:29:22.900 --> 01:29:25.620

loss of test efficiency. Maybe you say, you know what, I'm willing,

1271

01:29:25.760 --> 01:29:28.380

I'm willing to fly a few extra sorties. Um,

1272

01:29:28.380 --> 01:29:30.860

but then you have another scenario that traces back to something more

1273

01:29:30.860 --> 01:29:34.340

significant damage to your set injury, that type of thing. Um,

1274

01:29:34.560 --> 01:29:38.540

and you choose not to accept that risk. So that helps cuz one of the,

1275

01:29:38.560 --> 01:29:42.220

one of the common questions I get out of this is, okay,

1276

01:29:42.300 --> 01:29:44.140

I found 300 scenarios.

1277

01:29:44.700 --> 01:29:48.820

I don't have time or resources or people or, um, to,

1278

01:29:49.400 --> 01:29:53.940

to mitigate all those 300 scenarios. So what do I do? Um, so that's,

1279

01:29:54.030 --> 01:29:57.100

those are kind of one of the ways to do it is look at,

1280

01:29:57.100 --> 01:29:59.140

look at the hazard that it traces back to,

1281

01:29:59.450 --> 01:30:03.300

what are you willing to accept as far as risk within your system?

1282

01:30:04.000 --> 01:30:07.420

And the other thing too, and, and these guys found it in their test case,

1283

01:30:08.000 --> 01:30:12.980

was there are certain mitigations that, uh, resolve multiple scenarios.

1284

01:30:13.280 --> 01:30:16.540

And there's sometimes scenarios that that resolve, uh,

1285

01:30:16.820 --> 01:30:21.500

multiple or trace back to multiple ucas trace, trace back to multiple hazards.

1286

01:30:21.500 --> 01:30:24.940

So sometimes there's some low hanging fruit that if I do this one thing,

1287

01:30:25.480 --> 01:30:28.660

I'm gonna, I'm gonna satisfy or mitigate, uh, you know,

1288

01:30:28.660 --> 01:30:32.020

10 or 15 different scenarios so that, so you can get after those as well.

1289

01:30:32.240 --> 01:30:34.380

So the way you aggregate the,

1290

01:30:34.380 --> 01:30:37.620

the mitigations and understand that traceability is key,

1291

01:30:37.670 --> 01:30:40.740

since we're not coming up with some kind of probabilistic risk assessment.

1292

01:30:44.240 --> 01:30:47.780

All right, so I think we've, we've talked about this, um,

1293

01:30:47.780 --> 01:30:52.180

pretty significantly already. Um, again, emergent properties,

1294

01:30:53.280 --> 01:30:57.740

um, are, are very difficult to, to calculate a number.

1295

01:30:58.560 --> 01:31:00.860

Um, and when you have highly coupled,

1296

01:31:00.860 --> 01:31:04.940

which we talked about highly coupled systems, when you have human agency,

1297

01:31:05.210 --> 01:31:09.700

when you have complex software, uh, it's, you, you really can't put,

1298

01:31:10.320 --> 01:31:13.780

um, a, a probability to that. Um,

1299

01:31:14.800 --> 01:31:17.780

and then on the severity, severity side,

1300

01:31:18.170 --> 01:31:21.420

that feeds right back to your hazards and to your losses. So,

1301

01:31:21.480 --> 01:31:25.780

so we do look at the severity as part of s stpa, it's the probability,
uh,

1302

01:31:25.780 --> 01:31:29.180

that we don't consider. All right?

1303

01:31:31.040 --> 01:31:34.940

Um, so what do we do? I think I've talked about a decent amount of this
already,

1304

01:31:35.240 --> 01:31:40.060

but, um, but what this gives you is the ability to, to understand,

1305

01:31:40.840 --> 01:31:45.220

uh, various consequences of, of the scenarios. Uh,

1306

01:31:46.240 --> 01:31:49.220

and I think of, I think it probably beat this dead horse on,

1307

01:31:49.280 --> 01:31:51.580

on determining probability, but,

1308

01:31:52.000 --> 01:31:54.980

but hopefully you guys understand there's a lot that we do that you simply

1309

01:31:55.000 --> 01:31:58.260

cannot put a probability on. I have some examples there.

1310

01:31:58.410 --> 01:32:01.540

What happens if we missed a critical safety of flight test parameter during

1311

01:32:01.540 --> 01:32:05.180

safety, uh, planning? What's the, what's the probability of that occurring?

