WEBVTT

1
00:00:40.415 --> 00:00:41.265
Loud and clear, Tom.

2
00:01:03.515 --> 00:01:05.045
Well, everybody, welcome back from break

3
00:01:05.545 --> 00:01:09.005
and I sincerely hope you enjoyed our previous session.

4
00:01:10.025 --> 00:01:14.425
Um, I did wanna point out that if you do have interest in

5
00:01:14.945 --> 00:01:18.585
a workshop that, again, is held annually,

6
00:01:18.585 --> 00:01:21.585
generally at the end of March, up in Boston at MIT,

7
00:01:22.325 --> 00:01:23.465
um, it's free.

8
00:01:24.005 --> 00:01:25.945
So all you gotta do is, is get there and back

9
00:01:25.945 --> 00:01:27.265
and take care of your logistics.

10
00:01:27.925 --> 00:01:31.905
Um, what's really unique about, uh, the workshops, uh,

11
00:01:31.925 --> 00:01:34.345
at least what, what I witnessed, uh, when I went a year

12
00:01:34.345 --> 00:01:38.905
or two ago was the, uh, diversity of the industries

13
00:01:38.905 --> 00:01:42.385
that are there presenting medical industry, automotive,

14
00:01:42.575 --> 00:01:47.345
rail, um, power, uh, production.

15
00:01:47.805 --> 00:01:51.385
So you get to see a wide variety of industries

16
00:01:51.445 --> 00:01:53.185
and how they've applied STPA.

17
00:01:53.605 --> 00:01:56.185
So it, it's quite fascinating for those that are interested.

18
00:01:56.725 --> 00:01:59.265
Um, I also failed to mention that the handbook

19
00:01:59.365 --> 00:02:03.145
and other STPA resources are already, uh,

20
00:02:03.445 --> 00:02:05.665
hosted in the resources section

21
00:02:05.805 --> 00:02:08.945
of our flight test safety.org website.

22
00:02:09.805 --> 00:02:11.865
So those are there for your use.

23
00:02:12.125 --> 00:02:13.465
Uh, we encourage you to go there

24
00:02:13.685 --> 00:02:15.705
and, um, and tap into those.

25
00:02:16.805 --> 00:02:19.425
Uh, okay. So I think we're learning a few things about,

26
00:02:19.845 --> 00:02:21.385
uh, to webinar.

27
00:02:21.725 --> 00:02:23.985

It appears that you're not gonna be able to see

28
00:02:24.615 --> 00:02:27.185
everybody's questions as they come into the presenter.

29
00:02:27.185 --> 00:02:28.865
That's just a limitation of the system.

30
00:02:29.325 --> 00:02:31.825
Uh, but our moderators are monitoring those questions,

31
00:02:32.405 --> 00:02:35.025
and then we'll try to parrot those as we ask them.

32
00:02:35.285 --> 00:02:39.025
So, um, keep those questions coming in.

33
00:02:39.205 --> 00:02:42.105
And I know John really likes that interaction, uh,

34
00:02:42.975 --> 00:02:44.185
from the audience, uh,

35
00:02:44.185 --> 00:02:45.945
just like he would be if he was teaching a class.

36
00:02:46.045 --> 00:02:48.505
So it was really a treat to have, uh, you know, one

37
00:02:48.505 --> 00:02:52.265
of the more prominent instructors from MIT here in our midst

38
00:02:52.325 --> 00:02:54.825
and, and giving, uh, a presentation on STPA.

39
00:02:55.405 --> 00:02:59.685
Uh, we have a real special treat for you today with, uh,

40
00:02:59.685 --> 00:03:02.685
Colonel Doug Weikert, uh, who's coming from us from,

41
00:03:02.705 --> 00:03:03.885
uh, Colorado Springs.

42
00:03:03.885 --> 00:03:05.725
He's wearing a flight suit, I'm envious.

43
00:03:06.225 --> 00:03:08.165
Uh, he checked in earlier this morning.

44
00:03:08.265 --> 00:03:09.605
He was, uh, shooting his wife.

45
00:03:09.745 --> 00:03:12.645
So, uh, still a fighter, pilot's fighter pilot.

46
00:03:13.185 --> 00:03:15.765
Um, he's currently the head of the, uh,

47
00:03:15.765 --> 00:03:18.485
air Force Academy's aeronautical department.

48
00:03:18.665 --> 00:03:20.845
So he's growing our seed corn in the

49
00:03:20.845 --> 00:03:22.045
community, which is fantastic.

50
00:03:22.905 --> 00:03:25.525
Um, he's got combat experience, plenty

51
00:03:25.525 --> 00:03:28.445
of experience doing fast jet testing of all varieties.

52
00:03:28.915 --> 00:03:31.845
He's commanded test organizations at the group, uh,

53
00:03:31.865 --> 00:03:34.605
and squadron levels and, uh, served as chief

54
00:03:34.625 --> 00:03:36.125

of policy programs

55
00:03:36.305 --> 00:03:39.405
and resources for Air Force test and evaluation.

56
00:03:39.665 --> 00:03:41.925
So some, some really heady stuff there.

57
00:03:42.145 --> 00:03:46.365
Um, this is just a, a small snapshot of beaker's resume.

58
00:03:46.595 --> 00:03:47.605
It's very impressive.

59
00:03:48.395 --> 00:03:50.245
He's a distinguished graduate from both the Air Force

60
00:03:50.245 --> 00:03:52.365
Academy and US Naval Test Pilot School.

61
00:03:52.365 --> 00:03:54.645
And I noted that he was wearing that patch

62
00:03:54.715 --> 00:03:56.725
with Pride the other day on his flight suit.

63
00:03:57.145 --> 00:03:58.445
Um, I don't recall which class,

64
00:03:58.545 --> 00:04:00.725
but maybe he'll tell us that when I turn it over to him.

65
00:04:01.385 --> 00:04:04.285
Um, his educational background is equally impressive,

66
00:04:04.445 --> 00:04:06.045
engineering degrees from MIT

67
00:04:06.545 --> 00:04:09.365
and, uh, air Force Institute of Technology, including a PhD.

68
00:04:10.105 --> 00:04:12.725
So this guy is, uh, super smart, uh,

69
00:04:12.725 --> 00:04:14.005
and I really wanted to highlight

70
00:04:14.005 --> 00:04:18.085
that he is not just a winner of the rate E 10 off award

71
00:04:18.435 --> 00:04:23.285
that, uh, uh, is presented at the annual, uh,

72
00:04:23.285 --> 00:04:24.925
symposium, banquet at the Society

73
00:04:24.925 --> 00:04:26.165
of Experimental Test Pilots.

74
00:04:26.745 --> 00:04:28.725
Um, he's a two-time winner

75
00:04:29.265 --> 00:04:34.205
and his 2018, uh, paper, uh, that he won

76
00:04:34.715 --> 00:04:37.405
this award with, uh, was on this very subject.

77
00:04:38.415 --> 00:04:42.155
So we really can't do any better, uh, than having beaker

78
00:04:42.155 --> 00:04:44.475
with us today and talking about STPA

79
00:04:44.475 --> 00:04:45.635
and his experience with it.

80
00:04:45.815 --> 00:04:47.275
And just a bit of trivia, if I could.

81
00:04:47.695 --> 00:04:52.235

The Red Turnoff Award, uh, was, uh, made in,

82
00:04:52.775 --> 00:04:56.165
uh, uh, me a memory of, uh,

83
00:04:57.065 --> 00:05:00.235
for Ray Turnoff who was a, uh, uh, test pilot

84
00:05:00.335 --> 00:05:01.475
for Con Conveyor, uh,

85
00:05:01.495 --> 00:05:02.715
and also the first president

86
00:05:02.715 --> 00:05:04.435
of SETP for those that didn't know.

