WEBVTT

1
00:00:01.930 --> 00:00:03.140
Well, now that, uh,

2
00:00:04.960 --> 00:00:07.750
Murph and Poncho got us started off with all the hard stuff,

3
00:00:07.870 --> 00:00:11.270
I get to do the easy stuff for a little bit here. Uh,

4
00:00:11.970 --> 00:00:16.150
and so we wanted to just kind of talk through a little bit of a practical

5
00:00:16.150 --> 00:00:20.630
application of something. We shared this at S F T E, uh,

6
00:00:20.970 --> 00:00:25.190
at, at, uh, in London, Ontario last fall for, so for some of you,

7
00:00:25.190 --> 00:00:27.670
this is going to be a bit of a repeat, but, uh,

8
00:00:28.370 --> 00:00:33.270
we thought it was worth just kind of sharing of what we went through and why we

9
00:00:33.270 --> 00:00:37.950
did it and, and what it did for us and the, some of the results and,

10
00:00:38.010 --> 00:00:40.590
and the lessons we learned. We had a a,

11
00:00:40.760 --> 00:00:43.470
we've got a third member on our team here that isn't here today,

12
00:00:43.470 --> 00:00:44.990
Jordan Stringfield. But, uh,

13
00:00:45.880 --> 00:00:49.870
we'll just step into it. So,

14
00:00:50.880 --> 00:00:53.190
and we'll kind of just the,

15
00:00:54.610 --> 00:00:57.920
we'll give you a little bit of a background of the project. Uh,

16
00:00:58.670 --> 00:01:02.040
talk about how we applied this to, to what we did,

17
00:01:02.620 --> 00:01:06.240
and then kinda step through what, what were, uh,

18
00:01:06.380 --> 00:01:09.720
the high points and low points of, of what we experienced, uh,

19
00:01:09.720 --> 00:01:13.360
trying to apply s TPA in our organization for the first time.

20
00:01:15.780 --> 00:01:20.560
So we'll start with the Dutch Roll Initiator. Um, it's a really simple,

21
00:01:21.340 --> 00:01:25.440
uh, kind of, uh, pathfinding project that we did.

22
00:01:26.500 --> 00:01:31.360
Uh, we've got, um, dreams of, of, uh,

23
00:01:32.080 --> 00:01:36.560
building on this and, and moving on to, to other maneuvers. Uh,

24
00:01:37.060 --> 00:01:39.080
but we looked and said, you know,

25
00:01:39.080 --> 00:01:43.080
we wanna start doing automated maneuvers on large commercial transports.

26
00:01:43.860 --> 00:01:48.440
So we, we looked at all the different maneuvers that we thought could add value,

27
00:01:49.060 --> 00:01:54.040
and we decided that the simplest one we could do would be one that had a single

28
00:01:54.630 --> 00:01:57.280
control surface that needed to be manipulated.

29
00:01:57.860 --> 00:02:01.240
We could do an open loop and we could improve the results.

30
00:02:01.980 --> 00:02:06.360
And so by looking at that, we kind of decided that the, the Dutch roll was a,

31
00:02:06.460 --> 00:02:11.310
was a pretty easy target for us. And so the Dutch roll is just,

32
00:02:12.390 --> 00:02:16.370
we initiated it with, with a rudder input. Uh,

33
00:02:16.990 --> 00:02:20.490
and so the shaping of that rudder input is what's really important, uh,

34
00:02:20.490 --> 00:02:24.570
from the loads community. They never like to see us do anything oscillatory.

35
00:02:25.070 --> 00:02:29.610
And so they have a lot of concern when we start putting in oscillatory rudder

36
00:02:29.610 --> 00:02:33.610
inputs. And so they're really worried about the phasing,

37
00:02:33.610 --> 00:02:37.170
that we're making sure that our frequency matches the response to the aircraft.

38
00:02:37.400 --> 00:02:39.530
They're really worried about the amplitude.

39

00:02:40.270 --> 00:02:42.970
And depending on what part of the envelope we're in,

40
00:02:43.040 --> 00:02:46.450
it's a really tall order to ask a pilot to make such small,

41
00:02:46.800 --> 00:02:51.690
precise inputs, make them balanced, symmetric,

42
00:02:52.470 --> 00:02:56.610
and not exceed any limits, and to get the frequency exactly right.

43
00:02:57.510 --> 00:03:01.540
And so we said, well, we can, we can, you know,

44
00:03:01.540 --> 00:03:03.060
with a touch of a few buttons,

45
00:03:03.060 --> 00:03:07.580
we can get a perfect sinusoid and we can have everything we need. Uh,

46
00:03:07.640 --> 00:03:09.820
and then when we looked at our processes, it was like, well,

47
00:03:09.820 --> 00:03:11.340
it violates our process. We,

48
00:03:11.480 --> 00:03:15.860
we want it to be able to adjust so that if our frequency was off a little bit,

49
00:03:15.860 --> 00:03:18.300
if the natural frequency of the aircraft is a little bit different,

50
00:03:19.000 --> 00:03:22.740
we could adjust that and get maximum input into the structure to get maximum

51
00:03:23.260 --> 00:03:27.790
response. And so we needed to come up with some,

52

00:03:27.980 --> 00:03:32.030
some process to, uh, be able to do that. And we said, well,

53
00:03:32.040 --> 00:03:33.830
we've got our little tool here now.

54
00:03:34.250 --> 00:03:37.830
And so we went into our simulator and one of our pilots says,

55
00:03:38.490 --> 00:03:41.950
how can you prove to me that you've thought of all the ways that this thing

56
00:03:41.950 --> 00:03:45.930
could go wrong? And it was like, okay, um,

57
00:03:46.860 --> 00:03:48.490
we're, we've got a little work ahead of us.

58
00:03:48.910 --> 00:03:50.930
And then we also knew that at some point,

59
00:03:50.930 --> 00:03:54.810
we're gonna have to stand up in front of our program chief engineer

60
00:03:56.010 --> 00:04:00.810
on in the design organization and, you know,

61
00:04:00.830 --> 00:04:02.690
be able to look them straight in the eye and say,

62
00:04:02.690 --> 00:04:05.610
we're not gonna break your airplane. This is, this is a smart thing to do.

63
00:04:06.390 --> 00:04:08.930
So we'll just kind of walk through the,

64
00:04:09.430 --> 00:04:12.650
now this is most definitely not a safety control structure.

65

00:04:12.840 --> 00:04:16.890
This is just your kind of standard schematic, right? Of,

66
00:04:16.910 --> 00:04:21.450
of the components we had. So the green box is down at the bottom.

67
00:04:21.460 --> 00:04:25.810
We've got a yacht amper control in this aircraft that gives commands to the

68
00:04:25.810 --> 00:04:26.890
yacht amper actuator,

69
00:04:27.270 --> 00:04:32.150
and moves the rudder common flight test components we've had for a

70
00:04:32.150 --> 00:04:37.100
long time as a fault insertion box of a function generator that actually creates

71
00:04:37.100 --> 00:04:38.780
the voltage signals that goes to that.

72
00:04:39.480 --> 00:04:41.540
And then a control head that sits in the flight deck.

73
00:04:42.840 --> 00:04:47.500
The new pieces that we added to this system that were different is a

74
00:04:47.640 --> 00:04:51.420
laptop, running a, uh, very simple little software program.

75
00:04:51.590 --> 00:04:55.660
We've got a screenshot of the, the software there, uh,

76
00:04:55.730 --> 00:04:58.100
that was feeding a compact Rio,

77
00:04:58.500 --> 00:05:02.900
a standard device from national instruments that you can send a digital signal

78
00:05:02.960 --> 00:05:04.620
and it will actually create the voltage.

79
00:05:06.530 --> 00:05:08.350
So that was the basics of the system,

80
00:05:09.250 --> 00:05:12.590
and we knew that we needed to find some sort of a,

81
00:05:12.870 --> 00:05:17.390
a rigorous safety analysis that we could answer the questions that were being

82
00:05:18.000 --> 00:05:20.950
given to us. So with that, I'll, I'll let, uh,

83
00:05:21.160 --> 00:05:26.150
dunes kind of step through the, the details, uh, of,

84
00:05:26.930 --> 00:05:29.990
of what S T P A looked for, like for us in this case.

85
00:05:31.810 --> 00:05:35.950
All right. Thank you very much. Uh, so,

86
00:05:37.210 --> 00:05:40.830
uh, as, um, Sarah indicated earlier, uh,

87
00:05:40.830 --> 00:05:45.750
first step is to identify your losses. And, um, interestingly,

88
00:05:46.690 --> 00:05:51.430
uh, the, you know, the three that she mentioned were loss related to, uh,

89
00:05:51.530 --> 00:05:55.390
uh, personnel and to hardware aircraft, right?

90
00:05:55.970 --> 00:06:00.060
But you can also add some other aspects to your analysis,

91

00:06:00.060 --> 00:06:04.300
including in this case, we said, uh, loss of customer satisfaction,

92
00:06:04.880 --> 00:06:08.700
uh, data quality. So, you know, maybe you had, um, uh,

93
00:06:08.700 --> 00:06:11.020
something in your system that, that, uh, uh,

94
00:06:11.090 --> 00:06:15.620
your data was no good in the end and, uh, loss of flight test productivity,

95
00:06:16.010 --> 00:06:18.220
because, you know, in the end, we're spending money.

96
00:06:18.440 --> 00:06:20.380
So how do we improve on that?

97
00:06:22.750 --> 00:06:27.490
So the first one, first two, right? It's, it's a bad day, right? So we,

98
00:06:27.790 --> 00:06:32.440
the classic, um, losses that we want to avoid, then we've got, uh,

99
00:06:32.580 --> 00:06:36.640
not meeting the test goals, and finally, uh,

100
00:06:36.680 --> 00:06:41.400
a monetary loss. So you can cover more than just the classic, uh,

101
00:06:41.400 --> 00:06:44.000
losses if that's what you desire in your analysis.

102
00:06:45.940 --> 00:06:50.160
So from that, we came up with three hazards. So, uh,

103
00:06:50.280 --> 00:06:54.160
H one exceeding our vertical fin loads, uh, as sort of the,

104
00:06:54.180 --> 00:06:58.560

the first and foremost when you think about doing a Dutch roll excitation, and,

105
00:06:58.940 --> 00:07:03.720
um, you know, it's basically dynamic pressure times beta, cub, beta,

106
00:07:03.720 --> 00:07:06.240
right? And, uh, so we have that limit.

107
00:07:06.820 --> 00:07:11.320
We have reduction in control of the aircraft, uh, due to either, uh,

108
00:07:11.470 --> 00:07:15.640
divergent dutch roll or, uh, something in your system. Um,

109
00:07:15.640 --> 00:07:19.040
something that we're driving. So those relates to losses one and two.

110
00:07:19.260 --> 00:07:23.880
And then our third one, uh, sort of covers the other losses in, in our simple,

111
00:07:24.180 --> 00:07:28.590
uh, case here. So this is our control structure.

112
00:07:29.130 --> 00:07:31.550
Um, and, uh,

113
00:07:33.320 --> 00:07:35.260
so one of the things that, uh,

114
00:07:35.260 --> 00:07:40.180
we ran into is that having the design already sort of in

115
00:07:40.180 --> 00:07:44.220
place, like we came up with this rol initiator, uh,

116
00:07:44.220 --> 00:07:45.860
using our flight test hardware and everything,

117
00:07:45.860 --> 00:07:50.420

it was really easier for us to start by just copying the, uh, the,

118
00:07:50.480 --> 00:07:53.220
the schematic. Like, okay, well this box talks to this box,

119
00:07:53.220 --> 00:07:55.420
we'll put that box in there and this one talks to that box,

120
00:07:55.640 --> 00:07:59.700
so we'll put that box in there. Um, and so it took a little, um,

121
00:07:59.720 --> 00:08:03.380
we had some facilitators that, uh, were, um,

122
00:08:03.770 --> 00:08:06.060
more well versed in s TPA to help us out.

123
00:08:06.200 --> 00:08:10.940
And it took a little bit of effort for us to get out of that mindset and

124
00:08:10.990 --> 00:08:15.900
start collapsing certain, um, uh, architecture that was,

125
00:08:16.240 --> 00:08:18.540
uh, not really kinda just a pass through, right?

126
00:08:18.680 --> 00:08:23.060
Wasn't actually making a controlled this, uh, uh, operation. So,

127
00:08:23.720 --> 00:08:27.340
uh, and even now I look at this control structure having a little bit
more

128
00:08:27.340 --> 00:08:28.180
experience. It's like, well,

129
00:08:28.180 --> 00:08:30.940
we could probably even collapse a few more of those. So, you know, this
is our,

130
00:08:31.080 --> 00:08:34.850

our first, uh, attempt at s tpa. Uh,

131
00:08:34.850 --> 00:08:38.730
but we start at the top, um,

132
00:08:39.490 --> 00:08:42.490
I dunno if you can see the laser or not, but we have our test plan, right?

133
00:08:42.510 --> 00:08:44.970
And we sort of considered that our master controller, um,

134
00:08:45.460 --> 00:08:48.410
using a vetted process, right? We have all our, our, uh,

135
00:08:48.410 --> 00:08:53.290
review processes and we're saying, okay, that, that, that exists. And, uh,

136
00:08:53.510 --> 00:08:55.100
that's outta scope. We're not looking at that.

137
00:08:55.100 --> 00:08:58.100
We're gonna assume the test plan is, is perfect, right? Cuz it always is, right?