1312

01:32:06.520 --> 01:32:11.250

It's one or zero. Those are your two options. Uh, that's, so, and same with,

1313

01:32:11.280 --> 01:32:14.770

same with all of those other ones. It's one or zero, uh, which,

1314

01:32:14.900 --> 01:32:18.570

which makes our job of risk management, uh,

1315

01:32:18.570 --> 01:32:21.010

harder and risk communication, that's the big thing, right?

1316

01:32:21.190 --> 01:32:22.970

We all have to get approval for our test program.

1317

01:32:23.150 --> 01:32:26.890

So how do we communicate that risk? I talked about the,

1318

01:32:27.030 --> 01:32:29.530

the two different ways to, to, uh,

1319

01:32:30.030 --> 01:32:33.450

to work through the frequency and then the trade off priorities.

1320

01:32:34.630 --> 01:32:35.490

Any questions on that?

1321

01:32:41.350 --> 01:32:42.410

All right. Oh,

1322

01:32:44.790 --> 01:32:48.610

So, um, other challenge that

1323

01:32:57.430 --> 01:33:00.170

the right or time, right?

1324

01:33:00.230 --> 01:33:04.690

So time and you're looking at performance.

1325

01:33:14.040 --> 01:33:17.250

Yeah, so the comment, the comment was, um,

1326

01:33:17.530 --> 01:33:21.610

a lot of times these probabilities are over the lifespan of an aircraft,
uh, so,

1327

01:33:21.610 --> 01:33:25.450

you know, thousands and thousands and thousands of hours, whereas the,

1328

01:33:25.450 --> 01:33:30.450

the time span of the flight test program is a lot shorter. So, so that,

1329

01:33:30.600 --> 01:33:34.130

that reduces your, your exposure to risk. Um, but,

1330

01:33:34.270 --> 01:33:36.850

but can you still calculate what that risk might be?

1331

01:33:37.120 --> 01:33:40.410

Yeah. And the exposure time is very small, so that time,

1332

01:33:42.690 --> 01:33:43.523

whatever

1333

01:33:51.000 --> 01:33:51.833

Yeah.

1334

01:33:52.070 --> 01:33:52.903

One flight test.

1335

01:33:53.800 --> 01:33:58.330

Yeah. So if you have one flight test event and you divide it a small number by a

1336

01:33:58.330 --> 01:34:01.570

smaller number, you get something that, that may or not be helpful,

1337

01:34:01.710 --> 01:34:02.970

may not be helpful. Yep.

1338

01:34:03.470 --> 01:34:07.650

Agreed. Those prob probabilities are often based on normal operations as well,

1339

01:34:08.020 --> 01:34:09.610

which is not what we do. So.

1340

01:34:11.150 --> 01:34:11.983

Yep.

1341

01:34:13.970 --> 01:34:14.803

Question over here.

1342

01:34:17.350 --> 01:34:17.950

So, uh,

1343

01:34:17.950 --> 01:34:22.250

you just mentioned something there that touches on a question that I had.

1344

01:34:22.470 --> 01:34:27.290

So you, when you said with the KC 46 you have strong visual cues,

1345

01:34:27.290 --> 01:34:30.370

but you don't have tactile cues, you don't have the bow wave,

1346

01:34:30.390 --> 01:34:32.730

you don't have something else. You mentioned something,

1347
01:34:33.150 --> 01:34:37.410
but what that made me think is that when we did the initial fundamentals,

1348
01:34:37.880 --> 01:34:42.450
something could either send a command or something can send feedback,
right?

1349
01:34:42.450 --> 01:34:46.810
Mm-hmm. And I got the impression there that you get less feedback

1350
01:34:48.080 --> 01:34:50.250
with the new system than with the old system,

1351
01:34:50.990 --> 01:34:53.170
and that introduces its own risks.

1352
01:34:54.150 --> 01:34:58.540
So you know how we did the analysis of command, uh,

1353
01:34:58.540 --> 01:35:03.140
given at the wrong time or too long, or receipt or command given or not
given.

1354
01:35:03.400 --> 01:35:06.060
Mm-hmm. So we looked at things that could send commands,

1355
01:35:06.060 --> 01:35:08.060
which is basically do this. Mm-hmm.