87
00:05:04.575 --> 00:05:09.315
So, um, again, great to have, uh, uh, Colonel ert with us,

88
00:05:09.415 --> 00:05:10.955
uh, baker, good to see you there.

89
00:05:11.135 --> 00:05:13.195
And we really look forward to your presentation today.

90
00:05:13.495 --> 00:05:16.155
So I opened the vulnerability window

91
00:05:16.575 --> 00:05:19.955
and, uh, you can have your TOT at your leisure.

92
00:05:20.785 --> 00:05:22.835
Alright, well, thank you, Tom.

93
00:05:23.765 --> 00:05:26.745
The, uh, I think I'm finally showing the, uh,

94
00:05:26.845 --> 00:05:29.465
the correct screen if,

95
00:05:29.525 --> 00:05:33.965
um, alright.

96
00:05:34.305 --> 00:05:36.885
And, uh, so Poncho show gives me confirmation, sir,

97
00:05:36.885 --> 00:05:38.765
that we're, we're seeing the right, right, right scenes.

98
00:05:38.795 --> 00:05:41.895
This is, uh, it, it's really a strange new world, uh,

99
00:05:41.895 --> 00:05:44.495
that we find ourselves in, uh, with, uh,

100
00:05:45.685 --> 00:05:48.575
life will not be the same, uh, when we go back.

101
00:05:48.835 --> 00:05:50.455
Uh, and,

102
00:05:50.595 --> 00:05:52.455
and, you know, there's some things that, uh, you know,

103
00:05:52.455 --> 00:05:55.095
the silver lining in all of, uh, all of this right now is,

104
00:05:55.435 --> 00:05:57.205
you know, the ability to be multiple different places

105
00:05:57.225 --> 00:05:58.285
and do multiple different things.

106
00:05:58.945 --> 00:06:01.125
Of course, it'd be a whole lot neat to be all in person.

107
00:06:01.305 --> 00:06:04.565
But, uh, this morning I was, uh, was able to teach a class

108
00:06:04.585 --> 00:06:05.845

and attend this at the same time.

109
00:06:05.985 --> 00:06:07.445
And, and, uh, when I'm done here,

110
00:06:07.445 --> 00:06:09.605
I'll be going into a staff meeting, uh, all virtually.

111
00:06:10.145 --> 00:06:14.515
Um, so, so the the nature of this talk and, uh,

112
00:06:15.055 --> 00:06:19.595
and Ben Luther really, uh, hinted at it, uh, earlier, um,

113
00:06:20.545 --> 00:06:22.735
where, where he mentioned that the,

114
00:06:25.235 --> 00:06:27.855
on his question to, uh, to, to John about the, uh,

115
00:06:27.855 --> 00:06:29.175
the 2D risk matrix and, and,

116
00:06:29.195 --> 00:06:33.855
and how do we, uh, how can we incorporate STPA, uh, with

117
00:06:34.435 --> 00:06:36.695
what's, what's traditionally our, our tutor risk matrix.

118
00:06:37.635 --> 00:06:39.415
Um, and, and of,

119
00:06:39.415 --> 00:06:42.975
and of course, uh, I anticipated that, that,

120
00:06:43.045 --> 00:06:44.175
that comment from Ben,

121
00:06:44.455 --> 00:06:48.015
'cause, uh, he has been one of the, uh, the,

122
00:06:48.075 --> 00:06:51.895
the thought leaders in the domain of, of what, what do we,

123
00:06:52.115 --> 00:06:53.895
how do we move beyond the 2D risk matrix?

124
00:06:54.635 --> 00:06:56.655
Uh, because there's really no question that the,

125
00:06:57.235 --> 00:06:59.415
at least in, uh, in a lot of people's minds, uh,

126
00:06:59.415 --> 00:07:01.615
mine included that the, the 2D risk matrix is,

127
00:07:01.675 --> 00:07:03.015
is really ill suited.

128
00:07:03.595 --> 00:07:05.695
Uh, it's been abused, uh,

129
00:07:05.795 --> 00:07:07.215
and it's not particularly well suited

130
00:07:07.215 --> 00:07:09.095
for 21st century systems.

131
00:07:09.995 --> 00:07:12.055
Uh, what you see up there on the left is, uh,

132
00:07:12.115 --> 00:07:16.615
is Lieutenant John McGrady, uh, back in 1921, late 1921,

133
00:07:16.615 --> 00:07:18.095
right before he hopped in the, uh,

134
00:07:18.095 --> 00:07:20.695
that LaPierre biplane right there, uh,

135
00:07:20.795 --> 00:07:25.575

to set an altitude record, uh, almost 35,000 feet,

136
00:07:25.675 --> 00:07:27.135
uh, for that feet, he would win the first

137
00:07:27.135 --> 00:07:28.615
of three McKay trophies.

138
00:07:29.195 --> 00:07:32.815
Uh, it is a lot of fun to read the, um,

139
00:07:36.005 --> 00:07:37.895
read the flight test stories from, from that era.

140
00:07:38.215 --> 00:07:40.135
'cause, uh, they were, they were literally quite literally,

141
00:07:40.235 --> 00:07:41.055
uh, flying and doing

142
00:07:41.055 --> 00:07:42.295
flight tests by the seat of their pants.

143
00:07:43.075 --> 00:07:46.375
Uh, and, and the predominant kind of explanation

144
00:07:46.555 --> 00:07:50.055
or, uh, cause of actions at that time, the thinking was,

145
00:07:50.075 --> 00:07:52.215
was the domino model that you see there, uh,

146
00:07:52.315 --> 00:07:57.055
in which usually that very first domino that falls is,

147
00:07:57.115 --> 00:07:58.455
uh, is the fault of the worker.

148
00:07:58.595 --> 00:08:02.495
Uh, it comes from a industrial engineering, um, models, um,

149
00:08:03.475 --> 00:08:04.815
uh, it's a linear theory

150
00:08:04.815 --> 00:08:08.615
and it's just not, uh, it's not a good measure, uh,

151
00:08:08.715 --> 00:08:12.175
or not a good approach, uh, for 21st century, uh, systems.

152
00:08:12.315 --> 00:08:15.175
And, and the 20th century 2D risk matrix, uh,

153
00:08:15.315 --> 00:08:16.695
is also poorly suited.

154
00:08:16.695 --> 00:08:19.655
So in the 21st century, we've got increasingly complex

155
00:08:19.655 --> 00:08:22.495
systems and, and increasingly complex by multiple measures.

156
00:08:22.495 --> 00:08:24.455
If you just look at software lines of code, if you look at,

157
00:08:24.875 --> 00:08:26.015
you know, how far, how fast,

158
00:08:26.035 --> 00:08:28.375
or now much, you know, going much faster than we are in the,

159
00:08:28.475 --> 00:08:30.135
the LaPierre by plane there and,

160
00:08:30.155 --> 00:08:32.585
and definitely much higher, uh,

161
00:08:32.725 --> 00:08:34.945
the systems aren't increasingly coupled.

162
00:08:34.945 --> 00:08:36.665

They're systems of systems, uh,

163
00:08:36.665 --> 00:08:38.025
they're inherently non-linear.

164
00:08:38.565 --> 00:08:39.665
Uh, and,

165
00:08:39.685 --> 00:08:42.025
and so, you know, how do we understand these systems?