138
00:08:58.760 --> 00:09:01.660
Um, so from there, um,

139
00:09:01.680 --> 00:09:05.780
the flight test plan is used by the pilot test director, uh,

140
00:09:05.780 --> 00:09:06.900
in the front of our airplane,

141
00:09:07.320 --> 00:09:10.940
and then also by the flight test engineer in the back. Um,

142
00:09:11.520 --> 00:09:15.780
the pilot test director has some control operations, um,

143

00:09:15.780 --> 00:09:20.540
related to our function generator, um, and, uh,

144
00:09:20.610 --> 00:09:23.700
also some switching that, uh, controls, uh,

145
00:09:23.700 --> 00:09:27.260
the signals that go to the YA damper. And then on the other side,

146
00:09:27.270 --> 00:09:32.140
we've got our flight test engineer that is controlling that laptop that Darren

147
00:09:32.180 --> 00:09:33.380
talked about, the, the new,

148
00:09:33.480 --> 00:09:37.860
one of the new components that drives the compact Rio, uh,

149
00:09:37.860 --> 00:09:41.900
which sends a signal to our functioning generator and onward. And then also as,

150
00:09:42.200 --> 00:09:43.540
as a greater feedback loop,

151
00:09:43.880 --> 00:09:46.820
we have signals coming back to our flight test data system,

152
00:09:47.310 --> 00:09:51.740
which feedback to the flight test engineer that would, uh,

153
00:09:51.800 --> 00:09:56.620
impact their decision making. Uh, and then in the end,

154
00:09:56.880 --> 00:09:59.860
um, this is sort of our, the rudder is basically our,

155
00:10:00.400 --> 00:10:04.780
our base controlled process. That's the final output we're looking for is a,

156
00:10:04.880 --> 00:10:09.700
is a rudder signal or rud rudder motion. Sorry. Okay.

157
00:10:12.080 --> 00:10:13.500
All right. So let's, uh,

158
00:10:13.770 --> 00:10:16.620
what we're gonna do is just really quickly dive at one section,

159
00:10:16.890 --> 00:10:18.460
take a look at it, and come up with some,

160
00:10:18.490 --> 00:10:23.020
show you some examples of our yuca and, and, uh, causal scenarios and whatnot.

161
00:10:23.200 --> 00:10:27.700
So, uh, examples here, so we take a look at, uh, just the,

162
00:10:28.560 --> 00:10:33.020
um, the subsection here with the compact Rio and the laptop and the two,

163
00:10:33.400 --> 00:10:34.500
uh, human participants.

164
00:10:35.970 --> 00:10:40.350
So one of our undesirable control actions that we came up with is,

165
00:10:40.740 --> 00:10:43.510
what if the test director enables the E-stop,

166
00:10:43.520 --> 00:10:48.030
which controls the function generator, uh, while the program is running?

167
00:10:48.250 --> 00:10:52.790
So what yuca is that, that is a, an action too early.

168
00:10:53.010 --> 00:10:54.470
So at the end of the condition,

169

00:10:54.730 --> 00:10:58.510
our tourist test director is supposed to safe the function generator.

170
00:10:58.690 --> 00:11:02.070
And if they do that too early, that's an undesirable control action.

171
00:11:03.730 --> 00:11:07.350
Um, and you know, when you follow that back up the chain, okay,

172
00:11:07.350 --> 00:11:09.150
what hazard is that? Uh,

173
00:11:10.030 --> 00:11:13.710
probably stopping our function early isn't gonna cause a loss, uh,

174
00:11:13.710 --> 00:11:16.670
of the aircraft or control or, or, uh, an exceedance,

175
00:11:16.810 --> 00:11:21.110
but it will basically make our condition no good. So that kind of relates to,

176
00:11:21.610 --> 00:11:26.430
uh, loss of, um, um, H three, whatever we worded that,

177
00:11:26.450 --> 00:11:29.870
but the, uh, uh, it, uh, loss of a usable maneuver.

178
00:11:32.230 --> 00:11:34.890
And as another example on the other side, um,

179
00:11:35.100 --> 00:11:38.970
let's say that no voltage was commanded from the laptop,

180
00:11:39.860 --> 00:11:43.810
right? We hit go and nothing happened, no voltage came out.

181
00:11:44.950 --> 00:11:48.970
Um, so that's a example of a control action that is not provided.

182
00:11:52.520 --> 00:11:55.660

So in the end, uh, when we looked at the entire control structure,

183
00:11:56.240 --> 00:12:00.860
we came up with a table of 57 undesirable control actions, uh,

184
00:12:00.890 --> 00:12:05.500
16 of them related to H one safety, uh, hazard one.

185
00:12:05.760 --> 00:12:10.060
And, uh, the remaining was, were mainly addressing our efficiency part.

186
00:12:10.200 --> 00:12:12.380
So you can see that, um,

187
00:12:13.650 --> 00:12:16.740
part of this is in the importance of scoping out your analysis. So we,

188
00:12:17.120 --> 00:12:21.820
we had a lot of yuca that covered just test efficiency, and, you know,

189
00:12:21.820 --> 00:12:25.060
in the end, that's good for us. Um, we had a better product out of it,

190
00:12:25.530 --> 00:12:29.140
even though it didn't directly related to the safety of the, uh, of the system.

191
00:12:30.160 --> 00:12:34.290
Yeah, that was, that was an intentional scoping that we did because we're,

192
00:12:34.870 --> 00:12:37.930
you know, we're very aware that as a pathfinding exercise,

193
00:12:38.590 --> 00:12:43.570
we needed to be able to show that we could actually improve the efficiency

194
00:12:43.950 --> 00:12:47.850
and get better results. And so we wanted to,

195

00:12:48.230 --> 00:12:53.010
to use this opportunity to flesh out any other potential issues

196
00:12:53.070 --> 00:12:56.410
in our system that were beyond safety. So that was a,

197
00:12:56.410 --> 00:13:00.850
that was one of the things that was a, a real benefit to us of using s stpa.

198
00:13:03.230 --> 00:13:06.290
So from you, as you go to, uh,

199
00:13:06.400 --> 00:13:11.090
what we were calling it causal scenarios, um, and, uh,

200
00:13:12.310 --> 00:13:14.890
you'll see a few different terms for, for this step.

201
00:13:15.010 --> 00:13:19.810
I think in the SDPA handbook, uh, they use a different term,

202
00:13:19.810 --> 00:13:24.530
and I can't remember what it is offhand, but, uh, ultimately it's what,

203
00:13:24.530 --> 00:13:28.690
what ha what caused that undesirable control action? What is it?

204
00:13:28.950 --> 00:13:33.910
So if we look at the two examples that I just talked about, so why did the,

205
00:13:34.290 --> 00:13:39.070
why did the, uh, um, test director hit the e stop too early? Well,

206
00:13:39.070 --> 00:13:41.950
one causal scenario that we came up with is, uh,

207
00:13:41.950 --> 00:13:46.390
they incorrectly interpreted cues or communication from the back of the

208

00:13:46.550 --> 00:13:47.750
airplane. Um,

209
00:13:48.090 --> 00:13:51.870
you can have multiple yuca or multiple causal scenarios for that one yuca.

210
00:13:51.870 --> 00:13:56.680
This is just one example. Um, what about the other one? Well,

211
00:13:56.700 --> 00:14:00.840
the Dutch Roll Initiator client had to be in a, had two modes, right?

212
00:14:00.860 --> 00:14:04.840
We had a test mode to make sure we were gonna send the right signal,

213
00:14:05.220 --> 00:14:08.960
and then the actual operational mode where it actually sends the, uh,

214
00:14:08.980 --> 00:14:13.160
the signal out to the, uh, compact Rio. Well, you know,

215
00:14:13.160 --> 00:14:16.600
what if they were in the wrong mode? Like, oh, shoot, I, I didn't realize that,

216
00:14:16.700 --> 00:14:19.680
uh, I was in the test mode. Sorry about that. So,

217
00:14:22.140 --> 00:14:22.780
uh,

218
00:14:22.780 --> 00:14:27.720
we identified 39 causal scenarios to lead to the 57 yuasas.

219
00:14:27.940 --> 00:14:31.680
So there was a lot of cross uh, pollination there, right?

220
00:14:31.790 --> 00:14:35.840
Some causal scenarios, uh, were, uh, uh,

221

00:14:35.940 --> 00:14:40.850
traced to multiple yuasas and, and whatnot. Okay?

222
00:14:41.030 --> 00:14:45.570
And then from there, we generated requirements. Okay, so how did we prevent,

223
00:14:46.070 --> 00:14:49.130
uh, how do we mitigate, um, the, uh,

224
00:14:49.330 --> 00:14:53.220
causal scenario where the test director had, uh, received in, um,

225
00:14:53.410 --> 00:14:58.140
interpret cues incorrectly? So we added some, uh,

226
00:14:58.290 --> 00:14:59.260
onto our test card,

227
00:14:59.290 --> 00:15:03.820
some specific Dutch roll initiator operator call outs. So,

228
00:15:04.240 --> 00:15:07.540
uh, after the Dutch roll initiator, uh,

229
00:15:08.020 --> 00:15:12.340
finished executing the signal, uh, the rudder input,

230
00:15:12.640 --> 00:15:17.400
we called out free response. And then also when the, uh,

231
00:15:18.020 --> 00:15:22.960
uh, we needed six cycles of free response once we got the, the six cycles, uh,

232
00:15:23.360 --> 00:15:25.840
complete was called. And that was the signal that we,

233
00:15:26.020 --> 00:15:30.560
we were rigid about using that, uh, terminology to cue the flight direct, uh,

234
00:15:30.630 --> 00:15:35.480
test director to save the fg. Uh, and the other one,

235
00:15:35.620 --> 00:15:39.000
and, and this is an interesting one. So we, uh,

236
00:15:39.140 --> 00:15:43.280
not being programmers, uh, and just, you know, having enough, uh,

237
00:15:43.750 --> 00:15:45.440
knowledge of Lab U to be dangerous,

238
00:15:45.440 --> 00:15:49.280
we created this client to do what it had to do in order to execute the Dutch

239
00:15:49.280 --> 00:15:52.440
role. And, um, you know, it's like, okay,

240
00:15:52.440 --> 00:15:56.960
well we just need to be in the right mode. Uh, but we went ahead and we,

241
00:15:56.990 --> 00:16:00.800
when we created a requirement that, oh, the start button must only be available,

242
00:16:01.580 --> 00:16:06.440
uh, when you're ready to test, when you're actually ready to execute the signal,

243
00:16:07.300 --> 00:16:09.600
uh, it then it sort of light bulb went off like, oh, well,

244
00:16:09.600 --> 00:16:13.720
we can just engineer a solution. And it wasn't that hard. Uh,

245
00:16:13.720 --> 00:16:16.040
it's just that we hadn't, we just hadn't done it,

246
00:16:16.040 --> 00:16:19.440
and we hadn't occurred to us until we went through this process. Uh,

247
00:16:19.440 --> 00:16:20.600
and we also said, uh,

248
00:16:20.830 --> 00:16:24.920
made a requirement that the client status must be displayed, uh, on the, uh,

249
00:16:24.920 --> 00:16:29.760
the gui. Uh, so we made those changes and we had a better product cuz of it.

250
00:16:32.440 --> 00:16:36.580
Um, so we talked about scoping, um, we only,

251
00:16:36.760 --> 00:16:38.820
we constrained this, uh,

252
00:16:39.180 --> 00:16:43.340
analysis to the doctoral initiator system that we added. Um,

253
00:16:43.360 --> 00:16:46.420
so we didn't include, uh, uh,

254
00:16:47.440 --> 00:16:50.980
the airplane systems and, you know, all the stuff that's, uh, uh,

255
00:16:50.980 --> 00:16:55.940
would make the the analysis explode. Um, and the other thing is that we,

256
00:16:56.040 --> 00:16:57.340
as I mentioned, we already had a,

257
00:16:57.440 --> 00:16:59.660
the system was partially built and tested already. Um,

258
00:17:00.040 --> 00:17:03.020
if going back or going into the future, uh,

259
00:17:03.020 --> 00:17:07.020
we'll probably incorporate s stpa as part of the design, uh,

260
00:17:07.020 --> 00:17:11.540
of the tool so that rather than going back and changing, um, uh,

261
00:17:11.540 --> 00:17:13.580
the design based on the s stpa requirements,

262
00:17:13.580 --> 00:17:16.460
we actually evolved the design with the requirements that we create.

263
00:17:18.980 --> 00:17:20.880
And then, um, in the end,

264
00:17:20.900 --> 00:17:24.760
so five losses led to three hazards to 57 ucas,

265
00:17:25.100 --> 00:17:29.560
39 causal scenarios. And we came up with 27 requirements. Uh,

266
00:17:29.660 --> 00:17:33.440
so five requirements, uh, already covered by, uh,

267
00:17:33.920 --> 00:17:35.640
a system limitation, um,

268
00:17:35.640 --> 00:17:39.240
basically how much authority the yacht amper actuator had.

269
00:17:39.580 --> 00:17:43.880
So we didn't actually have to do anything, we just had to say, uh, this is,

270
00:17:43.930 --> 00:17:47.120
these, these requirements are already covered, um,

271
00:17:47.140 --> 00:17:50.980
and have that traceability in the documentation. Um,

272
00:17:51.190 --> 00:17:55.420
eight drove updates to our lab view code and 14, uh,

273
00:17:55.420 --> 00:17:58.420
updates to, uh, test procedures and checklist items.

274
00:18:00.770 --> 00:18:05.540
Okay. Um, I guess, uh, Darren, you wanna talk? Uh, sure.

275
00:18:05.540 --> 00:18:06.580
Facilitating the lessons learned?