1356
01:35:08.490 --> 01:35:13.220
What about things that rely on feedback or feedback dependent like,

1357
01:35:13.220 --> 01:35:17.580
like that, like what you said. So do we have to go through a similar, uh,

1358
01:35:17.980 --> 01:35:20.580
exercise for things that, uh,

1359
01:35:20.640 --> 01:35:23.140
are not commanding an action,

1360
01:35:23.280 --> 01:35:26.420
but things that are receiving feedback?

1361
01:35:27.050 --> 01:35:27.340
Yeah.

1362
01:35:27.340 --> 01:35:29.780
Cause cuz if, if the refueling system,

1363
01:35:30.400 --> 01:35:32.740
if the guy sitting or girl sitting in the back,

1364
01:35:32.740 --> 01:35:35.500
lady sitting in the back with the, who could visually see it,

1365
01:35:35.800 --> 01:35:37.140
who could feel when the,

1366
01:35:37.320 --> 01:35:41.620
the bomber comes up and who can fly the boom because they could actually feel

1367
01:35:41.620 --> 01:35:45.980
the stick forces to engage the, uh, the, the probe.

1368
01:35:46.680 --> 01:35:50.300
But if you remove that feedback, which is non-visual,

1369
01:35:50.720 --> 01:35:55.220
and you put the solely visual and they're struggling to do it,

1370
01:35:55.490 --> 01:35:57.340
then you've introduced, uh,

1371
01:35:57.530 --> 01:36:01.100
more a different set of failure modes because you've compromised the feedback

1372
01:36:01.780 --> 01:36:02.613
fidelity.

1373

01:36:02.890 --> 01:36:07.340

Yeah. So, so what, what you do, so you go through the,

1374

01:36:07.480 --> 01:36:12.220

the UCA process, right? And that's, that's all command specific. Um, when,

1375

01:36:12.220 --> 01:36:15.780

when you work through the scenarios, that's where the feedback comes back in.

1376

01:36:16.180 --> 01:36:20.020

Remember when I talked about the mental model and the control algorithm?

So,

1377

01:36:20.400 --> 01:36:23.500

so how does, how does the mental model, so, so the,

1378

01:36:23.500 --> 01:36:27.500

the boom operators mental model of, of where,

1379

01:36:27.750 --> 01:36:31.940

where the probe is in relation to the other aircraft or where the aircraft is in

1380

01:36:32.220 --> 01:36:35.100

relation to, to the refuel or, um, how,

1381

01:36:35.280 --> 01:36:39.660

how does that change as a result, uh, of a new system? So that's,

1382

01:36:39.660 --> 01:36:42.460

that's where that would feed into. So, so let's say,

1383

01:36:42.960 --> 01:36:45.660

I'm trying to think of a good example. Uh,

1384

01:36:46.130 --> 01:36:50.100

it's not gonna happen off the top of my head, but, um, uh, where,

1385

01:36:50.100 --> 01:36:54.660

where a boom operator does something, something that's unsafe, um, um,

1386

01:36:55.270 --> 01:37:00.140

maybe they, they, uh, try to try to connect and they, they,

1387

01:37:00.240 --> 01:37:03.060

uh, hit outside the slipway or something along those lines.

1388

01:37:03.370 --> 01:37:07.700

What would cause that to happen? So, so the mental model is he,

1389

01:37:07.800 --> 01:37:10.420

he probably thought he was gonna hit inside the slipway,

1390

01:37:10.420 --> 01:37:14.300

otherwise he or she wouldn't have done it. Um, so then you can talk about, well,

1391

01:37:14.300 --> 01:37:17.940

what would make that person think that they are? And so,

1392

01:37:18.000 --> 01:37:20.500

so that's where that feedback loop would come into.

1393

01:37:20.500 --> 01:37:22.020

And I think I didn't cover that very well,

1394

01:37:22.240 --> 01:37:26.560

so I appreciate you pointing that out. And that's another thing too,

1395

01:37:26.560 --> 01:37:28.680

when you go through those scenarios is you can look,

1396

01:37:28.680 --> 01:37:32.840

look at all the feedback that you have going back to that controller and,

1397

01:37:32.840 --> 01:37:34.840

and what happens if that feedback's not there?

1398

01:37:34.870 --> 01:37:38.120

What happens if that feedback is late? Um, you know,

1399

01:37:38.180 --> 01:37:40.560

how is that feedback presented to the operator?

1400

01:37:40.970 --> 01:37:44.480

Those are some of the types of things that you can think about as you go through

1401

01:37:44.480 --> 01:37:48.320

that analysis to, to create the scenarios associated with the uca,

1402

01:37:48.930 --> 01:37:50.880

Which is why it's powerful.