166
00:08:42.045 --> 00:08:44.785
And so I'm not gonna have the answers.

167
00:08:45.125 --> 00:08:48.345
Uh, and what the real point of today is to, is

168
00:08:48.345 --> 00:08:49.825
to really start the discussion.

169
00:08:50.365 --> 00:08:53.265
Um, this is something as a flight test community that we're,

170
00:08:53.265 --> 00:08:54.385
we're gonna have to get our arms around.

171
00:08:55.145 --> 00:08:58.325
Uh, and so that, I just wanna really plant some seeds as,

172
00:08:58.385 --> 00:09:02.005
you know, what, how do we move our risk management tools,

173
00:09:02.705 --> 00:09:04.605
um, and how do we develop appropriate ones

174
00:09:04.605 --> 00:09:05.845
for the, for the 21st century?

175
00:09:08.775 --> 00:09:11.195
So it's, uh, it, it's, it's useful to, uh,

176
00:09:11.655 --> 00:09:13.715
before we talk about risk management, to step back and,

177
00:09:13.715 --> 00:09:15.795
and think about what we mean by an accident.

178
00:09:16.215 --> 00:09:19.235
Uh, and an accident is a sudden, unexpected event

179
00:09:19.235 --> 00:09:21.355
that it resulted in an unwanted negative outcome.

180
00:09:21.575 --> 00:09:25.115
And, and so you can either prevent the unexpected event

181
00:09:25.215 --> 00:09:26.915
or prevent the negative outcome,

182
00:09:27.055 --> 00:09:28.115
and you prevent the accident.

183
00:09:28.115 --> 00:09:29.555
And that's exactly what we do through our,

184
00:09:29.895 --> 00:09:32.835
our safety planning, our T HHAs, our GCs, and,

185
00:09:33.175 --> 00:09:35.715
and STPA really, you know, falls into that as well.

186
00:09:35.715 --> 00:09:39.435
Where, you know, we're, we're, we're either trying to, uh,

187
00:09:39.795 --> 00:09:42.115
identify scenarios that result in the expectator events

188
00:09:42.115 --> 00:09:44.115
or if they happen, uh, through the control actions,

189
00:09:44.185 --> 00:09:45.275

keep them from happening.

190
00:09:45.815 --> 00:09:49.675
Um, but equally, uh, we should put a lot

191
00:09:49.675 --> 00:09:51.475
of effort over here on the design, uh,

192
00:09:51.695 --> 00:09:53.195
on the design side of things.

193
00:09:54.015 --> 00:09:55.035
Uh, and ultimately

194
00:09:55.035 --> 00:09:56.355
what we're doing a flight test is we

195
00:09:56.355 --> 00:09:57.395
are understanding the system.

196
00:09:57.655 --> 00:10:00.995
Uh, there is in inherent ignorance about the system, uh,

197
00:10:00.995 --> 00:10:02.475
that is the nature of our flight test.

198
00:10:02.895 --> 00:10:05.675
Uh, and that's where we, you know, kind of in came up

199
00:10:05.675 --> 00:10:08.555
and introduce the concept of risk awareness, uh, that,

200
00:10:08.555 --> 00:10:11.335
we'll, we'll talk about when you

201
00:10:11.525 --> 00:10:12.695
step back and think about it.

202
00:10:12.705 --> 00:10:15.215
We've really got some crazy ways of looking at accidents.

203
00:10:15.215 --> 00:10:17.895
This is, uh, probably the predominant one in the aviation,

204
00:10:18.195 --> 00:10:20.215
uh, world.

205
00:10:20.315 --> 00:10:25.015
And, and this is frankly, not very, very, very helpful.

206
00:10:25.235 --> 00:10:27.615
Um, you know, the idea that we design these barriers

207
00:10:27.635 --> 00:10:30.215
to prevent accidents, but all barriers have holes.

208
00:10:30.215 --> 00:10:32.095
And when the holes line up, you get an accident.

209
00:10:33.015 --> 00:10:36.315
Um, sure you can, you can look back after the fact

210
00:10:36.315 --> 00:10:37.555
and say, Hey, look, yep, there was

211
00:10:37.555 --> 00:10:38.635
a hole there, there's a hole there.

212
00:10:38.635 --> 00:10:40.035
But what we really want to know

213
00:10:40.135 --> 00:10:43.555
and what our, our tests, our our risk management

214
00:10:43.555 --> 00:10:45.595
and flight tests, you know, we need to identify the holes

215
00:10:45.935 --> 00:10:47.435
before the accident occurs.

216
00:10:48.325 --> 00:10:50.145

Uh, and of course, the, the, uh,

217
00:10:50.145 --> 00:10:51.465
Swiss cheese model's not the only one.

218
00:10:51.465 --> 00:10:54.525
We already talked about the domino model, uh, the, uh,

219
00:10:55.025 --> 00:10:58.965
in the sixties, the, uh, epidemiological model, uh,

220
00:10:58.965 --> 00:11:00.205
for accidents and,

221
00:11:01.885 --> 00:11:05.305
and what all these other accident models were really came

222
00:11:05.305 --> 00:11:07.545
about is systems in the 20th century we're

223
00:11:07.545 --> 00:11:08.665
getting more complex as well.

224
00:11:09.005 --> 00:11:10.905
Uh, and so they're looking for other ways to kind

225
00:11:10.905 --> 00:11:13.745
of explain these systemic failures.

226
00:11:14.165 --> 00:11:16.425
Uh, the epidemiological one is actually kind of funny.

227
00:11:16.485 --> 00:11:19.465
Now, as you know, we've got the SARS-CoV-2

228
00:11:19.825 --> 00:11:21.345
pandemic, uh, going on.

229
00:11:22.045 --> 00:11:24.905
Uh, but the real reason that none of these really work is

230
00:11:24.905 --> 00:11:28.825
that they typically see accidents as a consequence

231
00:11:28.825 --> 00:11:30.265
of a linear chain of events.

232
00:11:30.805 --> 00:11:33.305
Uh, and thus they really kind of fail to, uh,

233
00:11:33.305 --> 00:11:35.585
capture the nature of complex systems.

234
00:11:37.035 --> 00:11:38.225
Let's take a, you know,

235
00:11:38.385 --> 00:11:39.865
a look at the space shuttle Columbia, so, you know,

236
00:11:40.065 --> 00:11:42.145
a 20th century, uh, mishap.

237
00:11:42.165 --> 00:11:45.585
But, uh, the accident was, was clearly the result.

238
00:11:46.085 --> 00:11:47.745
Uh, you know, if you want to see, say

239
00:11:47.745 --> 00:11:49.905
what the very first domino that fell was, uh,

240
00:11:49.905 --> 00:11:53.065
the foam from the left bipod ramp, uh, hitting the, uh,

241
00:11:53.135 --> 00:11:54.495
hitting the orbiter leading edge,

242
00:11:54.515 --> 00:11:55.695
uh, that was the cause of the accident.

243
00:11:56.325 --> 00:11:58.905

Um, but that ignores the,

244
00:12:03.065 --> 00:12:07.435
that ignores the, uh, the culture that, that apparently

245
00:12:07.575 --> 00:12:08.715
or misses the, the culture

246
00:12:08.715 --> 00:12:10.635
that ignore the design requirement.

247
00:12:10.895 --> 00:12:13.155
Uh, and I'm gonna quote here, uh, the design.

248
00:12:13.155 --> 00:12:14.475
This is the design requirement.

249
00:12:14.815 --> 00:12:16.795
The design shall preclude ice

250
00:12:16.815 --> 00:12:19.355
and debris from hitting the orbiter during pre-launch

251
00:12:19.355 --> 00:12:20.355
and flight operations.