276
00:18:07.090 --> 00:18:07.380
Yeah,

277
00:18:07.380 --> 00:18:11.580
so one of the most important things we found was having people that knew what

278
00:18:11.580 --> 00:18:13.060
they were doing. Uh,

279
00:18:14.320 --> 00:18:18.780
we were always being pulled back off a bunny trail or, uh,

280
00:18:19.010 --> 00:18:22.180
several of the things that Sarah mentioned, like saying, oh,

281
00:18:22.730 --> 00:18:26.260
that'll never happen. Let's not bother writing this down. Um,

282
00:18:27.000 --> 00:18:31.020
and it was, there was still value in, in documenting all that,

283
00:18:31.520 --> 00:18:34.660
and it sets us up for future cases as well.

284
00:18:34.840 --> 00:18:37.020
But we had three different facilitators.

285
00:18:37.120 --> 00:18:41.140
We tried to have at least two in each one of the meetings we had. And, uh,

286
00:18:42.050 --> 00:18:46.740
that really helped us a lot of keeping us with forward progress. Um,

287
00:18:47.800 --> 00:18:51.380
and cuz it's, it's a different mindset. It's a different way of thinking.

288
00:18:51.380 --> 00:18:55.380
There's some abstract thought going on there. Um, and,

289
00:18:55.960 --> 00:19:00.780
and then so one facilitator kind of talking to us while the other facilitator

290
00:19:00.840 --> 00:19:02.820
was busy taking notes and,

291
00:19:02.880 --> 00:19:06.620
and filling out things in the tool because all these different elements of s

292
00:19:06.620 --> 00:19:10.420
stpa are a mini to mini relationship as you've already seen. And, um,

293
00:19:10.640 --> 00:19:15.020
having some way of tracking that and, and making sure that, that it's,

294
00:19:15.290 --> 00:19:18.140
that we're not skipping over anything, uh,

295
00:19:18.630 --> 00:19:22.860
makes it pretty tedious and methodical. So it,

296
00:19:22.880 --> 00:19:25.740
it took us a lot of hours. I think, you know,

297
00:19:25.740 --> 00:19:30.300
as we come up to speed this next time around, we're we're, uh,

298
00:19:30.300 --> 00:19:34.500
doing another sdpa on some other things. Uh, it, it's,

299
00:19:34.820 --> 00:19:36.980
I expect it to be a lot faster. Uh,

300
00:19:37.840 --> 00:19:41.000
we were able to work with just Excel fairly well.

301
00:19:41.220 --> 00:19:46.160
Our facilitators actually have a really well done model in

302
00:19:46.330 --> 00:19:49.680
cameo that, that makes it even better. That allows you to,

303
00:19:50.020 --> 00:19:53.280
to slice the data multiple ways and see those relationships better,

304
00:19:53.300 --> 00:19:55.520
and the traceability was a lot easier. Um,

305
00:19:56.460 --> 00:20:00.270
and so access to like that, to,

306
00:20:00.450 --> 00:20:04.750
to a tool like that is, is definitely, um, advantageous, uh,

307
00:20:04.750 --> 00:20:09.510
over just a, a simple Excel spreadsheet. But, um, whether it's a,

308
00:20:09.710 --> 00:20:12.750
a piece of paper or a whiteboard, um, it,

309
00:20:12.850 --> 00:20:15.590
you can really make progress no matter what. Um,

310
00:20:17.380 --> 00:20:21.760
so kind of some of those lessons for us is patience was the biggest thing.

311
00:20:21.760 --> 00:20:26.720
We wanted to get to those causal scenarios as soon as we could. Uh, for us,

312
00:20:26.720 --> 00:20:30.920
the losses and hazards really didn't take very long because, uh,

313
00:20:31.380 --> 00:20:35.280
in spite of the differences, if you kind of just start looking at, uh,

314
00:20:36.370 --> 00:20:40.230
the terminology and swapping out th a terminology,

315
00:20:40.370 --> 00:20:44.110
all of a sudden a lot of this looks really familiar to you and,

316
00:20:44.250 --> 00:20:49.100
and that that made life a lot easier for me. Uh, but at the same time,

317
00:20:49.650 --> 00:20:53.260
make sure that you're not bringing in your background and your

318
00:20:54.290 --> 00:20:58.820
notions about safety and mitigation of what we've always done can really,

319
00:21:02.200 --> 00:21:07.100
Of which preconceived safety notion. Uh, yeah.

320
00:21:07.280 --> 00:21:11.220
So the, the one example where we knew that our,

321
00:21:11.360 --> 00:21:15.740
our YA damper had very limited authority and we knew that the loads community

322
00:21:16.440 --> 00:21:19.820
had given us, uh, a peak to peak rudder deflection.

323
00:21:20.440 --> 00:21:24.580
So all of a sudden that was less than what the YA damper was capable of.

324
00:21:25.000 --> 00:21:29.100
And so as long as you have a system that can only move the rudder with the YA

325
00:21:29.100 --> 00:21:32.700
damper, we knew that we could never break the structure. Um,

326
00:21:32.840 --> 00:21:35.980
and so it was really tempting to go, okay, yeah, let's just,

327
00:21:36.120 --> 00:21:38.940
we know the answer to this, we're just gonna not write it down. Um,

328
00:21:39.310 --> 00:21:39.810
We're

329
00:21:39.810 --> 00:21:43.100
Glad we did because the next airplane we wanna put this system on,

330
00:21:43.590 --> 00:21:44.900
we're gonna have full authority.

331
00:21:45.720 --> 00:21:49.660
And so all of a sudden we can build on that and move on. And even though,

332
00:21:50.530 --> 00:21:53.500
even though we knew that that was the case, we actually did ground test, right?

333
00:21:53.520 --> 00:21:54.220
And said, okay,

334
00:21:54.220 --> 00:21:57.620
we're gonna give it way too much voltage and watch and see what happens to make

335
00:21:57.620 --> 00:22:01.500
sure that there's an something that's somebody isn't, you know,

336
00:22:02.310 --> 00:22:06.380
going to surprise us. So, um, some of those things where I could,

337
00:22:07.360 --> 00:22:10.460
you know, see where you've got something that you believe to be true,

338
00:22:10.680 --> 00:22:13.780
and if you do a ground test or a bench test or something,

339
00:22:13.780 --> 00:22:14.980
all of a sudden you realize like, oh,

340
00:22:14.980 --> 00:22:18.900
we've got some new path that we can defeat this system that we didn't think

341
00:22:18.900 --> 00:22:19.733
about.

342
00:22:19.740 --> 00:22:24.620
I, I'll give another example. And that's, um, you know, we use our,

343
00:22:24.920 --> 00:22:27.460
our function generator quite often, right?

344
00:22:27.480 --> 00:22:31.060
As I'm sure a lot of operators do to excite, um,

345
00:22:31.900 --> 00:22:34.260
flexible body modes, right? We're trying to test the flutter, uh,

346
00:22:34.700 --> 00:22:35.860
stability of the aircraft and whatnot.

347
00:22:35.860 --> 00:22:40.860
We haven't done use it to do rigid body motion before. And so,

348
00:22:41.600 --> 00:22:46.300
um, our facilitators would ask some pointed questions about the f r function

349
00:22:46.300 --> 00:22:51.020
generator and how we use it. And there was just a lot of like, like,

350
00:22:51.210 --> 00:22:53.940
like we know this, we've done this before. We use this all the time, right?

351
00:22:54.050 --> 00:22:58.860
Like, we don't need to address these little, um, uh, aspects of the fg.

352
00:22:59.000 --> 00:23:01.580
And, um, in the end, um,

353
00:23:01.800 --> 00:23:06.180
we did discover a few things and, uh, and we also, um,

354
00:23:06.620 --> 00:23:10.380
documented all, you know, it helped to document all the, um,

355
00:23:11.810 --> 00:23:12.560
ucas the,

356
00:23:12.560 --> 00:23:17.340
the causal scenarios and what processes we already have in place that take

357
00:23:17.340 --> 00:23:18.900
care of that. Um, and, you know,

358
00:23:18.930 --> 00:23:22.100
some of the great processes that we already have that will cover those,

359
00:23:22.150 --> 00:23:24.820
those uh, uh, cases. And then another one,

360
00:23:25.840 --> 00:23:30.140
the facilitator asks us, like, you know, we have a button for execute, right?

361
00:23:30.440 --> 00:23:33.780
And well, what happens if the operator pushes that button twice?

362
00:23:33.960 --> 00:23:35.900
And you're just like, well, we're not idiots, right?

363
00:23:35.910 --> 00:23:38.340
We're not gonna push it twice. But, you know,

364
00:23:38.560 --> 00:23:41.500
if you've tested on a flight with buffet or turbulence, you know,

365
00:23:41.520 --> 00:23:45.940
and you're trying to do delicate operation, sometimes that happens. And,

366
00:23:45.940 --> 00:23:49.230
you know, we actually tested it and, you know, the, the,

367
00:23:49.250 --> 00:23:51.910
the software didn't do anything bad, but didn't do anything desirable either,

368
00:23:52.130 --> 00:23:56.470
so we fixed it. Right? So those are some examples of, uh,

369
00:23:56.630 --> 00:23:58.950
preconceived notions that we just kind of had to go in.

370
00:23:59.010 --> 00:24:01.550
We had to change our mindset on how we approached, uh,

371
00:24:01.850 --> 00:24:06.350
the analysis rather than focusing just on this new component and what it could

372
00:24:06.350 --> 00:24:09.150
do. Uh, let's look at the entire interaction.

373
00:24:10.620 --> 00:24:10.910
Yeah.

374
00:24:10.910 --> 00:24:15.390
A really powerful aspect of stpa is if you're willing to follow through that

375
00:24:15.390 --> 00:24:19.870
process, um, it can expose errors in mental models.

376
00:24:20.330 --> 00:24:25.070

And I think that's one of the biggest differentiators compared to any other

377
00:24:25.070 --> 00:24:28.270
safety analysis that I've been a part of is,

378
00:24:28.970 --> 00:24:33.470
is that piece where if you dig in and you're persistent on it, you can,

379
00:24:33.490 --> 00:24:36.990
you can expose potential for mental model errors, um,

380
00:24:37.920 --> 00:24:39.750
which is really, you know,

381
00:24:39.750 --> 00:24:42.750
where we like to blame the human operator at the end of the day, right?

382
00:24:42.890 --> 00:24:46.790
Of the human error. Well, let's try and design it out. Uh,

383
00:24:47.770 --> 00:24:51.390
so we're, we're going to continue using s stpa the,

384
00:24:51.410 --> 00:24:55.830
the value in being able to stand up in front of the chief engineer

385
00:24:56.370 --> 00:24:59.310
in a, in a test review board and

386
00:25:00.980 --> 00:25:02.270
feel like I,

387
00:25:02.750 --> 00:25:06.310
I had every confidence that any scenario that they could come up with any

388
00:25:06.510 --> 00:25:09.630
question they were gonna ask me that we'd already thought of it and we'd covered

389
00:25:09.630 --> 00:25:13.830

it and we had it. Um, that was pretty powerful. Um, and,

390
00:25:14.290 --> 00:25:18.940
and so then we already talked a little bit about, you know,

391
00:25:19.340 --> 00:25:23.540
applying this earlier in the, in the process, we'll avoid rework, um,

392
00:25:23.680 --> 00:25:25.860
be less costly. Um,

393
00:25:26.960 --> 00:25:31.900
but now I'm thinking about how can we take elements of s stpa and improve our

394
00:25:32.020 --> 00:25:32.853
t a process.

395
00:25:33.240 --> 00:25:37.580
And it's that balance there between time and resources available

396
00:25:38.240 --> 00:25:42.140
and, and desiring something that's more complete. Um,

397
00:25:42.400 --> 00:25:45.420
and something that is the structure that it,

398
00:25:45.440 --> 00:25:49.940
it really resonated with me that one of our concerns that Sarah brought up this

399
00:25:49.940 --> 00:25:51.300
morning is, um,

400
00:25:52.290 --> 00:25:54.980
when we do test safety analysis,

401
00:25:55.090 --> 00:25:58.950
that it really has heavy reliance on experience.

402
00:25:59.290 --> 00:26:03.550

And so any structure that we can bring to make it less unstructured

403
00:26:03.550 --> 00:26:07.830
brainstorming and more structured focused, uh, analysis,

404
00:26:08.430 --> 00:26:12.550
I think is, is, uh, something that will improve that and lower the,

405
00:26:12.890 --> 00:26:15.350
the barrier to, uh, experience,

406
00:26:15.350 --> 00:26:19.790
whether that's experience of the individuals or, um,

407
00:26:20.010 --> 00:26:20.540
you know,

408
00:26:20.540 --> 00:26:25.510
that are just new to flight test or all of us run into new airplanes that have

409
00:26:25.610 --> 00:26:27.870
thrown new curve wells at us all the time. So,

410
00:26:29.790 --> 00:26:32.650
And, um, if you back up one more, I'll,

411
00:26:32.650 --> 00:26:36.690
I'll give another example of feature deployment. So we, uh,

412
00:26:37.370 --> 00:26:40.530
replaced our function generator, uh,

413
00:26:40.770 --> 00:26:43.780
recently with new hardware update, modern technology, right? Same.

414
00:26:43.780 --> 00:26:45.140
But it does the same exact thing.

415
00:26:45.720 --> 00:26:49.900
And so we basically adopted all the same exact processes that we had from

416
00:26:49.900 --> 00:26:54.540
before. Should be good, right? But as, as Sarah mentioned, right,

417
00:26:54.540 --> 00:26:57.060
you bring in this new hardware, but you use your old processes,

418
00:26:57.060 --> 00:27:01.540
your old safety assumptions, uh, what could you be missing? So we, uh,

419
00:27:01.540 --> 00:27:06.140
we have a pilot project to use s tpa to go back and look at,

420
00:27:06.640 --> 00:27:11.340
um, uh, the, our function generator function generator and a holistic look.