1403

01:37:51.340 --> 01:37:54.840

TPA is powerful in the design phase because you might find that there is a piece

1404

01:37:54.840 --> 01:37:56.860

of feedback that is missing, uh,

1405

01:37:56.860 --> 01:37:59.300

and catch it there as opposed to at the other end.

1406

01:38:00.270 --> 01:38:01.103

Yep.

1407

01:38:04.410 --> 01:38:09.190

All right. Next slide. All right. I think this is my,

1408

01:38:09.410 --> 01:38:14.110

my last slide. Um, so we, we've talked about coupling already,

1409

01:38:14.570 --> 01:38:17.790

but modern systems are, are tightly coupled, which,

1410

01:38:17.840 --> 01:38:21.670

which makes some of that probabilistic assessment, uh, inaccurate.

1411

01:38:21.730 --> 01:38:26.070

It also creates emergent properties where if you, if you, uh,

1412

01:38:26.070 --> 01:38:30.990

reduce your system to various subsystems, um, that those, um,

1413

01:38:31.220 --> 01:38:34.910

subsystem feedback and, and, and, um,

1414

01:38:35.410 --> 01:38:39.310

is not gonna be present. Those, those coupling, that coupling is not gonna be,

1415

01:38:39.610 --> 01:38:44.310

uh, present when you do that analysis as you reduce those subsystems. Um,

1416

01:38:44.850 --> 01:38:48.470

and, uh, uh, I think we've, I think we've hit probabilistic risk,

1417

01:38:48.580 --> 01:38:50.670

risk assessment pretty, pretty hard already.

1418

01:38:51.130 --> 01:38:53.870

But understand your system ask tough questions,

1419

01:38:54.290 --> 01:38:59.070

really understands that safety control structure. Um, I've, it's really,

1420

01:38:59.140 --> 01:39:01.750

it's really neat being in the room when folks are doing this with,

1421

01:39:01.750 --> 01:39:04.230

with whatever their test program is, and they,

1422

01:39:04.340 --> 01:39:07.910

they get this understanding of the system under tests that they did not

1423

01:39:07.910 --> 01:39:09.030

understand before,

1424

01:39:09.410 --> 01:39:13.230

and they're asking questions that they didn't think to ask until they actually

1425

01:39:13.450 --> 01:39:16.590

saw, saw their system, uh, you know, up on,

1426

01:39:16.610 --> 01:39:18.950

up on a whiteboard or PowerPoint or whatever,

1427

01:39:19.130 --> 01:39:23.430

and it gave them a different viewpoint, uh, of their system. Um,

1428

01:39:24.690 --> 01:39:26.510

and then focus on the functionality.

1429

01:39:27.080 --> 01:39:31.550

We're all super technical and it's easy to dive into the details. You know,

1430

01:39:31.550 --> 01:39:36.270

when you're talking about hazards, focus on those system level states,

1431

01:39:36.890 --> 01:39:40.070

uh, of, of whatever your system under test is, um,

1432

01:39:40.120 --> 01:39:42.910

don't dive into the details yet. You will find time, uh,

1433

01:39:43.010 --> 01:39:47.670

to do that as you go through the analysis. Um, and then if a,

1434

01:39:47.670 --> 01:39:51.990

if a mishap does happen, uh, dig into the systemic cause,

1435

01:39:52.370 --> 01:39:56.670

try to understand it. So, so cast analysis, um,

1436

01:39:57.290 --> 01:40:00.750

is, is another falls under the stamp umbrella. Uh,

1437

01:40:01.170 --> 01:40:03.990

so if a mishap occurs, uh,

1438
01:40:04.060 --> 01:40:06.830
cast is how you can investigate that mishap,

1439
01:40:06.980 --> 01:40:10.950
essentially using the same system, theoretic underpinnings. Um,

1440
01:40:10.950 --> 01:40:12.990
and it's a pretty powerful tool. Uh,

1441
01:40:12.990 --> 01:40:17.710
what's nice is if you've done s tpa and then, and then something happens,

1442
01:40:18.130 --> 01:40:20.830
you already have your system, your safety control structure.