252
00:12:20.895 --> 00:12:22.955
And yet, it happened, it happened 65

253
00:12:22.955 --> 00:12:24.755
times prior to Columbia.

254
00:12:25.295 --> 00:12:28.525
Um, and yet we did nothing about it.

255
00:12:28.905 --> 00:12:31.125
Uh, what about NASA's budget and launch schedule?

256
00:12:31.185 --> 00:12:32.645
How do they fall into this?

257
00:12:32.665 --> 00:12:35.925
Uh, you know, how they explain, you know, the mere fact

258
00:12:35.925 --> 00:12:37.205
that the, the accident was caused

259
00:12:37.225 --> 00:12:38.725
by the phone from the left bipod ramp.

260
00:12:39.195 --> 00:12:43.245
None of those factors fit into, uh, the Swiss cheese model.

261
00:12:44.195 --> 00:12:48.335
Uh, so this is Nancy Leviton's system, dynamic explanation

262
00:12:48.435 --> 00:12:49.975
of, of Columbia, and it captures many

263
00:12:49.975 --> 00:12:51.855
of those additional elements, uh,

264
00:12:52.035 --> 00:12:54.055
of a complex socio technological system.

265
00:12:54.635 --> 00:12:57.735
Uh, this is, uh, you heard John Thomas talk about stamp.

266
00:12:57.885 --> 00:12:59.695
This is an early example of stamp.

267
00:13:00.475 --> 00:13:03.575
Um, and of course, STPA is a natural byproduct,

268
00:13:03.875 --> 00:13:04.975
uh, from stamp.

269
00:13:05.665 --> 00:13:06.885
Uh, so this is definitely a,

270
00:13:06.925 --> 00:13:10.285

a move in the right direction towards embracing complexity,

271
00:13:10.745 --> 00:13:13.285
uh, which is a nature of the, uh, inherent nature

272
00:13:13.305 --> 00:13:15.605
of the 21st, uh, 21st century.

273
00:13:16.185 --> 00:13:19.005
Uh, this is a, a graph of software lines of code, uh,

274
00:13:19.005 --> 00:13:20.045
in military systems.

275
00:13:20.625 --> 00:13:23.685
Uh, NASA's got a great study on flight software complexity.

276
00:13:24.265 --> 00:13:27.765
Um, any way that you measure it, uh,

277
00:13:28.265 --> 00:13:30.285
our systems are becoming increasingly complex,

278
00:13:30.505 --> 00:13:32.485
and as they become more complex,

279
00:13:32.485 --> 00:13:34.525
they become more difficult to understand.

280
00:13:35.135 --> 00:13:37.245
Every time that you add a node to a system,

281
00:13:37.345 --> 00:13:39.605
you increase the number of possible system states

282
00:13:39.905 --> 00:13:41.605
by a factorial by in factorial.

283
00:13:41.665 --> 00:13:42.845
So, uh,

284
00:13:42.985 --> 00:13:47.085
and in factorial grows faster than an exponential does.

285
00:13:47.825 --> 00:13:49.645
And so as we add more

286
00:13:49.745 --> 00:13:53.965
and more states, uh, it quickly becomes very, very difficult

287
00:13:54.025 --> 00:13:57.245
for us as testers to completely characterize

288
00:13:57.705 --> 00:13:58.965
and understand the systems.

289
00:13:59.145 --> 00:14:00.685
So the question is, how do we get our arms

290
00:14:00.685 --> 00:14:02.485
around this as testers?

291
00:14:03.385 --> 00:14:05.165
Um, and so this was one attempt,

292
00:14:05.745 --> 00:14:08.785
um, risk awareness.

293
00:14:09.125 --> 00:14:13.305
Uh, we defined as, uh, as the perception of uncertainty

294
00:14:13.885 --> 00:14:16.865
and the projected potential projected outcomes resulting

295
00:14:16.865 --> 00:14:21.275
from uncertainty and just as situational awareness,

296
00:14:21.655 --> 00:14:23.995
uh, you can, you can develop that and grow that over time.

297
00:14:24.595 --> 00:14:27.555

I remember being surprised in pilot training when

298
00:14:28.175 --> 00:14:29.635
at the very bottom of our grade sheet,

299
00:14:29.635 --> 00:14:31.755
we would always get an assessment from the IP

300
00:14:31.755 --> 00:14:32.955
on, on situational awareness.

301
00:14:33.055 --> 00:14:34.595
And it started out very, very low.

302
00:14:34.735 --> 00:14:37.155
And, and, and slowly we got, we improved.

303
00:14:37.155 --> 00:14:38.715
And I thought, how could they possibly know?

304
00:14:39.275 --> 00:14:40.395
I mean, they were usually right that

305
00:14:40.435 --> 00:14:41.555
I had no clue what was going on.

306
00:14:42.015 --> 00:14:43.555
Uh, but how did they really know that?

307
00:14:43.895 --> 00:14:47.275
Um, and it turns out that you can, you, you, we, we,

308
00:14:47.345 --> 00:14:49.555
over time, by paying attention to it,

309
00:14:49.975 --> 00:14:53.205
we develop a certain sense of, you know, how

310
00:14:53.465 --> 00:14:54.925
how good is our essay at this point?

311
00:14:55.145 --> 00:14:56.765
Uh, there's some warning signs as you start

312
00:14:56.765 --> 00:14:59.805
to miss radio calls, as you start to skip checklist items.

313
00:14:59.815 --> 00:15:02.605
Those are, you know, warning signs

314
00:15:02.605 --> 00:15:04.605
that your situational awareness is starting to go low.

315
00:15:05.375 --> 00:15:08.395
Uh, I think the same thing can be true for risk awareness.

316
00:15:08.775 --> 00:15:12.275
Uh, if we, if we put the focus on what we don't know,

317
00:15:12.275 --> 00:15:13.435
and then the uncertainty

318
00:15:13.655 --> 00:15:16.395
and putting bounds on what we don't know, that starts

319
00:15:16.455 --> 00:15:20.155
to enhance our level of, of where the risk is.

320
00:15:20.355 --> 00:15:23.315
'cause risk is ultimately all about uncertainty.

321
00:15:24.245 --> 00:15:27.465
Uh, so we wrote a paper on this, uh, presented it, uh,

322
00:15:27.645 --> 00:15:29.345
two years ago in Anaheim.

323
00:15:29.645 --> 00:15:31.425
Uh, it's, the easiest way to get a copy

324
00:15:31.425 --> 00:15:33.625

of it is if you merely Google risk awareness,

325
00:15:33.625 --> 00:15:36.265
flight test safety, uh, the very first link that'll come up.

326
00:15:36.605 --> 00:15:38.905
Uh, and again, another plug plug for the, uh,

327
00:15:38.905 --> 00:15:40.785
flight test safety facts, uh,

328
00:15:40.815 --> 00:15:42.465
that the Flight Test Safety Committee is putting out.

329
00:15:42.465 --> 00:15:44.465
The very first link that'll come out when you Google risk

330
00:15:44.465 --> 00:15:47.585
awareness, flight test safety, uh, is, uh,

331
00:15:47.845 --> 00:15:49.225
is is the paper from Anaheim.

332
00:15:49.245 --> 00:15:53.065
Uh, you're also welcome to, to email me, um, uh,

333
00:15:53.065 --> 00:15:54.505
and carry on the conversation as well.

334
00:15:55.315 --> 00:15:57.415
Uh, so why the focus on uncertainty?