421
00:27:11.880 --> 00:27:15.180
And, uh, ideally we come out all the requirements and say,

422
00:27:15.180 --> 00:27:19.620
we've covered all the requirements cuz our, our safety processes are great,

423
00:27:20.520 --> 00:27:22.180
but we might find something. And so,

424
00:27:22.180 --> 00:27:24.740
and we'll feel better about it at the end of the day.

425
00:27:25.290 --> 00:27:25.580
Yeah,

426
00:27:25.580 --> 00:27:29.060
we've got two or three flight test systems like that that we're gonna go back

427
00:27:29.060 --> 00:27:32.060
through and apply sdpa to that are, you know,

428
00:27:32.500 --> 00:27:34.260

existing systems that have been around for any,

429
00:27:34.300 --> 00:27:38.100
anywhere from a couple years to a couple decades. Um,

430
00:27:38.450 --> 00:27:40.540
just to see what we can learn. Uh,

431
00:27:40.800 --> 00:27:45.220
our water barrel transfer water system for CG control is,

432
00:27:45.280 --> 00:27:46.980
is one of those, right? If we've got,

433
00:27:47.350 --> 00:27:50.860
we've got systems that we rely on inherently for safety all the time.

434
00:27:51.520 --> 00:27:55.420
And we think this is a tool that's probably overdue to get applied against those

435
00:27:55.640 --> 00:28:00.420
to, to do our own homework, if you will, internal to our organization.

436
00:28:00.840 --> 00:28:04.260
So, uh, we're really glad we used this.

437
00:28:05.020 --> 00:28:08.100
I I have no regrets. Uh, it was, uh,

438
00:28:08.280 --> 00:28:11.700
it was a good opportunity for me to learn about s stpa and one of the simplest

439
00:28:11.700 --> 00:28:15.740
systems that I think will ever come across. Uh, and so it was a,

440
00:28:15.870 --> 00:28:19.820
everything just kinda lined up at the right time. Um,

441
00:28:20.960 --> 00:28:25.820

and Dunes actually last year presented at the annual m mit,

442
00:28:26.280 --> 00:28:30.900
uh, workshop that they hold. And, uh, Dr. Thomas and Dr.

443
00:28:30.900 --> 00:28:33.180
Levison were both really excited, uh,

444
00:28:33.240 --> 00:28:38.020
to see this being applied kind of on the flight test side of things. They've,

445
00:28:38.090 --> 00:28:42.220
they've been part of a lot of s stpa analysis, uh,

446
00:28:42.220 --> 00:28:46.260
within aviation on the design side of the house. And, and, uh,

447
00:28:46.260 --> 00:28:50.500
they've been wanting to see this expand more into flight tests.

448
00:28:50.520 --> 00:28:54.220
So it's part of why we're here today, uh, and,

449
00:28:54.480 --> 00:28:59.220
and really think I expect to see more and more of our

450
00:28:59.220 --> 00:29:02.460
design organization is, is embracing s stpa.

451
00:29:03.000 --> 00:29:05.340
And so the question is how do we take, you know,

452
00:29:05.340 --> 00:29:10.020
we're all familiar as flight testers dealing with ssas and FHAs and,

453
00:29:10.040 --> 00:29:13.780
and whatever safety analysis tools have been used by our,

454
00:29:13.920 --> 00:29:16.460
our design organizations. Uh,

455
00:29:17.010 --> 00:29:21.620
when we start interacting with our design teams that have used stpa,

456
00:29:22.320 --> 00:29:23.020
at the very least,

457
00:29:23.020 --> 00:29:27.140
we need to be ready and figure out how to interpret those add in the flight test

458
00:29:27.140 --> 00:29:28.740
pieces. Ideally,

459
00:29:28.840 --> 00:29:32.940
we should be involved early in that design so we can add in the flight test

460
00:29:32.940 --> 00:29:35.620
components to their control structures and,

461
00:29:35.720 --> 00:29:39.700
and we can have it done and ready and have a better understanding of the system

462
00:29:39.700 --> 00:29:44.500
on day one when we're ready to flight test. So With that,

463
00:29:44.540 --> 00:29:48.780
I think we're ready to turn it over to Pancho again. Ah, we'll take,

464
00:30:06.760 --> 00:30:07.593
Right,

465
00:30:23.390 --> 00:30:27.220
Right. Yeah, we definitely had some cart before the horse. This was a,

466
00:30:27.580 --> 00:30:31.900
a very small, you know, kind of side project home, uh,

467
00:30:31.900 --> 00:30:33.660

to a large extent. So we had,

468
00:30:34.080 --> 00:30:38.260
we had an existing Dutch roll test plan for doing it manually.

469
00:30:38.920 --> 00:30:39.753
We, uh,

470
00:30:40.240 --> 00:30:44.300
put all the pieces together and went and tried it in the simulator and saw that

471
00:30:44.300 --> 00:30:47.180
it worked. And then we're like, okay,

472
00:30:47.400 --> 00:30:51.060
now how do we get approval and how do we assure, you know,

473
00:30:51.060 --> 00:30:54.500
how do we get a safe to fly gold star on this thing? Um,

474
00:30:54.560 --> 00:30:58.500
and that's when we then I, I knew a couple, uh,

475
00:30:58.500 --> 00:31:03.060
people that are well versed in sdpa and I said, help, I need your help. And, uh,

476
00:31:03.320 --> 00:31:06.460
so it just kind of, I'd been wanting to explore Sdpa for a long time,

477
00:31:06.460 --> 00:31:09.740
and now I had a, a need and it coalesced that way.

478
00:31:09.920 --> 00:31:13.820
So we had a working early version of,

479
00:31:13.820 --> 00:31:17.620
of the Dutch Roll Initiator client already going before we started sdpa.

480
00:31:18.160 --> 00:31:22.500

And then as we learned things, we made changes. And then, uh,

481
00:31:22.780 --> 00:31:26.460
ultimately we, uh, made some pretty significant, uh,

482
00:31:26.460 --> 00:31:30.660
modifications the test plan to, to, to drive a,

483
00:31:31.140 --> 00:31:33.500
a better communication and,

484
00:31:33.720 --> 00:31:38.100
and process into the test plan to make sure that we were going to get the

485
00:31:38.100 --> 00:31:42.580
results we wanted. And it was really successful. We very intentionally said,

486
00:31:42.590 --> 00:31:47.540
we're not going to even attempt to improve the productivity on

487
00:31:47.540 --> 00:31:52.380
the first time. We're just going to do it safely. And in spite of that,

488
00:31:52.560 --> 00:31:56.300
we cut our repeats down to, I think 20% or something like that.

489
00:31:56.520 --> 00:31:58.380
So right out of the gate, we,

490
00:31:58.640 --> 00:32:03.130
we actually saw usefulness and, um,

491
00:32:03.810 --> 00:32:07.330
a reduction in workload and everything else and, and did it all safely. So

492
00:32:11.000 --> 00:32:11.833
Did you talk,

493
00:32:14.920 --> 00:32:16.300

you did very small

494
00:32:17.470 --> 00:32:18.240
Yeah.

495
00:32:18.240 --> 00:32:21.440
A new airplane program that all kinds of,

496
00:32:23.260 --> 00:32:25.560
is it scalable if,

497
00:32:25.700 --> 00:32:29.080
so in some of the process you bought

498
00:32:31.190 --> 00:32:32.023
ai?

499
00:32:33.560 --> 00:32:36.050
Yeah, I'm not sure about the AI part of it.

500
00:32:36.210 --> 00:32:40.180
I think that this is all surrounding, um,

501
00:32:40.980 --> 00:32:43.660
engineering judgment and, uh,

502
00:32:44.430 --> 00:32:48.940
using the creativity of, you know, thought. Uh,

503
00:32:49.740 --> 00:32:54.700
I do also know that a growing number of our design organizations are

504
00:32:54.700 --> 00:32:58.900
embracing sdpa. Uh, one of the things that stood out to me,

505
00:33:00.440 --> 00:33:02.140
uh, first is, is

506
00:33:03.810 --> 00:33:08.670
one of the consternations I have with ssas is, uh, um,

507
00:33:09.460 --> 00:33:10.000
you know,

508
00:33:10.000 --> 00:33:13.840
poncho already talked about the fact that it really doesn't cover mental model

509
00:33:13.840 --> 00:33:16.360
breakdowns. It's only failures of systems, right?

510
00:33:16.700 --> 00:33:19.920
And so if you've got an algorithm problem, you've got a logic issue,

511
00:33:20.620 --> 00:33:23.720
an SSA isn't going to uncover that ever. Uh,

512
00:33:23.780 --> 00:33:28.320
but the other thing is it gets you away from that statistics, uh, uh,

513
00:33:28.320 --> 00:33:30.280
conundrum I'll call it, uh,

514
00:33:30.890 --> 00:33:33.800
where instead of using statistics to,

515
00:33:33.940 --> 00:33:37.200
to make a problem go away or hope that it's not going to be an issue,

516
00:33:37.700 --> 00:33:38.720
you can design it out.

517
00:33:38.720 --> 00:33:42.560
And so if you start early with one or two boxes in your control structure,

518
00:33:43.680 --> 00:33:47.880
I think it's, it's entirely scalable and usable. And, and that's what our, uh,

519
00:33:47.880 --> 00:33:52.240
you compare it, that's really the comparison is this to an ssa, right?

520
00:33:52.340 --> 00:33:57.080
And we know how much engineering time goes into an s ssa,

521
00:33:57.580 --> 00:34:01.360
and I think this is equivalent, but it's gonna give you a lot more output.

522
00:34:02.140 --> 00:34:03.800
You know, interestingly enough, um,

523
00:34:03.930 --> 00:34:07.920
after the MIT presentation last year at the stamp conference, uh,

524
00:34:07.960 --> 00:34:12.920
I did have somebody reach out to me, uh, from industry who was looking at,

525
00:34:13.380 --> 00:34:16.880
uh, automating aspects of s tpa. Um,

526
00:34:16.980 --> 00:34:20.040
and so that work is out there. So, um,

527
00:34:20.650 --> 00:34:24.840
there might be opportunity for, for making some of the processes deal faster.

528
00:34:29.000 --> 00:34:30.370
Yeah. Dr. Thomas and Dr.

529
00:34:30.480 --> 00:34:35.330
Levison are actively working improvements to this whole thing all the time

530
00:34:35.330 --> 00:34:39.210
and working with a lot of different industries.

531
00:34:39.350 --> 00:34:43.130
So yeah, I shouldn't be so close-minded as far as automation.

532

00:34:43.270 --> 00:34:45.610
I'm sure there's ways to make it simpler,

533
00:34:45.830 --> 00:34:50.170
but at some point you've gotta have a human in the loop to really break it down

534
00:34:50.230 --> 00:34:54.770
and, and figure out what those four possible ways are of,

535
00:34:54.950 --> 00:34:59.050
of a desirable control action becoming un undesirable or unsafe.

536
00:35:19.630 --> 00:35:21.760
Yeah, I think there are tools out there if you Google,

537
00:35:21.760 --> 00:35:26.240
there are definitely tools out there. Um, and yeah,

538
00:35:26.420 --> 00:35:31.200
the making sure you have something to help you maintain all those linkages, um,

539
00:35:32.500 --> 00:35:35.520
you know, if you're good with pivot tables, that would be a,

540
00:35:35.720 --> 00:35:39.540
a simple way to do it. I think that that would be entirely possible. Um,

541
00:35:40.710 --> 00:35:42.870
poncho's probably come across some tools too, but,

542
00:35:44.130 --> 00:35:45.310
Uh, but you wouldn't, uh,

543
00:35:45.310 --> 00:35:48.750
like I would say you wouldn't want the tool to prevent you from doing s stpa,

544
00:35:48.800 --> 00:35:51.870
right? Like, it shouldn't be a barrier to entry. And,

545
00:35:52.090 --> 00:35:55.550
and so maybe not at an airplane, a whole airplane level,

546
00:35:55.690 --> 00:35:59.550
but if you've got a test hardware or something you want to try this on, um,

547
00:35:59.750 --> 00:36:04.070
I mean, Excel is perfectly reusable, so yeah, you don't need, you don't need to,

548
00:36:04.370 --> 00:36:05.870
to start with complex software.

549
00:36:11.200 --> 00:36:14.900
I think the key thing that asking

550
00:36:24.160 --> 00:36:24.993
Mm-hmm.

551
00:36:37.110 --> 00:36:40.160
Process, but you know what, you need to take what,

552
00:36:42.790 --> 00:36:47.480
Yeah, the MIT has a really good s stpa handbook that,

553
00:36:47.550 --> 00:36:52.080
that is, is pretty detailed. Um, but again, that's kind of the,

554
00:36:53.140 --> 00:36:55.560
if you read the handbook and do it on your own, you're,

555
00:36:55.560 --> 00:36:58.640
you're not likely to get the results you're looking for. Um,

556
00:36:58.640 --> 00:37:03.360
having somebody that really dunes and I sat down and started trying to do

557
00:37:03.430 --> 00:37:05.920
kind of the next generation of this system on a different,

558
00:37:05.920 --> 00:37:09.680
different airplane and the second hour of,

559
00:37:09.780 --> 00:37:11.040
of working through it,

560
00:37:11.140 --> 00:37:15.840
we got ourselves mired down and just came to a halt and called the facilitators

561
00:37:15.860 --> 00:37:18.200
and said, we need your help again. We can't,

562
00:37:18.200 --> 00:37:21.240
we're not ready to do this on our own yet. So, yeah,

563
00:37:21.500 --> 00:37:25.080
But the, the structure, like having the control structure, the,

564
00:37:25.140 --> 00:37:27.040
the visual model, so you know,

565
00:37:27.040 --> 00:37:31.600
where you're focusing your question and then having those four methods of,

566
00:37:32.100 --> 00:37:36.560
uh, undesirable control action really helps you focus, uh,

567
00:37:37.140 --> 00:37:41.040
to find the, find those, those bad control actions.