1443
01:40:21.130 --> 01:40:23.310
So now you can try to understand, okay, was,

1444
01:40:23.490 --> 01:40:25.990
was there an aspect of the system behavior that I,

1445
01:40:25.990 --> 01:40:30.190
that we didn't understand and we didn't properly capture in our analysis,
uh,

1446
01:40:30.290 --> 01:40:33.630
was, was there a command or a feedback, um, that,

1447
01:40:33.630 --> 01:40:37.790
that was missing or out of order, et cetera with, with the ucas that we
created?

1448
01:40:38.130 --> 01:40:41.870
So you can really understand your system and then hopefully come up with
a,

1449
01:40:41.870 --> 01:40:45.670
with a fix that's, that's, um, uh, systemic and holistic.

1450
01:40:48.010 --> 01:40:52.470
All right, next slide. All right, so,

1451
01:40:52.850 --> 01:40:57.740
um, that first link there, that, that's, uh, Nancy Levinson's, uh,

1452
01:40:57.740 --> 01:41:00.740
homepage at mit, and you're gonna have,

1453
01:41:00.870 --> 01:41:03.660
we're gonna post these slides so you don't necessarily have to scribble that

1454
01:41:03.660 --> 01:41:07.820
down. Um, that's where they're gonna have information about the,

1455
01:41:08.080 --> 01:41:12.460
the S stpa workshop or stamp workshop that's gonna happen in June.

1456
01:41:12.840 --> 01:41:17.420
So again, that, that's a free workshop. It's gonna be virtual, so you can,

1457
01:41:17.520 --> 01:41:21.540
you can sign up and, and hit whatever you wanna hit on that. Um,

1458
01:41:22.020 --> 01:41:26.940
MPHs PhD, uh, dissertation is there, got my, uh,

1459
01:41:26.960 --> 01:41:29.660
my master's thesis. And then, um, again,

1460
01:41:29.660 --> 01:41:33.420
some of the workshop information in the handbook, there's an S STPA handbook,

1461
01:41:33.500 --> 01:41:37.180
I believe now there's also a CAST handbook as well. So those are two,

1462
01:41:37.280 --> 01:41:41.340
two really good resources. The, the S STPA handbook has been, uh,

1463
01:41:41.340 --> 01:41:46.100

translated into I think 12 or 15 different languages as well. Uh,

1464

01:41:46.100 --> 01:41:49.020

so there's, there's a lot of worldwide interest, uh, in that.

1465

01:41:53.610 --> 01:41:56.050

I also add that TPA workshop

1466

01:41:56.590 --> 01:42:01.530

As Dr. John Thomas. Mm-hmm. Give an introduction to stpa, uh,

1467

01:42:02.430 --> 01:42:06.650

as, as a web podcast, so you can listen to him as,

1468

01:42:06.790 --> 01:42:09.730

as a compliment to what we learned today. Mm-hmm. Give a little

1469

01:42:09.730 --> 01:42:10.050

Bit more

1470

01:42:10.050 --> 01:42:14.130

Detail. Yeah. Dr. Thomas is gonna, is gonna provide a,

1471

01:42:14.290 --> 01:42:18.170

a tutorial at the workshop. He is far smarter than I am,

1472

01:42:18.270 --> 01:42:23.050

and he actually does this every day versus it's my, it's my side gig. Um, so,

1473

01:42:23.830 --> 01:42:26.730

so I definitely recommend, and he, he has tremendous energy.

1474

01:42:27.250 --> 01:42:30.970

I love listening to that guy. He will get you excited about life. It's awesome.

1475

01:42:31.550 --> 01:42:34.370

And he's there in the 2020 workshop, you

1476

01:42:35.960 --> 01:42:40.450

Yeah. 2020 workshop, uh, that he, he came and participated in that.

1477

01:42:41.740 --> 01:42:46.470

Thank you. All right.

1478

01:42:48.890 --> 01:42:51.510

Any other, any other questions?

1479

01:42:56.250 --> 01:43:00.470

Did you get Yep.

1480

01:43:05.660 --> 01:43:09.310

Yeah. So stamp is the theoretical underpinning, um,

1481

01:43:10.020 --> 01:43:14.950

systems theoretic something model something

1482

01:43:15.160 --> 01:43:15.510

model

1483

01:43:15.510 --> 01:43:16.120

And process.

1484

01:43:16.120 --> 01:43:18.510

There we go. Yeah. Um, and so,

1485

01:43:18.930 --> 01:43:21.150

so you have stamp is the theoretical underpinning,

1486

01:43:21.330 --> 01:43:23.910

and then you have TPA and cast, uh,

1487

01:43:23.910 --> 01:43:27.630

which are more the applications associated with the theoretical underpinning.