335
00:15:58.595 --> 00:16:01.365
It's because flight test is the gradual process

336
00:16:01.945 --> 00:16:03.245
of reducing uncertainty.

337
00:16:03.245 --> 00:16:06.125
And if we examine the scope of what we mean by uncertainty,

338
00:16:06.585 --> 00:16:08.605
we can start to appreciate the fact that there are,

339
00:16:08.735 --> 00:16:10.485
there are different types of uncertainty.

340
00:16:11.385 --> 00:16:14.165
You can predict the role of a die,

341
00:16:14.825 --> 00:16:16.245
or you can't predict actually

342
00:16:16.245 --> 00:16:17.405
what the role of the die is gonna be.

343
00:16:17.405 --> 00:16:19.965
But you can talk about accurately about the probabilities

344
00:16:20.265 --> 00:16:21.845
of particular roles occurring.

345
00:16:22.435 --> 00:16:24.015
Uh, that's one type of uncertainty.

346
00:16:24.015 --> 00:16:25.135
That's one type of unknown.

347
00:16:25.555 --> 00:16:29.015
And that's different than when you have ambiguous scenarios

348
00:16:29.015 --> 00:16:30.135
that are bounded, you know,

349
00:16:30.135 --> 00:16:31.375
that something is going to happen.

350
00:16:31.755 --> 00:16:35.175
Uh, you can't say specifically like which one, uh,

351
00:16:35.235 --> 00:16:37.735

but you might be able to put bounds on different

352
00:16:37.735 --> 00:16:38.855
likelihoods of different of those.

353
00:16:39.435 --> 00:16:43.895
Uh, then also things that we know that we can't know.

354
00:16:44.275 --> 00:16:46.535
Uh, so for example, in physics, there's the, the concept

355
00:16:47.155 --> 00:16:49.495
of you, you can't heisenberg certain principle.

356
00:16:49.495 --> 00:16:53.255
You, you can't simultaneously know the, the position

357
00:16:53.255 --> 00:16:54.575
and momentum of a particle in physics.

358
00:16:54.915 --> 00:16:57.215
Uh, so there are limitations to our knowledge

359
00:16:57.445 --> 00:16:59.215
that are known and acknowledged.

360
00:16:59.955 --> 00:17:02.015
Um, and then of course, there's the things

361
00:17:02.215 --> 00:17:03.295
that we, we don't know.

362
00:17:04.255 --> 00:17:09.195
And it's, it's common to divide these domains of uncertainty

363
00:17:09.195 --> 00:17:10.235
to two different axes.

364
00:17:11.255 --> 00:17:15.635
Uh, there are, uh, types of uncertainty that,

365
00:17:15.635 --> 00:17:17.635
that are variable in nature, uh,

366
00:17:17.695 --> 00:17:19.355
and uncertainty due to randomness.

367
00:17:19.815 --> 00:17:22.275
Uh, and that's what's, uh, shown up here in the, uh,

368
00:17:22.415 --> 00:17:25.315
the left hand side of this, uh, of this knowledge thing.

369
00:17:25.335 --> 00:17:28.515
You, so all your casino games, you can, you can write down

370
00:17:28.515 --> 00:17:32.025
what the probability of any of a particular role, uh,

371
00:17:32.045 --> 00:17:35.145
of a die is in a casino or a particular hand in blackjack.

372
00:17:35.195 --> 00:17:36.505
Those are known, uh,

373
00:17:36.505 --> 00:17:37.665
and you have, uh,

374
00:17:37.665 --> 00:17:39.385
very well known probabilities what those are.

375
00:17:39.445 --> 00:17:42.345
So those are sta stochastic, uh, risk unknowns.

376
00:17:42.345 --> 00:17:43.865
And this is typically called the risk domain.

377
00:17:44.365 --> 00:17:46.825
But then there's also this other half

378
00:17:46.885 --> 00:17:47.905

of the knowledge plane,

379
00:17:48.845 --> 00:17:50.885
and that's where we live in flight test.

380
00:17:51.315 --> 00:17:53.445
That is due to low knowledge, is known

381
00:17:53.445 --> 00:17:55.205
as epistemic uncertainty.

382
00:17:55.825 --> 00:17:59.565
Uh, and it's, it's here that makes it very, very difficult.

383
00:17:59.565 --> 00:18:02.805
Unfortunately, in flight test with our 2D risk matrix,

384
00:18:02.865 --> 00:18:05.845
we tend to treat problems like this, uh,

385
00:18:05.985 --> 00:18:10.285
as if they were risk problems, our ths and GMCs.

386
00:18:10.745 --> 00:18:12.485
And when we come up with the 2D risk matrix,

387
00:18:12.745 --> 00:18:14.765
we treat the problems as this when they're really

388
00:18:15.365 --> 00:18:16.405
a right half plane.

389
00:18:16.505 --> 00:18:17.805
And we, we collectively call

390
00:18:17.805 --> 00:18:19.005
that right half plane ignorance.

391
00:18:19.025 --> 00:18:21.965
And that is not a, a pejorative term.

392
00:18:21.965 --> 00:18:24.765
Ignorance is merely lack of knowledge.

393
00:18:25.505 --> 00:18:29.085
And so what we do in flight test when we take a a new

394
00:18:29.085 --> 00:18:32.365
system, is we gradually migrate things from this half

395
00:18:32.365 --> 00:18:34.325
of the knowledge plane over

396
00:18:34.425 --> 00:18:36.325
to the left half of the knowledge plane.

397
00:18:38.365 --> 00:18:42.065
And, and the reason, uh, that is important,

398
00:18:42.065 --> 00:18:43.305
shows up in the box scores.

399
00:18:43.365 --> 00:18:48.015
So I have not updated this, uh, Tom at, uh,

400
00:18:48.015 --> 00:18:49.775
today's opening did give the, uh,

401
00:18:49.875 --> 00:18:51.655
the additional three events that we, uh,

402
00:18:51.675 --> 00:18:53.775
we had the latter half of, of 2019.

403
00:18:53.795 --> 00:18:55.415
So this is up through May of 2019.

404
00:18:55.835 --> 00:18:58.375
Uh, but the fact is that uncertainty tends to dominate,

405
00:18:59.115 --> 00:19:00.895

uh, accidents and flight tests.

406
00:19:00.895 --> 00:19:03.295
It's, it's clear there on the statistics, um,

407
00:19:04.275 --> 00:19:05.295
for the accidents.

408
00:19:05.315 --> 00:19:07.535
Uh, they're all listed there on this, on the left hand side.

409
00:19:07.535 --> 00:19:10.055
That's 18 total class a's a total

410
00:19:10.055 --> 00:19:11.335
loss class a's in eight years.

411
00:19:11.675 --> 00:19:12.695
Um, all

412
00:19:12.695 --> 00:19:16.455
but five of those involved a fatality, uh, which

413
00:19:17.175 --> 00:19:19.055
represents 29 testers that have been killed in eight years.

414
00:19:20.415 --> 00:19:22.675
And, and for the ones that I could get an accident report

415
00:19:22.735 --> 00:19:25.035
for, uh, we've been them according

416
00:19:25.095 --> 00:19:26.475
to these three categories.

417
00:19:27.295 --> 00:19:31.035
And, and I think it's, it's not an unreasonable conjecture

418
00:19:31.035 --> 00:19:33.955
that, uh, the preponderance of flight test mishaps

419
00:19:34.475 --> 00:19:37.155
actually fall, uh, in this uncertainty

420
00:19:37.575 --> 00:19:38.955
or ignorance side of things.