568
00:37:41.110 --> 00:37:44.360
Because if it's an open-ended question, it's like, how can these go,

569
00:37:44.360 --> 00:37:47.680
how can it go wrong? Then, you know, you, you get overwhelmed, right? So that,

570
00:37:47.680 --> 00:37:48.920
that structure really helps you out.

571
00:37:50.760 --> 00:37:51.560
Architecture

572
00:37:51.560 --> 00:37:56.320
Paragraph, the, the methodology of the, of approaching the problem. Yeah.

573
00:37:56.780 --> 00:37:59.080
So we probably should hand it off before we get to, right?

574
00:37:59.080 --> 00:38:02.080
But we're happy to like, talk to anybody offline.

575
00:38:05.020 --> 00:38:09.390
Alright, so if you guys don't mind helping me, um, pass out those handouts.

576
00:38:09.530 --> 00:38:10.363
Yep. Perfect.

577
00:38:10.570 --> 00:38:15.390
So we're gonna go over a UAV example. It's one that I did in my, uh,

578
00:38:15.620 --> 00:38:19.830
with my thesis. Um, so, so it's a good one just to kind of work through.

579
00:38:20.720 --> 00:38:21.553
Thank you.

580
00:38:25.990 --> 00:38:30.830
I think we've got about 45 minutes-ish until, until lunchtime.

581
00:38:31.090 --> 00:38:34.870
So, so we'll see, see how this works through.

582
00:38:34.890 --> 00:38:39.740
But we put together a little handout, uh, just for you guys to, to jot on,

583
00:38:39.840 --> 00:38:43.420
uh, if you would like, um, a couple, couple notes.

584
00:38:43.640 --> 00:38:47.540
So a couple folks asked if, uh, if the slides are gonna be available.

585
00:38:47.920 --> 00:38:51.700
So I'm gonna work with Darren to get the slides, um, put on the,

586
00:38:51.880 --> 00:38:55.740
the workshop website. We can also put that handout on the works, uh,

587
00:38:55.740 --> 00:38:59.780
on the website. And we're also recording this. And that's gonna be, um,

588
00:38:59.920 --> 00:39:04.300
PO posted as well. So, so you'll have all that available. Um,

589
00:39:04.330 --> 00:39:08.300
there's also, Darren mentioned the, the, or the statement conference,

590
00:39:08.490 --> 00:39:12.500
it's coming up in June. It's gonna be virtual, it's free. Um,

591
00:39:12.640 --> 00:39:16.260
so it's a really good opportunity to learn more about s TPA and,

592
00:39:16.260 --> 00:39:21.140
and various applications. Uh, so definitely look that up. Just, just search, uh,

593
00:39:21.340 --> 00:39:25.140
m MIT stamp stamp workshop and you'll, you'll be able to find it.

594
00:39:25.140 --> 00:39:29.220
And I think we do have a link at the end of the slides too, to the website. Um,

595
00:39:29.840 --> 00:39:34.100
and the common mental model. That's, that's a really important aspect of this.

596
00:39:34.760 --> 00:39:39.700

Um, so I've sat in rooms where I've, I've facilitated and, uh, and, you know,

597
00:39:39.720 --> 00:39:41.700
sub various subsystem engineers, they don't,

598
00:39:41.700 --> 00:39:44.420
they don't understand that their system's talking to this other system.

599
00:39:44.680 --> 00:39:47.220
The lead engineer doesn't understand the interactions.

600
00:39:47.520 --> 00:39:50.460
And so as they're building this out, they're like, oh, holy smoke.

601
00:39:50.460 --> 00:39:53.780
Cause I had no idea it worked this way. I had no idea that input affected this,

602
00:39:54.050 --> 00:39:58.140
this control action. Um, so it's, it's a really powerful technique.

603
00:39:58.280 --> 00:40:02.100
One of the things that, that Murph and I have worked with, um, uh,

604
00:40:02.100 --> 00:40:03.020
at Edwards is,

605
00:40:03.120 --> 00:40:06.220
is if we can just get folks to create the safety control structure,

606
00:40:06.650 --> 00:40:10.020
that is a huge, huge win. Just, just to get that,

607
00:40:10.050 --> 00:40:12.260
even if you don't go through the rest of the analysis,

608
00:40:12.490 --> 00:40:15.980
just to create that safety control structure and then have a common mental model

609

00:40:16.000 --> 00:40:19.900
and be able to talk about it, uh, will, will provide value, uh,

610
00:40:19.920 --> 00:40:22.860
to your organization. And I'm glad that,

611
00:40:22.860 --> 00:40:27.100
that they mentioned documented assumptions. That's, that's really important. Um,

612
00:40:27.560 --> 00:40:32.180
uh, I've, I've been in a situation where we had a program, um,

613
00:40:32.360 --> 00:40:34.700
it got delayed. We had people move,

614
00:40:34.760 --> 00:40:36.620
we had new folks trying to pick up that program,

615
00:40:37.120 --> 00:40:39.900
and they're looking at the safety plan that was completed.

616
00:40:40.160 --> 00:40:42.980
And they have no understanding of why,

617
00:40:43.440 --> 00:40:47.380
why the ths that were chosen were chosen, and why other ths were not chosen.

618
00:40:47.690 --> 00:40:51.940
Because there's, there's no documented assumptions, uh, or, or, um,

619
00:40:51.940 --> 00:40:55.940
background as to why that occurred. So, so those assumptions are really,

620
00:40:55.940 --> 00:40:59.300
really important. Most of what we do is not gonna be done, you know, in,

621
00:40:59.400 --> 00:41:03.700
in a few months or even maybe a few years. It's gonna be, you know,

622

00:41:03.700 --> 00:41:08.500
potentially decades of a life cycle of a, of a, of an aircraft. Uh, so,

623
00:41:08.600 --> 00:41:12.220
so having that documented for, for future generations is really,

624
00:41:12.220 --> 00:41:16.130
really important. Alright,

625
00:41:16.550 --> 00:41:20.930
so I'm gonna describe the system. We're gonna do the losses and hazards,

626
00:41:21.270 --> 00:41:25.930
and then hopefully get into the safety control structure before we break for

627
00:41:25.930 --> 00:41:29.090
lunch. Um, all right, so,

628
00:41:30.150 --> 00:41:33.050
so the system under test, it's a general aviation aircraft.

629
00:41:33.210 --> 00:41:38.180
It's been converted to a uav. So, uh, they, they actually, um,

630
00:41:38.200 --> 00:41:42.380
put actuators, um, in, uh, in the cockpit, uh,

631
00:41:42.380 --> 00:41:46.980
to make it a uav. Um, it's controlled by ground stations. There's a, uh,

632
00:41:47.010 --> 00:41:49.700
line of sight ground station at the airfield,

633
00:41:50.080 --> 00:41:54.980
and then there's a beyond line of sight, um, ground station somewhere else,

634
00:41:55.240 --> 00:41:59.820
uh, not in the immediate vicinity. And there's a handoff. Um, the,

635

00:42:00.200 --> 00:42:04.860
the autopilot is in the vehicle management system and it controls the actuators,

636
00:42:05.240 --> 00:42:07.060
um, uh, that,

637
00:42:07.090 --> 00:42:10.660
that connect to the elevator aileron's rudder and the engine throttle.

638
00:42:11.960 --> 00:42:16.500
It also has alternators to power the VMs, um, and the,

639
00:42:16.520 --> 00:42:19.140
the systems and the payload. Um,

640
00:42:19.160 --> 00:42:21.540
it also has modified fuel tanks for longer endurance.

641
00:42:21.690 --> 00:42:24.060
There's a camera attached above the instrument panel,

642
00:42:24.520 --> 00:42:28.580
so whoever's flying it on the ground can see kind of more or less, uh,

643
00:42:28.580 --> 00:42:29.740
what the aircraft is seeing.

644
00:42:30.160 --> 00:42:34.220
And the mission for this particular aircraft is ISR support to,

645
00:42:34.280 --> 00:42:38.900
to ground troops. That's what we're gonna be working on today.

646
00:42:41.410 --> 00:42:43.190
Um, so this is just, um,

647
00:42:43.490 --> 00:42:47.550
my attempt at a cartoon there. Um,

648
00:42:48.370 --> 00:42:50.350

so you've got your, your pre-flight,

649
00:42:50.350 --> 00:42:54.270
which looks like any other general aviation pre-flight. Uh, it's,

650
00:42:54.270 --> 00:42:58.390
this aircraft is not allowed a taxi, so you tow it to the engine runup area,

651
00:42:58.490 --> 00:43:03.110
you conduct the engine runup, um, remotely, then you tow it to the runway,

652
00:43:04.210 --> 00:43:06.430
you, you hit a button and it takes off.

653
00:43:06.690 --> 00:43:10.550
It climbs and cruises based off of a pre-programmed route.

654
00:43:11.090 --> 00:43:14.630
And then there's a handoff from the line of site controller to the beyond line

655
00:43:14.630 --> 00:43:17.430
of site controller. Um, and then it cruises,

656
00:43:17.430 --> 00:43:21.150
it conducts its mission out and about it comes back, does another handoff,

657
00:43:21.370 --> 00:43:24.230
it lands on the runway and then it's towed back to park.

658
00:43:26.320 --> 00:43:27.380
Any questions on that?

659
00:43:30.860 --> 00:43:35.030
Alright. Um, so what do you think the,

660
00:43:35.090 --> 00:43:39.430
the losses are for this particular, this particular system?

661
00:43:41.970 --> 00:43:45.830
And I'm gonna attempt to drag this over maybe.

662
00:43:47.470 --> 00:43:48.890
Ah, yes. All right.

663
00:43:59.080 --> 00:44:04.040
So what do you think the, um, the losses might be? Mission Yep.

664
00:44:09.540 --> 00:44:12.110
Loss. Yep. Loss of,

665
00:44:12.770 --> 00:44:16.910
you're gonna see my poor typing skills. You got it. Type. All right.

666
00:44:16.910 --> 00:44:19.790
Sounds good. All right, we got a scribe. So, loss of mission.

667
00:44:20.310 --> 00:44:25.070
I heard loss of vehicle. Say again?

668
00:44:25.340 --> 00:44:29.230
Loss of life. Loss of life. Yep. Potentially, uh,

669
00:44:29.230 --> 00:44:33.860
what would be the life potentially lost for this one? On the ground?

670
00:44:34.120 --> 00:44:39.060
On the ground? So it, it crashes into something on the ground Yep.

671
00:44:40.950 --> 00:44:44.490
And in infrastructure as well. Yep.

672
00:44:44.630 --> 00:44:48.470
So you could put a fourth loss on there. Uh,

673
00:44:48.470 --> 00:44:51.150
loss of infrastructure if it were to,

674
00:44:53.010 --> 00:44:56.430

to land somewhere. It's not supposed to. All right.

675
00:44:57.770 --> 00:44:59.100
What do we think? Is that pretty good?

676
00:45:00.090 --> 00:45:03.150
That loss, loss of life on ground

677
00:45:04.420 --> 00:45:05.220
Yep. Damage

678
00:45:05.220 --> 00:45:05.910
Or,

679
00:45:05.910 --> 00:45:08.040
Yeah, you definitely could. You definitely could.

680
00:45:08.100 --> 00:45:11.360
The question was could you combine losses three and four and,

681
00:45:11.380 --> 00:45:12.560
and you absolutely can.

682
00:45:15.980 --> 00:45:20.200
So I think getting it on paper to the conversation we had during the break,

683
00:45:20.900 --> 00:45:23.640
um, getting it on paper is the, the biggest thing.

684
00:45:23.640 --> 00:45:26.760
Making sure that you stay high level and that it's documented in some way.

685
00:45:26.860 --> 00:45:30.880
And when we provide these slides, the goal is to provide you this as,

686
00:45:30.980 --> 00:45:34.240
as an artifact. So, so you guys will have it if you, if you're not taking notes,

687

00:45:35.640 --> 00:45:38.420
but it is good to take the notes cause we're gonna be referencing this right as

688
00:45:38.420 --> 00:45:41.980
we go through hazards. All right. So hazards, it's a system level,

689
00:45:42.070 --> 00:45:46.940
state or condition combined with the environmental factors that could lead to

690
00:45:47.060 --> 00:45:49.620
a loss. So the reason I have the loss,

691
00:45:50.040 --> 00:45:53.940
and then the underscore there is because we need to make sure any hazard that we

692
00:45:53.940 --> 00:45:57.140
talk about, uh, traces back to one of the losses.

693
00:45:59.320 --> 00:46:03.260
All right? Say again? Conductivity. Conductivity.

694
00:46:03.840 --> 00:46:08.400
So is that, is that a system level? System level state?

695
00:46:16.750 --> 00:46:17.470
Loss of

696
00:46:17.470 --> 00:46:22.280
Control. Loss of control, yep. Yep. And a loss of connectivity may,

697
00:46:22.380 --> 00:46:27.160
may drive to loss of, uh, control, structural failure.

698
00:46:27.660 --> 00:46:28.493
Yep.

699
00:46:35.690 --> 00:46:36.523
Yeah,

700
00:46:38.470 --> 00:46:41.010
you can throw it down and you can always adjust, right?

701
00:46:41.010 --> 00:46:43.490
One of the things we talked about was iteration. Uh,

702
00:46:43.490 --> 00:46:47.850
so we can always adjust this. Say again,

703
00:46:48.870 --> 00:46:49.703
engine failure.