1488

01:43:32.920 --> 01:43:36.930

Any other questions? All right.

1489

01:43:37.750 --> 01:43:41.330

So I guess I can, uh, hand it back and I'll be,

1490
01:43:41.390 --> 01:43:45.570
I'm here the rest of the next couple of days, so if you have questions,
um,

1491
01:43:45.730 --> 01:43:49.570
sidebars or whatever, please, uh, please come find me.

1492
01:44:03.380 --> 01:44:04.213
Thanks.

1493
01:44:09.670 --> 01:44:12.640
Well, I was, uh, fantastic. Um,

1494
01:44:13.590 --> 01:44:17.200
I've heard lots about s stpa over the last few years and, uh,

1495
01:44:17.790 --> 01:44:21.480
it's always been this nebulous thing that I was like, sounds great.

1496
01:44:21.790 --> 01:44:24.000
Show me the money, right? Uh,

1497
01:44:24.060 --> 01:44:27.560
how on earth do you actually implement this in a real world scenario?

1498
01:44:27.560 --> 01:44:32.000
Especially from my point of view as a test safety, uh, person,

1499
01:44:32.240 --> 01:44:34.680
I really wanna see how do you get the meat and potatoes outta this and
actually

1500
01:44:34.680 --> 01:44:39.480
implement it. And I think today, finally, the light was turned on. So,
uh,

1501
01:44:39.480 --> 01:44:42.440
I think you guys did a fantastic job. I really appreciate the effort.

1502
01:44:42.440 --> 01:44:46.120

That was a lot of work that both Dunes, Sarah and Darren all put together here.

1503

01:44:46.860 --> 01:44:49.520

Um, really, I, for me, it's like, okay, I,

1504

01:44:49.840 --> 01:44:52.360

I think I understand enough now that I could actually ask an intelligent

1505

01:44:52.680 --> 01:44:54.680

question. Um, barely. But, you know,

1506

01:44:54.780 --> 01:44:56.600

and we can actually start to move forward with this.

1507

01:44:56.700 --> 01:44:59.400

So I just really wanna say thanks to everyone, um,

1508

01:44:59.900 --> 01:45:02.880

as a little moment of our appreciation dunes, you can come back up here too,

1509

01:45:02.880 --> 01:45:06.280

where'd you run off to? So, got a little thank you for all of you folks.

1510

01:45:07.820 --> 01:45:09.240

Little, uh, gift

1511

01:45:13.420 --> 01:45:15.040

for you. Thank you, thank you, thank you.

1512

01:45:15.420 --> 01:45:18.320

And if everyone could give these folks just a huge round of applause for the

1513

01:45:18.320 --> 01:45:19.153

work today,

1514

01:45:25.860 --> 01:45:29.120

I'm sure there'll be, uh, plenty more questions for them. Uh,

1515

01:45:29.120 --> 01:45:32.760

there's the kickback at the hotel at five 30 for staying there. Um,

1516

01:45:32.780 --> 01:45:35.240

I'm sure we'll see some of these folks there and have a chance to ask them more

1517

01:45:35.360 --> 01:45:38.200

questions. And we got the next couple of days. Um, so yeah, again,

1518

01:45:38.200 --> 01:45:39.720

thank you so much. Uh,

1519

01:45:39.960 --> 01:45:43.480

tomorrow breakfast starts at seven in the bozen ballroom.

1520

01:45:43.500 --> 01:45:47.160

That's the down in the, in the jury hotel. And then, uh,

1521

01:45:47.160 --> 01:45:49.840

the sessions start at eight o'clock tomorrow. So,

1522

01:45:50.100 --> 01:45:53.400

and then tomorrow evening we have our banquet dinner at six, for six 30.

1523

01:45:54.200 --> 01:45:57.880

I think that is about it. The bus leaves in about 15 minutes,

1524

01:45:58.780 --> 01:46:03.760

so it's, if you miss it, it's um, I got five more seats. Other than that,

1525

01:46:03.870 --> 01:46:06.840

it's, uh, you'll have to Uber at home, back to the hotel. So turbo.

1526

01:46:07.000 --> 01:46:09.520

Anything else to add? All right. Thanks again, everyone,

1527

01:46:09.560 --> 01:46:12.320

I really appreciate you coming today, and thanks again for a great job by our,

1528

01:46:12.320 --> 01:46:13.120
uh, speakers today.