421
00:19:39.235 --> 00:19:40.635
'cause, 'cause that's what we're doing in flight test.

422
00:19:41.055 --> 00:19:44.395
Uh, we don't really know fully about the system,

423
00:19:44.455 --> 00:19:46.315
and we're characterizing the system in flight test.

424
00:19:47.055 --> 00:19:48.275
And so that's why it's important.

425
00:19:48.775 --> 00:19:52.635
Uh, let's take a look at, uh, at risk awareness through the,

426
00:19:52.655 --> 00:19:53.915
uh, challenger mishap.

427
00:19:53.915 --> 00:19:57.155
And again, this is a, uh, a 20th century, uh, mishap.

428
00:19:57.155 --> 00:19:59.595
But this one is, is particularly well known, I think,

429
00:19:59.595 --> 00:20:01.035
by almost everybody in the audience.

430
00:20:01.375 --> 00:20:04.275
Uh, which is why it's useful to examine, uh,

431
00:20:04.855 --> 00:20:06.555
the risk awareness framework, uh,

432
00:20:06.555 --> 00:20:07.835

through this particular Mac app.

433
00:20:08.215 --> 00:20:09.955
Uh, and of course, anytime you,

434
00:20:09.955 --> 00:20:10.955
you look back at an accident,

435
00:20:10.955 --> 00:20:12.875
there's always a risk of hindsight bias.

436
00:20:13.495 --> 00:20:15.075
Um, but let's characterize the unknowns.

437
00:20:15.695 --> 00:20:19.515
So, so again, the, you know, what caused this, you know,

438
00:20:19.515 --> 00:20:21.955
the very first domino, or the only domino, right, uh,

439
00:20:22.215 --> 00:20:23.835
was the, the blow by of the O-rings.

440
00:20:24.455 --> 00:20:27.515
Um, and this SRB field joint, uh,

441
00:20:27.935 --> 00:20:30.835
should never have been exposed to, to combustion gases.

442
00:20:30.835 --> 00:20:32.475
There's this putty, the zinc grate putty here.

443
00:20:32.815 --> 00:20:37.185
Um, and so there never should have been, um, uh, any,

444
00:20:37.325 --> 00:20:40.345
any type of hot gas exposure, uh, to these O-rings.

445
00:20:40.685 --> 00:20:44.265
Um, but rather than characterize that unknown,

446
00:20:44.285 --> 00:20:47.045
the shuttle manager spent a lot of time, you know, know,

447
00:20:47.045 --> 00:20:49.325
looking at it and arguing that, well, we've, you know,

448
00:20:49.335 --> 00:20:52.605
we've got 66%, uh, margin here.

449
00:20:52.805 --> 00:20:55.485
'cause we've only had, uh, or we've got 33% margin

450
00:20:55.725 --> 00:20:58.445
'cause we've only had 66% blow by of the,

451
00:20:58.545 --> 00:20:59.605
of the first O-ring.

452
00:21:00.155 --> 00:21:02.485
That completely ignores the fact

453
00:21:02.835 --> 00:21:05.125
that the O-ring should not have any erosion whatsoever

454
00:21:05.145 --> 00:21:06.285
due to hot gases.

455
00:21:06.505 --> 00:21:08.165
Uh, this is an unexpected result.

456
00:21:08.665 --> 00:21:11.925
And so this is something, this, there was an unknown here

457
00:21:12.275 --> 00:21:15.365
that we failed to understand and failed to characterize.

458
00:21:16.065 --> 00:21:18.965
Uh, the thiol engineers were pretty sure

459
00:21:18.965 --> 00:21:21.445

that there was a temperature dependence, um,

460
00:21:21.665 --> 00:21:25.645
or to temperature relationship, uh, on the, uh,

461
00:21:25.665 --> 00:21:27.005
on, on the erosion problem.

462
00:21:27.345 --> 00:21:28.405
Uh, it was a known

463
00:21:28.465 --> 00:21:30.765
and acknowledged problem that was just not understood.

464
00:21:31.465 --> 00:21:33.125
And so this, these were the launches,

465
00:21:33.125 --> 00:21:34.405
these are the temperatures that launch,

466
00:21:35.205 --> 00:21:36.665
and this is exactly the data.

467
00:21:37.005 --> 00:21:40.545
Uh, this is a recreation from the report, uh, of

468
00:21:40.545 --> 00:21:41.745
what the shuttle managers looked on

469
00:21:41.745 --> 00:21:42.825
on the eve of the launch.

470
00:21:43.565 --> 00:21:45.065
Um, and

471
00:21:45.205 --> 00:21:47.385
so there's really no clear temperature dependence here.

472
00:21:47.385 --> 00:21:49.705
You know, we had a couple, couple launches where there were,

473
00:21:49.705 --> 00:21:51.945
where there was erosion up at 70, 75 degrees.

474
00:21:52.765 --> 00:21:57.415
Um, but if you consider all of the launches

475
00:21:58.035 --> 00:21:59.975
and the fact that every time that you've launched

476
00:22:00.545 --> 00:22:01.855
below 65 degrees,

477
00:22:01.855 --> 00:22:04.215
you've experienced erosion starts to paint a different picture.

478
00:22:04.915 --> 00:22:07.495
Uh, and then when you realize that, hey, we are about

479
00:22:07.495 --> 00:22:09.175
to launch colder than we've ever launched

480
00:22:09.175 --> 00:22:12.935
before, uh, completely outside the family of data,

481
00:22:13.235 --> 00:22:14.255
the data that we have.

482
00:22:14.355 --> 00:22:16.615
So, so here, what we've done is we've identified

483
00:22:16.985 --> 00:22:19.135
where the unknowns are and where the uncertainty is.

484
00:22:19.135 --> 00:22:20.735
Does that mean that we're gonna make a good decision?

485
00:22:20.955 --> 00:22:22.575
No, but we're a step closer.

486
00:22:24.135 --> 00:22:27.275

Um, I, I won't go into this too much t in in too much time,

487
00:22:27.575 --> 00:22:28.675
uh, in the interest of time,

488
00:22:28.695 --> 00:22:32.195
but there's a, there's a great backstory on, uh,

489
00:22:32.335 --> 00:22:34.915
on which physicist actually had the, uh,

490
00:22:35.375 --> 00:22:36.395
had, had the real story.

491
00:22:36.615 --> 00:22:37.915
Uh, so we'll save that one.

492
00:22:38.855 --> 00:22:42.625
Um, and then finally, there's this, uh, this, this concept

493
00:22:42.725 --> 00:22:44.625
of organizational drift, uh,

494
00:22:44.655 --> 00:22:46.665
that we'll talk a little bit more about now.

495
00:22:46.765 --> 00:22:48.425
And nasa, uh, at the time

496
00:22:48.425 --> 00:22:52.495
of the challenger accident had clearly drifted so, so drift.

497
00:22:52.715 --> 00:22:54.055
The concept of drift is something that I think

498
00:22:54.055 --> 00:22:56.295
that we've all experienced, uh, with any program there.

499
00:22:56.295 --> 00:22:57.935
There's time, uh,

500
00:22:58.075 --> 00:22:59.895
and resource limits, uh,

501
00:22:59.925 --> 00:23:03.535
that work against you gaining a knowledge of the system.

502
00:23:03.535 --> 00:23:06.695
There's always a boundary of unacceptable program delays.

503
00:23:07.235 --> 00:23:11.135
Uh, there's always a, a, a limit to the resources

504
00:23:11.135 --> 00:23:13.175
that can be invested in understanding the system.