704
00:46:50.350 --> 00:46:55.050
So I probably would not include that because the engine is a,

705
00:46:55.070 --> 00:46:57.250
is a subsystem. Um,

706
00:46:57.430 --> 00:47:00.370
and I'd probably rewrite the communication failure something,

707
00:47:00.370 --> 00:47:05.250
something to the effect of, uh, lo loss of, loss of communication between,

708
00:47:05.790 --> 00:47:10.090
uh, you know, ground station and in vehicle or something along those lines.

709
00:47:14.670 --> 00:47:15.503
Why?

710
00:47:16.350 --> 00:47:17.970
Why? Um,

711
00:47:17.970 --> 00:47:22.850
because because trying to make it more of a system level, uh,

712
00:47:22.850 --> 00:47:24.250
hazard versus

713
00:47:35.400 --> 00:47:36.233
Stating.

714
00:47:50.760 --> 00:47:54.980
Yep. Thank you. Yeah, that's, that's the biggest thing we're in. We're,

715
00:47:54.980 --> 00:47:59.980
we're technical. We like to dive deep and try to stay high level. All right.

716
00:47:59.980 --> 00:48:03.110
What are some other, other hazards

717
00:48:10.110 --> 00:48:11.970
you could, you can say that I think we,

718
00:48:12.170 --> 00:48:13.650
I think I wrote something along those lines.

719
00:48:13.830 --> 00:48:17.970
You could say controlled flight into obstacles or something along those lines.

720
00:48:25.550 --> 00:48:26.383
Mm-hmm.

721
00:48:28.350 --> 00:48:29.183
Yep.

722
00:48:29.600 --> 00:48:30.433
Control.

723
00:48:30.710 --> 00:48:31.930
Yep. Yep.

724
00:48:33.830 --> 00:48:35.370
Uh, failure always kinda,

725
00:48:36.640 --> 00:48:39.010
Yeah. So you're saying a higher level,

726
00:48:39.080 --> 00:48:41.450
just loss of control and that would cover a lot of those things?

727
00:48:47.320 --> 00:48:51.220
It would. That's where I would put it. So you'll find it as you go deeper in,

728
00:48:51.480 --> 00:48:55.260
you'll, you'll find that as, as a potential, uh, scenario.

729
00:48:57.930 --> 00:49:00.390
All right. Any other thoughts? Oh, what you got,

730
00:49:07.930 --> 00:49:11.980
Greg? Ground equipment failure or damage? So,

731
00:49:14.240 --> 00:49:18.620
So I did have one, um, in here. I think we'll see it on the,

732
00:49:18.620 --> 00:49:22.060
on the next slide. It was something to the effect of, um, you know,

733
00:49:22.060 --> 00:49:25.020
what if it collides with ground equipment, something like that,

734
00:49:25.020 --> 00:49:28.700
it's not supposed to taxi, that doesn't mean it's not gonna, if,

735
00:49:28.700 --> 00:49:30.540
if we don't do what we're supposed to do, right?

736
00:49:31.410 --> 00:49:33.270
So does that kind of hit what you're asking?

737
00:49:33.410 --> 00:49:36.870
Are you saying the ground control or, uh, sorry, the ground equipment.

738
00:49:36.870 --> 00:49:41.680
There's an issue and that leads to something the second one. Yeah.

739

00:49:41.980 --> 00:49:42.920
So I, I think,

740
00:49:43.240 --> 00:49:47.160
I think you would find that as you go deeper into the analysis as a, as a cause

741
00:49:48.530 --> 00:49:49.500
Loss, of course.

742
00:49:50.180 --> 00:49:55.160
Loss of course. Yep. So I would, um,

743
00:49:55.860 --> 00:49:57.920
so you could put that one in there.

744
00:49:59.150 --> 00:49:59.983
Collision,

745
00:50:02.450 --> 00:50:07.070
Midair. Collision. Yep. So you would say, um, you could say,

746
00:50:07.570 --> 00:50:12.110
um, you could potentially aggregate that up into hazard four,

747
00:50:12.210 --> 00:50:14.110
or you could say, um,

748
00:50:14.550 --> 00:50:19.550
a minimum separation distance between objects, something like that. And that,

749
00:50:19.570 --> 00:50:22.070
and you could do, and you'll see when we get to the next one,

750
00:50:22.790 --> 00:50:25.950
I had a minimum separation distance for ground and for air.

751
00:50:26.030 --> 00:50:28.980
I separated that out. Um, you could combine them

752

00:50:33.510 --> 00:50:37.670
icing, I think, I think that'll get, once you get in deeper into the analysis.

753
00:50:43.980 --> 00:50:44.813
Mm-hmm.

754
00:50:46.500 --> 00:50:47.920
It seems like the system level. I,

755
00:50:49.630 --> 00:50:53.880
Yeah. So I think you'll find that through the,

756
00:50:53.900 --> 00:50:56.720
the course and, and potentially, and the big,

757
00:50:56.720 --> 00:51:00.480
the biggest concern if you go into another airspace is you're hitting something

758
00:51:00.480 --> 00:51:03.200
you're not supposed to hit. Right? So I think you'll find that through other,

759
00:51:03.650 --> 00:51:04.483
other means

760
00:51:10.970 --> 00:51:13.070
in losses. Um,

761
00:51:15.790 --> 00:51:20.450
yeah. Loss. Uh, okay.

762
00:51:21.640 --> 00:51:24.450
Yeah. So, so you don't need 'em in both spots,

763
00:51:24.950 --> 00:51:29.250
but I would not put loss link as one of your, your losses.

764
00:51:30.070 --> 00:51:33.330
Um, that's really, it's the thing you wanna, it's the thing you wanna prevent.

765
00:51:33.330 --> 00:51:36.370
Loss link is gonna cause bad things to happen.

766
00:51:36.720 --> 00:51:40.330
Loss link in and of itself is, is not a mishap.

767
00:51:40.870 --> 00:51:42.850
So your loss is an actual mishap.

768
00:51:46.120 --> 00:51:50.870
All right. Any other, oh, what you got?

769
00:51:53.400 --> 00:51:57.690
Situational? Mm-hmm.

770
00:52:01.160 --> 00:52:02.570
Yeah, situational awareness.

771
00:52:02.930 --> 00:52:07.290
I think you'll find that as you go deeper into the analysis as well as you go

772
00:52:07.290 --> 00:52:08.123
along,

773
00:52:13.900 --> 00:52:16.360
it, it should not be, um, it,

774
00:52:16.450 --> 00:52:20.560
there should be some aspect of the hazard that's within your, your, uh,

775
00:52:20.820 --> 00:52:25.640
system boundaries and the environment is outside of your system. So,

776
00:52:25.780 --> 00:52:28.000
so like, flying too low and,

777
00:52:28.020 --> 00:52:30.680
and the aircraft impacts a mountain or something like that. The,

778
00:52:31.100 --> 00:52:32.600
the flying too low is the problem.

779
00:52:33.100 --> 00:52:36.080
And then you have environmental factors such as your,

780
00:52:36.080 --> 00:52:38.000
you're flying in mountainous terrain, something like that.

781
00:52:42.330 --> 00:52:46.750
Say again? Yeah. Loss of the payload.

782
00:52:47.730 --> 00:52:52.710
So you could, let's see. Yeah, I think,

783
00:52:52.830 --> 00:52:55.470
I think since that's a subsystem, I think it'll,

784
00:52:55.470 --> 00:52:58.910
you'll find that later on if you have some kind of payload failure or
something

785
00:52:58.910 --> 00:53:02.070
like that, or something, uh, electrical failure or something like that.

786
00:53:03.130 --> 00:53:07.270
So how do you differentiate between argue loss,

787
00:53:08.040 --> 00:53:12.230
uhhuh, ultimate leads? The loss of aircraft mm-hmm. Scenarios. I can
think of

788
00:53:14.170 --> 00:53:18.750
losses. Sounds somewhat redundant. Mm-hmm. Two separate things.

789
00:53:20.590 --> 00:53:24.750
I think they're, they're two separate things. Um, oh.

790
00:53:24.750 --> 00:53:27.660
Cuz you can lose control of an aircraft and you don't lose aircraft,
right.

791
00:53:27.680 --> 00:53:30.460
You can recover. Um, so, so, but

792
00:53:30.460 --> 00:53:33.980
In the UAB scenario, it seems to be loss of control, like loss of mm-hmm.

793
00:53:34.060 --> 00:53:36.780
Loss of, mm-hmm. Loss of structure, all of these things mm-hmm.

794
00:53:37.860 --> 00:53:40.680
Ultimately end up loss of aircraft. Mm-hmm.

795
00:53:42.240 --> 00:53:46.040
I guess what I'm asking is there more to that, cause in my mind there mm-hmm.

796
00:53:46.320 --> 00:53:49.840
U you can't control it. Mm-hmm. And it goes off, you know,

797
00:53:50.950 --> 00:53:53.720
over the ocean and disappears mm-hmm. Aircraft. Mm-hmm.

798
00:53:55.360 --> 00:53:57.840
Aircraft loss of control. Mm-hmm.

799
00:54:00.260 --> 00:54:02.160
Mm-hmm. Just trying to see if it's,

800
00:54:03.470 --> 00:54:06.520
Yeah, no, yeah, you can,

801
00:54:06.520 --> 00:54:08.640
you can reestablish connection or you

802
00:54:08.640 --> 00:54:11.920
Can design it out. So it's gotta return to base mode. So if you do lose,

803
00:54:13.460 --> 00:54:13.900
One of,

804
00:54:13.900 --> 00:54:18.800
one of my favorite definitions of a hazard that I think applies here too is, uh,

805
00:54:19.140 --> 00:54:24.000
you're in a, you're in an undesirable state, but nothing bad has happened yet.

806
00:54:24.140 --> 00:54:28.800
Mm-hmm. The, the loss really is the,

807
00:54:28.900 --> 00:54:33.400
the losses in stpa lingo are really the same as our effects in

808
00:54:33.820 --> 00:54:37.840
ths. Um, so if you think of losses akin to effects,

809
00:54:38.630 --> 00:54:41.480
like something bad has happened now, um,

810
00:54:41.480 --> 00:54:46.360
versus hazards are very much like the way we

811
00:54:46.360 --> 00:54:48.000
define hazards in DHAs.

812
00:54:49.940 --> 00:54:54.640
So if you go to the next slide, I'll show you guys what I came up with. Um,

813
00:54:55.540 --> 00:55:00.240
so, so a one, uh, accident, one was loss of life or injury.

814
00:55:00.960 --> 00:55:03.720
A two was loss of or damage to the uav,

815
00:55:04.340 --> 00:55:06.040
and three was loss of mission.

816
00:55:06.420 --> 00:55:10.160

So I actually did not include any kind of infrastructure or any other obstacles

817
00:55:10.160 --> 00:55:11.800
that you might have in the airspace, but I think that's,

818
00:55:11.800 --> 00:55:15.920
that's a good one that you could include. Um, and so my hazards there,

819
00:55:15.940 --> 00:55:19.680
and you can see how they trace back to the accidents. Uh,

820
00:55:19.700 --> 00:55:23.840
so hazard one was the UAV is too close to a ground or building a person.

821
00:55:24.700 --> 00:55:28.960
Um, so, um, so that was focused, um,

822
00:55:30.070 --> 00:55:33.400
that one could kind of go if you're in the air and, uh,

823
00:55:34.200 --> 00:55:38.900
or on the ground, H two UAV violates minimum separation requirements.

824
00:55:38.900 --> 00:55:43.300
So that's focused on, uh, aircraft, other aircraft in the, in the environment.

825
00:55:44.100 --> 00:55:48.420
H three UAV does not complete mission. We, we call it loss of mission. Um,

826
00:55:48.460 --> 00:55:52.580
I think does not complete mission is probably a better way to say it. Um,

827
00:55:52.730 --> 00:55:57.660
when you say loss of, back to the redundancy question, it makes you think of,

828
00:55:57.680 --> 00:55:59.820
of the accidents. Um,

829
00:56:00.260 --> 00:56:04.820
H four UAV departs controlled flight, I think we did have that one. Uh,

830
00:56:04.820 --> 00:56:07.780
I think we called it loss of controlled flight. Uh,

831
00:56:07.900 --> 00:56:12.340
H five is UAV departs apron, taxiway runway during ground operations.

832
00:56:12.630 --> 00:56:15.260
Again, this thing is not supposed to taxi, uh,

833
00:56:15.260 --> 00:56:17.460
we don't wanna make the assumption it's not gonna taxi, right?

834
00:56:17.550 --> 00:56:21.820
Cause what happens if we don't chalk it during the engine run up, or,

835
00:56:22.600 --> 00:56:23.860
um, you know, you hit the,

836
00:56:23.880 --> 00:56:26.900
hit the takeoff button when you're not supposed to hit the takeoff button,

837
00:56:27.290 --> 00:56:30.460
it's still in park or something like that. Uh, so it could taxi with,

838
00:56:30.460 --> 00:56:33.580
it could taxi H six, uh,

839
00:56:33.650 --> 00:56:36.140
loss of UAV airframe integrity.

840
00:56:36.280 --> 00:56:39.340
So I think we did have like a structural failure or something along those lines

841
00:56:40.650 --> 00:56:44.010
with the last one, ones we came up with.

842
00:56:46.110 --> 00:56:50.850
So that's, that's what I came up with for, uh, for this uav. Um,

843
00:56:51.110 --> 00:56:53.890
and you could, you could slice this a couple different ways. You could,

844
00:56:53.950 --> 00:56:56.490
you could aggregate some of these potentially. Uh,

845
00:56:56.490 --> 00:56:59.290
you may be able to break a couple apart, but for the most part,

846
00:56:59.310 --> 00:57:03.930
you want 'em to be, to be high level. You want 'em to cover a lot of, uh,

847
00:57:04.530 --> 00:57:09.520
a lot of ground if you will. Any questions on that? Sorry.