505
00:23:13.175 --> 00:23:15.495
And these two boundaries create a gradient

506
00:23:15.765 --> 00:23:18.495
that naturally push you towards a mishap.

507
00:23:18.995 --> 00:23:20.975
And unfortunately, because of uncertainty,

508
00:23:21.075 --> 00:23:22.855
we don't really know where that boundary is.

509
00:23:23.355 --> 00:23:25.055
And so, recognizing drift

510
00:23:25.475 --> 00:23:27.375
and resisting the pressure, uh,

511
00:23:27.375 --> 00:23:31.015
that flight test teams often find, uh, ourselves under,

512
00:23:31.355 --> 00:23:33.695
you know, no program ever moves left.

513
00:23:33.955 --> 00:23:36.735

Uh, the schedule always pushes us to the right.

514
00:23:36.795 --> 00:23:40.615
And usually programs always try to maintain, you know,

515
00:23:40.615 --> 00:23:42.495
their, you know, it's almost like they look at the flight

516
00:23:42.495 --> 00:23:44.695
test schedule as margin, uh,

517
00:23:44.835 --> 00:23:46.205
for the overall program schedule.

518
00:23:46.205 --> 00:23:48.085
They hit, they hit with a, you know, date.

519
00:23:48.385 --> 00:23:49.885
Uh, the flight test team gets the, uh,

520
00:23:49.885 --> 00:23:53.045
system under tests late, uh, and we're expected to compress.

521
00:23:53.265 --> 00:23:55.245
And that, that pushes us, uh,

522
00:23:55.245 --> 00:23:56.685
and gives us less and less time.

523
00:23:57.455 --> 00:24:01.395
Uh, so, uh, and recognizing when drift is happening

524
00:24:01.615 --> 00:24:03.795
and resisting the pressure, uh, to give away

525
00:24:03.795 --> 00:24:08.195
that safety margin is, is a, is an important mindset here.

526
00:24:08.695 --> 00:24:10.835
Um, this isn't a flight test example,

527
00:24:10.895 --> 00:24:14.715
but it is a great example that illustrates, uh,

528
00:24:15.005 --> 00:24:16.195
drift in practice.

529
00:24:16.575 --> 00:24:20.475
Uh, this is Alaska Airlines 2 61, uh, back in 2000,

530
00:24:20.585 --> 00:24:24.155
crashed off the coast of California while en route from, uh,

531
00:24:25.015 --> 00:24:28.075
uh, Mexico up to, uh, up to San Francisco.

532
00:24:28.075 --> 00:24:29.555
Final destination was gonna be Seattle.

533
00:24:30.445 --> 00:24:34.305
Um, the failure was the, uh, trim jack screw,

534
00:24:34.645 --> 00:24:36.385
um, that failed.

535
00:24:36.525 --> 00:24:38.145
Uh, this, uh, was considered,

536
00:24:38.145 --> 00:24:39.785
it was based on a DC nine design.

537
00:24:40.585 --> 00:24:43.245
Uh, the jack screw was, was considered primary structure.

538
00:24:43.665 --> 00:24:45.325
Uh, this trim motor sits on top

539
00:24:45.425 --> 00:24:50.125
and turns, uh, this, this big three foot long jack screw.

540
00:24:50.865 --> 00:24:54.365

Um, in order to adjust the angle of incidents to trim the,

541
00:24:54.365 --> 00:24:55.445
uh, the horizontal tail here.

542
00:24:56.355 --> 00:25:00.255
Um, it was based on the DC nine des, uh, design, um, um,

543
00:25:00.545 --> 00:25:02.335
which was certified in 1965.

544
00:25:02.335 --> 00:25:04.695
And inherit inherited the certification from that.

545
00:25:06.345 --> 00:25:09.365
And, uh, by the time that the MD 11 was certified,

546
00:25:09.365 --> 00:25:12.085
if they had applied the updated certification criteria,

547
00:25:12.105 --> 00:25:13.845
you would not have been allowed to, uh,

548
00:25:13.935 --> 00:25:14.965
carry this flight control

549
00:25:14.965 --> 00:25:16.005
through primary structure like this.

550
00:25:16.065 --> 00:25:19.685
But at the time that it was, uh, there's not much, much, uh,

551
00:25:19.685 --> 00:25:20.965
there's very little doubt as to

552
00:25:20.965 --> 00:25:22.725
what happened in this mishap, uh,

553
00:25:22.725 --> 00:25:24.685
because we recovered the jack screw from the bottom

554
00:25:24.685 --> 00:25:27.685
of the Pacific, and the threads, uh, uh,

555
00:25:27.835 --> 00:25:29.365
from the, the Acme nut.

556
00:25:29.545 --> 00:25:32.645
Um, were, were still around, uh, the,

557
00:25:32.645 --> 00:25:34.245
the now Threadless Acme nut were still

558
00:25:34.245 --> 00:25:35.525
wrapped around the jack screw.

559
00:25:35.545 --> 00:25:37.685
So there, there's, it's very clear, uh,

560
00:25:37.685 --> 00:25:40.205
this Acme nut was made of the softer material in order

561
00:25:40.205 --> 00:25:42.085
to wear pre, uh, wear prematurely.

562
00:25:42.245 --> 00:25:44.685
'cause it was much easier to replace this part than it

563
00:25:44.805 --> 00:25:46.325
replaced the, uh, Jcrew.

564
00:25:47.085 --> 00:25:50.105
Um, and so that metal on metal lubrication is,

565
00:25:50.405 --> 00:25:52.545
is an essential key maintenance task.

566
00:25:53.125 --> 00:25:56.305
Uh, and when the DC nine was originally certified in 1965,

567
00:25:56.575 --> 00:26:00.465

premature wear of this Acme nut was a, was a known problem.

568
00:26:00.925 --> 00:26:04.425
And so the recommended lube interval was every 350 hours.

569
00:26:04.525 --> 00:26:05.905
Now, luing, this is not easy.

570
00:26:06.165 --> 00:26:08.545
Uh, it sits up here at the, the top of the tail.

571
00:26:08.695 --> 00:26:09.625
There's this blind

572
00:26:09.625 --> 00:26:10.865
access panel that you have to get through.

573
00:26:11.865 --> 00:26:15.645
Um, when the MD 11 was originally certified, uh,

574
00:26:16.015 --> 00:26:18.685
based on the original manufacturer recommendation interval

575
00:26:18.755 --> 00:26:22.845
from, uh, from the DC nine, it was 350 hours, uh, interval,

576
00:26:22.845 --> 00:26:25.155
where you had to lube this jack screw, uh,

577
00:26:25.465 --> 00:26:27.675
that was, uh, relaxed.

578
00:26:27.735 --> 00:26:30.235
Uh, at the time of, um, in 1970 and,

579
00:26:30.415 --> 00:26:34.995
or 1985 rather, uh, Alaska Airlines moved it to a, a,

580
00:26:35.175 --> 00:26:38.035
the beach check, every other beach check, which meant, uh,

581
00:26:38.035 --> 00:26:40.195
that they were every 700 hours, uh,

582
00:26:40.195 --> 00:26:41.675
that part was being lubricated.

583
00:26:42.635 --> 00:26:44.975
Uh, two years later, b checks were extended.

584
00:26:45.195 --> 00:26:48.055
Uh, so now it was being lubed every thousand hours, uh,

585
00:26:48.315 --> 00:26:52.495
in 1991, um, or in 88, they eliminated B checks.

586
00:26:52.495 --> 00:26:54.575
They moved it to every eighth a check, uh,

587
00:26:54.595 --> 00:26:55.935
but still kept at the same interval.