848
00:57:09.820 --> 00:57:13.000
Little bit. So lot.

849
00:57:14.740 --> 00:57:15.573
Yep. So

850
00:57:15.980 --> 00:57:20.800
For something like that where obviously the a a1 a two probably mean loss

851
00:57:20.960 --> 00:57:21.793
ion as well,

852
00:57:21.870 --> 00:57:22.703
Correct.

853
00:57:23.060 --> 00:57:27.960
But cause you uniquely said that nothing's broken and the

854
00:57:27.960 --> 00:57:29.040
only bad thing that's happened

855
00:57:29.630 --> 00:57:30.640

Just mm-hmm.

856
00:57:31.180 --> 00:57:36.120
Um, would that maybe drive there to be a different, different hazard?

857
00:57:36.270 --> 00:57:39.120
That different hazard? Um, so,

858
00:57:39.260 --> 00:57:42.720
so what's tough is you want it to be something that's, that's, um,

859
00:57:42.920 --> 00:57:47.200
a system state. So, um, you know,

860
00:57:47.200 --> 00:57:49.600
you've got a payload, right? Some kind of ISR payload.

861
00:57:49.910 --> 00:57:52.120
It's gotta be above whatever your target is.

862
00:57:52.310 --> 00:57:54.760
It's gotta be there at the time that it's supposed to be.

863
00:57:54.900 --> 00:57:59.280
So time on target and those types of things, all that is really important. Um,

864
00:57:59.620 --> 00:58:03.680
but, but we're gonna find those things deeper in the analysis. Um, so I,

865
00:58:03.800 --> 00:58:07.320
I think what you, what you hit on is, uh, you can,

866
00:58:07.340 --> 00:58:08.720
you can not lose the aircraft,

867
00:58:09.100 --> 00:58:13.000
but you still weren't successful in supporting the ground troops, uh,

868
00:58:13.000 --> 00:58:16.360
in the ISR mission. And that's what that's trying to, to get after.

869
00:58:21.120 --> 00:58:24.020
All right? Yes.

870
00:58:34.870 --> 00:58:36.340
Sorry, I'm gonna come closer.

871
00:58:37.800 --> 00:58:38.633
Not too many

872
00:58:40.120 --> 00:58:43.620
Too ha too many hazards at the beginning. Yes. So,

873
00:58:44.800 --> 00:58:45.280
so the,

874
00:58:45.280 --> 00:58:48.180
one of the reasons you want 'em to be high level and you don't want a lot is

875
00:58:48.180 --> 00:58:52.500
because then you have a decent idea of completeness. Uh, if you have,

876
00:58:53.200 --> 00:58:57.060
you know, 50 hazards that are deeper in the weeds,

877
00:58:57.060 --> 00:59:00.580
you have no idea if those are the only 50 hazards you should consider cuz

878
00:59:00.580 --> 00:59:03.340
there's too many. Uh, so at some point it's,

879
00:59:03.340 --> 00:59:06.700
it's gonna be beyond our ability to, to make sure that we've,

880
00:59:06.700 --> 00:59:07.660
we've been complete,

881
00:59:07.830 --> 00:59:12.420
which is why we start with the super high level losses and then get down into

882
00:59:12.420 --> 00:59:13.253
the system states.

883
00:59:14.460 --> 00:59:17.700
I found it easier to add hazards.

884
00:59:18.440 --> 00:59:19.040
Yes.

885
00:59:19.040 --> 00:59:20.300
Um, and, and you know,

886
00:59:20.300 --> 00:59:25.180
you don't have to feel like you have to have this perfect before you're ready to

887
00:59:25.180 --> 00:59:25.660
move on.

888
00:59:25.660 --> 00:59:29.860
Because once you get your control structure built and all your control actions,

889
00:59:30.440 --> 00:59:35.020
as you start stepping through your control actions and you're uncovering, uh,

890
00:59:35.280 --> 00:59:39.660
unsafe control actions, if there's no hazard for it to map to,

891
00:59:39.810 --> 00:59:43.620
then all of a sudden the clarity comes and you go, oh, we're missing a hazard.

892
00:59:43.710 --> 00:59:44.543
Let's go add that.

893
00:59:45.050 --> 00:59:49.980
Yeah. Yeah. This, these were not the original six hazards that I came up with.

894
00:59:49.980 --> 00:59:52.460
The first, my first blush through this analysis,

895
00:59:52.860 --> 00:59:56.100
I came up with something and then I kind of re wicked, um,

896
00:59:56.100 --> 00:59:57.740
either cuz there wasn't a clear,

897
00:59:57.960 --> 01:00:01.860
wasn't a clear hazard or I had a UCA and I thought it needed to be broken out a

898
01:00:01.860 --> 01:00:03.500
little bit more. That type of thing.

899
01:00:03.680 --> 01:00:07.340
So that goes back to that iterative process. So you get,

900
01:00:07.340 --> 01:00:09.580
you get something on paper that you think is, is pretty,

901
01:00:09.920 --> 01:00:12.980
pretty decent and don't ns your teeth over it for two weeks.

902
01:00:13.120 --> 01:00:15.860
You get something on paper that you think seems reasonable,

903
01:00:15.860 --> 01:00:19.820
that you think meets the definition of a, you know, a system level state.

904
01:00:20.240 --> 01:00:24.500
And then as you go through the ucas, that will, will become more clear.

905
01:00:24.740 --> 01:00:26.460
I think there was a question. Yep.

906
01:00:26.920 --> 01:00:28.500
So, um, it looks like have

907

01:00:35.330 --> 01:00:36.163
Yes.

908
01:00:38.300 --> 01:00:39.190
Hazards that,

909
01:00:49.860 --> 01:00:52.470
Yeah. So the, the question was, there's,

910
01:00:52.470 --> 01:00:55.310
there's hazards that trace to more than one accident.

911
01:00:55.690 --> 01:00:59.310
Can you have accidents that trace down to more than one hazard as well,

912
01:00:59.350 --> 01:01:00.430
I think was part of the question.

913
01:01:00.610 --> 01:01:03.950
And then can you use that for some kind of prioritization or something along

914
01:01:03.950 --> 01:01:08.030
those lines? And you absolutely can, I'll talk about that in the afternoon, uh,

915
01:01:08.030 --> 01:01:12.390
because you don't get a risk matrix out of this. So y you have 30 mitigations,

916
01:01:12.420 --> 01:01:16.110
what do you go after? You only have so much time and money. Um,

917
01:01:16.170 --> 01:01:19.270
so we'll talk more about that. It comes into two things. One,

918
01:01:19.440 --> 01:01:21.430
maybe you're willing to accept a loss of mission,

919
01:01:21.430 --> 01:01:24.790
but you're not willing to accept a loss of life. So, so part of it is,

920
01:01:25.170 --> 01:01:29.030
is how you, um, prioritize your accidents, but then also how many,

921
01:01:29.810 --> 01:01:31.990
how many, uh, do they affect as well?

922
01:01:35.890 --> 01:01:39.150
All right, go to the next one.

923
01:01:41.350 --> 01:01:42.920
Alright, so I got about 20 minutes.

924
01:01:43.140 --> 01:01:47.120
So what I'd like to do is work on the safety control structure next.

925
01:01:47.320 --> 01:01:50.240
I don't know that we'll necessarily get a fully completed in the next 20

926
01:01:50.240 --> 01:01:54.680
minutes, but at least take a, take a good hack at it. Um,

927
01:01:54.820 --> 01:01:59.760
so first off, what do you guys think are important elements to this?

928
01:01:59.980 --> 01:02:04.160
I'm gonna write this down As we go along.

929
01:02:04.740 --> 01:02:06.920
Oh yeah, we've got boards. Thank you.

930
01:02:07.700 --> 01:02:09.160
You want to grab the markers or

931
01:02:15.090 --> 01:02:17.840
We'll make sure he writes big to you guys in the back.

932
01:02:29.160 --> 01:02:29.993
Thank you.

933
01:02:30.140 --> 01:02:30.973

Okay.

934
01:02:31.970 --> 01:02:34.310
All right. So what are some, um, important elements?

935
01:02:35.450 --> 01:02:36.283
Ground,

936
01:02:36.490 --> 01:02:38.110
Ground control station. Yep.

937
01:02:40.650 --> 01:02:42.230
And I have really terrible handwriting.

938
01:02:43.170 --> 01:02:47.990
Can you guys see that at all in the back? Yeah. All right.

939
01:02:48.140 --> 01:02:51.960
Well, all right. Ground control station.

940
01:02:55.380 --> 01:02:57.080
The operator. Yep.

941
01:03:04.180 --> 01:03:07.760
You can throw those on there too if you want. What else?

942
01:03:08.620 --> 01:03:10.560
The autopilot. Yep.

943
01:03:13.800 --> 01:03:18.300
Can you go back to Yeah.

944
01:03:20.740 --> 01:03:21.573
Maintainer.

945
01:03:22.390 --> 01:03:25.810
The maintainers, the guys who are towing it around and all that type of stuff.

946
01:03:27.120 --> 01:03:31.410
Yep. Maintainer,

947
01:03:35.970 --> 01:03:37.130
Antennas and spectrum.

948
01:03:37.770 --> 01:03:40.370
Antennas and spectrum. Yep. We'll find,

949
01:03:40.690 --> 01:03:44.330
I think that'll be a little bit too detailed for what we're gonna do so far,

950
01:03:44.750 --> 01:03:48.170
but I think we'll find that comes out when we get into the scenarios.

951
01:03:49.980 --> 01:03:51.860
Communications. So radios,

952
01:03:52.740 --> 01:03:57.260
communications or com system of some kind, calm links,

953
01:03:57.290 --> 01:03:58.420
calm system. Okay.

954
01:03:59.840 --> 01:04:01.340
Are you relying on gps?

955
01:04:03.900 --> 01:04:08.810
We can make an assumption if we're relying on GPS or not.

956
01:04:13.560 --> 01:04:15.460
So we can say nav, nav system

957
01:04:18.380 --> 01:04:23.270
weather. So weather would not be within our,

958
01:04:23.370 --> 01:04:27.070
the scope of our system, so we won't include that,

959
01:04:27.290 --> 01:04:31.390
but it could come up for sure. Um, one of the things that came out of this was,

960
01:04:31.570 --> 01:04:36.270
you know, it didn't have, you know, there's no anti-icing. So, uh, how do you,

961
01:04:36.650 --> 01:04:40.580
how do you sort through that? The camera?

962
01:04:43.410 --> 01:04:45.120
Sorry, I heard, I heard a few different things.

963
01:04:48.140 --> 01:04:53.030
Emergency procedures. So I think we'll get to that. We'll get to that later on.

964
01:04:53.090 --> 01:04:56.630
Deeper down. So I heard, I heard, um, flight control system

965
01:04:58.890 --> 01:05:01.670
was the flight control system. Is that what Yeah,

966
01:05:07.780 --> 01:05:09.270
What you said about weather. How about

967
01:05:13.800 --> 01:05:14.633
The limitation?

968
01:05:17.800 --> 01:05:20.740
So as far as like operational limitations,

969
01:05:21.960 --> 01:05:22.793
Um,

970
01:05:23.200 --> 01:05:28.200
Yeah, I think we'll find that out as we go, as we go deeper as well. Payload,

971
01:05:28.630 --> 01:05:30.640
mission. Payload. Yep. Payload.

972
01:05:41.840 --> 01:05:42.673

Camera.

973
01:05:42.880 --> 01:05:43.740
Camera. Yep.

974
01:05:43.760 --> 01:05:48.150
You said that and I didn't write it down camera.

975
01:05:49.370 --> 01:05:50.630
All right. I I

976
01:05:50.630 --> 01:05:51.463
Don't have any,

977
01:05:53.730 --> 01:05:58.190
But I imagine if hostile territory equivalent,

978
01:05:58.930 --> 01:06:03.670
you don't want your enemy to, to break and deal you

979
01:06:04.570 --> 01:06:05.310
System

980
01:06:05.310 --> 01:06:07.030
Yourself and bring the plane down. Yep.

981
01:06:07.450 --> 01:06:11.710
Is that classify a system that designed by shielding?

982
01:06:12.370 --> 01:06:12.860
Uh,

983
01:06:12.860 --> 01:06:13.693
Yeah,

984
01:06:13.710 --> 01:06:14.950
Unauthorized. Uh,

985
01:06:16.580 --> 01:06:19.920
So basically cybersecurity risk, uh, unauthorized control.

986
01:06:20.120 --> 01:06:22.560
I think we'll find that when we get down into scenarios.

987
01:06:27.180 --> 01:06:28.013
Yeah,

988
01:06:28.210 --> 01:06:32.390
The actual uav. Yeah, yeah, yeah. You can,

989
01:06:32.390 --> 01:06:33.510
you can do the airframe.

990
01:06:37.270 --> 01:06:37.560
I'll

991
01:06:37.560 --> 01:06:38.393
Put it up here.

992
01:06:41.390 --> 01:06:42.223
Prop

993
01:06:46.530 --> 01:06:47.520
Propulsion. I heard

994
01:06:48.330 --> 01:06:49.163
Propulsion,

995
01:06:52.170 --> 01:06:55.430
So when I did it, I, I broke it out.

996
01:06:55.590 --> 01:06:57.790
I had the engine as a separate,

997
01:06:58.510 --> 01:07:01.910
I just called it engine or propulsion system, something along those lines.

998
01:07:06.090 --> 01:07:06.923
Sensor.

999

01:07:07.650 --> 01:07:08.483
Say that again?

1000
01:07:10.740 --> 01:07:11.573
Upgrade

1001
01:07:11.610 --> 01:07:12.443
Sensor.

1002
01:07:12.540 --> 01:07:17.190
Yeah, you could, you can split out the autopilot and uh, actuators and sensors.

1003
01:07:17.890 --> 01:07:22.590
Um, so for now, I'm not gonna do that. We don't wanna make something that,

1004
01:07:22.740 --> 01:07:25.390
that, you know, it's gonna take us quite a while to,

1005
01:07:25.690 --> 01:07:30.390
to run through the analysis, but, um, But you could,

1006
01:07:30.390 --> 01:07:35.150
actuators, sensors, and this goes back to what Murph was saying, right?

1007
01:07:35.210 --> 01:07:39.870
He started off with three boxes for his analysis for the, uh, loyal wingman.

1008
01:07:40.210 --> 01:07:44.350
And then he ended up with, I don't know, 10 ish, somewhere in that vicinity,

1009
01:07:44.350 --> 01:07:48.870
eight 10, uh, by the end of it. So it's best to start high level.

1010
01:07:49.290 --> 01:07:52.830
And then as you go through, as you go through the ucas and you're like, Hey,

1011
01:07:52.830 --> 01:07:55.870

this would be a really important thing to talk about, but I don't have it on my,

1012
01:07:56.130 --> 01:07:57.030
on my control diagram,

1013
01:07:57.540 --> 01:08:01.710
then you can break it out as you need aerospace.

1014
01:08:02.010 --> 01:08:06.230
That's also gonna be outside the, uh, the, yeah,

1015
01:08:06.260 --> 01:08:10.710
it's environmental. Mm-hmm. So, and, and honestly,

1016
01:08:11.530 --> 01:08:12.363
say again.

1017
01:08:16.760 --> 01:08:19.980
So you could do it a couple different ways. I, I didn't include it in,

1018
01:08:20.040 --> 01:08:22.940
in my analysis and it came out later on. Um,

1019
01:08:25.080 --> 01:08:28.420
um, so I think, you know, this is, this is really about how,

1020
01:08:28.640 --> 01:08:29.940
what's important to you and what,

1021
01:08:29.940 --> 01:08:32.700
what do you think is important in the analysis. So you,

1022
01:08:32.840 --> 01:08:35.980
if you wanted to include it, you could always include it. And then if you find,

1023
01:08:36.720 --> 01:08:40.460
um, that, yeah, you can always remove it.

1024
01:08:43.990 --> 01:08:47.010

All right. What do you guys think?

1025
01:08:47.010 --> 01:08:51.210
So we've got ground control station, the operator, the autopilot,

1026
01:08:51.430 --> 01:08:56.170
the maintainer com system, nav system, flight control system,

1027
01:08:56.800 --> 01:09:00.250
payload camera, and airframe.

1028
01:09:00.410 --> 01:09:04.050
I think we also talked propulsion, prop, propulsion system as well.

1029
01:09:07.960 --> 01:09:11.780
Air traffic control, you could include them in the system.

1030
01:09:16.720 --> 01:09:17.553
We said that.

1031
01:09:22.320 --> 01:09:26.700
So I did not include ATC in, in mind, but you, you could, whoever's telling,

1032
01:09:26.890 --> 01:09:31.860
telling the operator what to do. So when I,

1033
01:09:32.130 --> 01:09:34.340
when I did my analysis,

1034
01:09:35.740 --> 01:09:39.780
I aggregated those three together,

1035
01:09:40.250 --> 01:09:44.020
calm nav and the, the flight control system. I just call it the,

1036
01:09:44.240 --> 01:09:48.940
the vehicle management system just for, for ease of, of my analysis.

1037
01:09:51.120 --> 01:09:53.460
And I did not include the camera, but,

1038
01:09:53.520 --> 01:09:57.900
but it's definitely gonna be providing some feedback, so that could be useful.

1039
01:10:01.400 --> 01:10:02.233
All right.

1040
01:10:05.560 --> 01:10:06.393
Laptop.

1041
01:10:12.970 --> 01:10:16.140
Yeah. How does the relevant data get back? So I didn't,

1042
01:10:16.480 --> 01:10:20.300
that'd be a very good thing to include. I did, I did not include that in mine.

1043
01:10:21.040 --> 01:10:24.140
Um, but that would be a very good thing to include. So you can say, uh,

1044
01:10:24.680 --> 01:10:29.510
you know, ground, ground personnel or, I, I think,

1045
01:10:29.570 --> 01:10:33.510
uh, I think my analysis, I called them supported personnel or, you know, some,

1046
01:10:33.510 --> 01:10:35.750
something, something along those lines.

1047
01:10:38.200 --> 01:10:41.060
So I didn't have 'em in the, I didn't have 'em in the, uh,

1048
01:10:41.920 --> 01:10:46.140
safety control structure, but it, but it came out, uh,

1049
01:10:46.140 --> 01:10:48.500
throughout the analysis. But if you,

1050
01:10:48.560 --> 01:10:53.220

if you wanted to have some kind of link from the aircraft directly down to them,

1051
01:10:54.210 --> 01:10:57.040
There is the room, the operator.

1052
01:11:00.430 --> 01:11:02.760
Yeah. So, so just in this case,

1053
01:11:02.870 --> 01:11:05.840
it's one due to duet sitting on a laptop

1054
01:11:06.590 --> 01:11:06.880
That

1055
01:11:06.880 --> 01:11:08.640
Is, that is the control room. Would you

1056
01:11:08.800 --> 01:11:10.000
Separate the hardware from the person?

1057
01:11:10.820 --> 01:11:15.180
You could, yep, you could. So in this case, and when we,

1058
01:11:15.210 --> 01:11:18.500
when we go through, when I show you what I did for the safety control structure,

1059
01:11:18.760 --> 01:11:23.420
you'll see that the laptop had no culation uh,

1060
01:11:23.600 --> 01:11:27.020
um, power. It was literally just a pass through. You know, say, Hey,

1061
01:11:27.020 --> 01:11:30.180
go to 10,000 feet. It says go to 10,000 feet to the VMs,

1062
01:11:30.320 --> 01:11:34.620
and then the VMs would do whatever the culation is to, to make that happen. So,

1063

01:11:34.960 --> 01:11:39.660
uh, so I included the laptop, but it had no command,

1064
01:11:40.360 --> 01:11:42.780
um, uh, authority if you will,

1065
01:11:45.890 --> 01:11:50.600
Would include the total vehicle or operator.

1066
01:11:54.460 --> 01:11:55.640
You could, you could,

1067
01:11:55.660 --> 01:11:59.280
if you were particularly worried about ground ops and you wanted to focus in on

1068
01:11:59.280 --> 01:12:03.840
that, you could put in the, the, the tow vehicle operator and, and all that.

1069
01:12:03.840 --> 01:12:08.560
You know, what, what does, what does he or she need to get clearance to tow? Uh,

1070
01:12:08.560 --> 01:12:09.680
how do we make sure that we,

1071
01:12:09.900 --> 01:12:13.760
we put the chalks in once once we've gotten the aircraft to the engine runup

1072
01:12:13.960 --> 01:12:16.560
location, those types of things. You could definitely include that.

1073
01:12:16.560 --> 01:12:19.840
How do we make sure we pointed, pointed down the right end of the runway?

1074
01:12:20.220 --> 01:12:21.053
All of those things.

1075
01:12:23.490 --> 01:12:27.210
A lot of that lot of like down with scope.

1076
01:12:27.720 --> 01:12:28.120
Yeah.

1077
01:12:28.120 --> 01:12:32.610
What are you trying to analyze? And so obviously there's a lot of rabbit holes

1078
01:12:34.150 --> 01:12:36.170
mm-hmm. Like the autopilot system for example.

1079
01:12:37.030 --> 01:12:39.850
Or in our example with the initiator, you know,

1080
01:12:39.850 --> 01:12:42.490
the FG generator.

1081
01:12:42.870 --> 01:12:47.210
We just assumed that that cause we've a long time,

1082
01:12:50.910 --> 01:12:51.770
so at some point Yeah.

1083
01:12:52.640 --> 01:12:57.410
What trying to evaluate can sort things out.

1084
01:12:57.760 --> 01:12:58.190
Yeah.

1085
01:12:58.190 --> 01:13:01.490
And that's a little tough to do with the toy problem cuz you're not actually

1086
01:13:01.490 --> 01:13:03.530
trying to do this in, in real life.

1087
01:13:03.550 --> 01:13:07.850
So you don't know what the scope ought to be, um, as we, as we work through it.

1088
01:13:07.910 --> 01:13:12.650

But, but yeah, that's very, very correct. And, and,

1089
01:13:12.710 --> 01:13:15.130
and again, with that iterativeness, uh,

1090
01:13:15.130 --> 01:13:18.130
you may find that you wanna open up the scope. Uh,

1091
01:13:18.130 --> 01:13:21.810
we've also seen where folks have done a a another safety control structure.

1092
01:13:21.810 --> 01:13:25.090
Maybe they have a safety control structure for once systems's up in the air,

1093
01:13:25.090 --> 01:13:28.170
they have another safety control structure for ground operations.

1094
01:13:28.230 --> 01:13:31.010
That's something that you can, you can look at as well.

1095
01:13:33.150 --> 01:13:34.170
How does, how does

1096
01:13:34.270 --> 01:13:38.810
The process deal with the scope? You know,

1097
01:13:38.810 --> 01:13:41.770
from a mechanic standpoint, I could say that, well,

1098
01:13:41.830 --> 01:13:46.450
my scope is set up in my conditions of my losses mm-hmm. Made,

1099
01:13:47.110 --> 01:13:49.210
but we talked about loss, you know,

1100
01:13:49.550 --> 01:13:52.790
damage to the thing which could happen during total.

1101
01:13:53.370 --> 01:13:53.970

Yep. So,

1102
01:13:53.970 --> 01:13:56.790
Or we say, well, we're only worried about loss or take off the land.

1103
01:13:56.790 --> 01:14:00.630
We don't care about either side of. Mm-hmm. So where,

1104
01:14:00.730 --> 01:14:04.270
how does the process for he help you deal with the

1105
01:14:04.270 --> 01:14:07.670
Scope? Yeah. How does the process help you deal with the scope? That was,

1106
01:14:07.700 --> 01:14:11.030
that was the question. And I think, I think that's really about giving,

1107
01:14:11.100 --> 01:14:14.220
getting everyone on the, on the same mental model. What is it,

1108
01:14:14.250 --> 01:14:19.060
what is it you wanna accomplish as part of your safety evaluation? Um, what is,

1109
01:14:19.090 --> 01:14:22.260
what is the, you know, whoever the approval authority is for your,

1110
01:14:22.260 --> 01:14:26.180
for your test program, what do they care about? If, if maybe, uh,

1111
01:14:27.400 --> 01:14:27.620
uh,

1112
01:14:27.620 --> 01:14:31.420
this is an already operational system and you're putting a new payload on it and

1113
01:14:31.420 --> 01:14:35.700
you wanna test that new payload, maybe the, the ground ops is something that's,

1114

01:14:35.700 --> 01:14:38.820
that's well established and outside of the scope of a particular test program.

1115
01:14:39.680 --> 01:14:42.860
So, so that would just be part of the, what what's the goal of your analysis?

1116
01:14:43.200 --> 01:14:46.020
Uh, if this is a brand new thing that's never been done before, ever,

1117
01:14:46.690 --> 01:14:51.060
then you probably do wanna include ground ops to, to make sure that you've,

1118
01:14:51.060 --> 01:14:51.900
you've thought through it all.

1119
01:14:59.570 --> 01:15:03.590
Say again? Uh, two operators. Yep. Yep.

1120
01:15:03.590 --> 01:15:07.710
There's a line of sight and beyond line of sight. So you could do that as well.

1121
01:15:07.830 --> 01:15:12.470
I think I, I aggregated it into, into one, uh, for my safety control structure.

1122
01:15:12.970 --> 01:15:15.590
But you could have a beyond line of sight and a line of sight,

1123
01:15:15.650 --> 01:15:17.950
ground operator for sure. And you may,

1124
01:15:18.250 --> 01:15:22.810
you may find that that's useful as you go, go through the analysis. Alright,

1125
01:15:24.550 --> 01:15:28.050
so let's see. Got about eight minutes left.

1126

01:15:28.350 --> 01:15:31.130
So you guys all have your, your pieces of paper.

1127
01:15:31.950 --> 01:15:35.530
So based off of the things that we've talked about, um,

1128
01:15:35.590 --> 01:15:38.050
ground control station operator, autopilot,

1129
01:15:38.950 --> 01:15:42.810
the maintainers com, nav, flight control systems,

1130
01:15:43.720 --> 01:15:46.130
your payload camera,

1131
01:15:47.950 --> 01:15:52.930
the airframe propulsion system, atc, and then your ground personnel.

1132
01:15:53.720 --> 01:15:56.930
Just draw up something what you think that might look like as far as the

1133
01:15:57.170 --> 01:16:01.090
hierarchical structure. Uh, so what's, what's gonna be up on top?

1134
01:16:02.030 --> 01:16:05.490
Uh, I'll give you a hand. It's probably this guy, um, atc,

1135
01:16:06.270 --> 01:16:09.970
what's gonna be on top, what's gonna be on bottom, uh, what's,

1136
01:16:09.970 --> 01:16:14.210
what are the relationships, uh, between these systems?

1137
01:16:14.350 --> 01:16:16.730
And if you want, we can go ahead and aggregate this if you,

1138
01:16:16.990 --> 01:16:21.090
the calm nav and flight control systems, if you want and call it VMs,

1139
01:16:22.230 --> 01:16:25.170
uh, might make it easier since we've got a short timeline.

1140
01:16:26.350 --> 01:16:29.410
But just draw out what you think that might, might look like.