588
00:26:55.935 --> 00:26:58.495
But then in 1991, uh, the a checks, uh,

589
00:26:59.115 --> 00:27:00.415
uh, interval was extended.

590
00:27:02.045 --> 00:27:04.665
Um, so now we're lubing it every 1600 hours,

591
00:27:04.685 --> 00:27:08.705
and then we extend, and again, in 94 to, uh, to 200 hours.

592
00:27:09.245 --> 00:27:11.865
And then finally, they moved it to a, uh,

593
00:27:12.025 --> 00:27:13.265
a time phase task card.

594
00:27:13.265 --> 00:27:14.825

So that was being lubed every eight months.

595
00:27:15.285 --> 00:27:16.865
Uh, so 2,500 hours.

596
00:27:16.865 --> 00:27:19.225
So what we have is over 30 years,

597
00:27:19.845 --> 00:27:22.705
in almost order magnitude extension of the lule,

598
00:27:22.775 --> 00:27:27.505
from a critical part, from 350 hours to 2,500 hours in,

599
00:27:27.885 --> 00:27:30.385
in no single decision anywhere along here

600
00:27:30.525 --> 00:27:31.665
was, was irrational.

601
00:27:32.045 --> 00:27:34.345
Um, it was all, you know, all kind of made sense.

602
00:27:34.375 --> 00:27:36.665
Well, you know, what's the big deal going from 700,000?

603
00:27:36.665 --> 00:27:38.945
What's the big deal going from a, but when you step back

604
00:27:38.945 --> 00:27:41.145
and look at from the big scheme of things, uh,

605
00:27:41.285 --> 00:27:42.945
so this is the essence of drift.

606
00:27:43.205 --> 00:27:44.265
Uh, the exact same thing

607
00:27:44.465 --> 00:27:45.585
happened with the, uh, the inplay checks.

608
00:27:45.585 --> 00:27:48.665
You can actually measure how much free play, uh, there is

609
00:27:48.665 --> 00:27:50.865
between the jack screw and, and the Inplay check.

610
00:27:50.865 --> 00:27:52.905
And, and, and we see the exact same type of drift.

611
00:27:53.155 --> 00:27:56.265
Again, no single decision anywhere here is

612
00:27:56.525 --> 00:27:57.865
by itself unreasonable,

613
00:27:57.925 --> 00:28:01.225
but taken in, in sum total, it's, it's, it's mind boggling,

614
00:28:01.685 --> 00:28:04.345
um, that this happens over time to organizations.

615
00:28:04.345 --> 00:28:05.625
That's organizational drift.

616
00:28:06.645 --> 00:28:09.145
The real tragic footnote about Alaska 2 61 is

617
00:28:09.145 --> 00:28:10.145
that they almost caught it.

618
00:28:10.405 --> 00:28:14.345
Uh, this is the work card, uh, from the a sea check.

619
00:28:14.845 --> 00:28:17.545
Uh, this is the sea check two years prior to the accident.

620
00:28:18.285 --> 00:28:22.475
And they measured, uh, they measured the, uh,

621
00:28:22.475 --> 00:28:24.155

inplay at 40 mills, uh,

622
00:28:24.155 --> 00:28:26.435
which is right at the allowable limit.

623
00:28:26.495 --> 00:28:27.955
The allowable limit was 40 mills,

624
00:28:27.955 --> 00:28:29.115
and that's what they, they measured.

625
00:28:29.845 --> 00:28:33.225
Uh, and so originally, uh, the maintainer, uh,

626
00:28:33.225 --> 00:28:37.805
planned on replacing, uh, the part, uh, replacing that.

627
00:28:37.805 --> 00:28:38.925
They, uh, they put out an order.

628
00:28:39.665 --> 00:28:43.955
Um, it took a while to get the new part.

629
00:28:44.005 --> 00:28:45.475
Three days later, they said,

630
00:28:45.475 --> 00:28:46.555
Hey, that part still doesn't right.

631
00:28:46.575 --> 00:28:47.835
Go out there and measure that again.

632
00:28:47.935 --> 00:28:49.995
So they go back out, measure it one more time.

633
00:28:50.055 --> 00:28:53.235
And this time, they measured at 33 mils, seven thousands

634
00:28:53.415 --> 00:28:54.515
of an inch within limits.

635
00:28:55.015 --> 00:28:57.315
So they said, Hey, return it to service, um,

636
00:28:58.625 --> 00:28:59.955
with the, uh, with the warm nut.

637
00:29:00.565 --> 00:29:03.385
Um, so what this highlights, again,

638
00:29:03.385 --> 00:29:06.425
not a flight test example, but in terms of communicating

639
00:29:07.015 --> 00:29:09.465
uncertainty and communicating knowledge, uh,

640
00:29:09.465 --> 00:29:12.065
the designers clearly understood the criticality

641
00:29:12.065 --> 00:29:15.265
of the part, but over time, that knowledge was lost.

642
00:29:15.605 --> 00:29:17.305
Uh, and we'll, we see that again

643
00:29:17.305 --> 00:29:18.505
and again through accidents.

644
00:29:20.505 --> 00:29:23.975
So understanding, uh, so applying, uh,

645
00:29:24.005 --> 00:29:25.575
risk awareness lessons and flight test.

646
00:29:25.575 --> 00:29:27.135
Uh, here are just a few examples.

647
00:29:27.795 --> 00:29:30.775
Um, you know, we already talked about the, uh, the o-rings

648
00:29:30.775 --> 00:29:34.175

with the Challenger, uh, understanding unexpected deviations

649
00:29:34.175 --> 00:29:35.255
before continuing on flight tests.

650
00:29:35.255 --> 00:29:37.335
This is kind of baked into a lot of our manuals,

651
00:29:37.335 --> 00:29:40.535
but in practice, uh, we often don't do that.

652
00:29:41.185 --> 00:29:46.005
Uh, so the C one 30 J mishap back in 2015 where they, uh,

653
00:29:46.005 --> 00:29:47.835
stalled the rudder, uh,

654
00:29:47.895 --> 00:29:50.075
and ended up departing the flight over geeing, uh,

655
00:29:50.455 --> 00:29:52.675
the airplane did recover, but it was a total loss.

656
00:29:53.375 --> 00:29:57.865
Um, that stall, uh,

657
00:29:57.865 --> 00:29:59.905
that rudder stall had happened on our previous test point.

658
00:30:00.725 --> 00:30:02.865
Um, so that was an unexpected result.

659
00:30:03.005 --> 00:30:06.225
Uh, there was clearly knowledge, uh,

660
00:30:06.245 --> 00:30:08.705
or a lack of knowledge about some key thing

661
00:30:08.895 --> 00:30:10.025
that we failed to understand.

662
00:30:10.205 --> 00:30:12.385
Uh, so again, that's, that's a lack of risk awareness.

663
00:30:13.085 --> 00:30:15.985
If, if the way the world is behaving starts to deviate from,

664
00:30:16.215 --> 00:30:19.345
from your kind of inherent model of the world, world,

665
00:30:19.345 --> 00:30:23.385
that's a sign, uh, that something, uh, something is amiss,

666
00:30:23.385 --> 00:30:24.505
that your model is not accurate.

667
00:30:24.645 --> 00:30:27.975
Um, same thing happened with the, uh, with the Gulfstream,

668
00:30:28.115 --> 00:30:29.895
uh, 2011 Gulfstream mishap.

669
00:30:30.035 --> 00:30:34.015
Uh, there had been two previous stalls, um,

670
00:30:34.835 --> 00:30:36.935
in ground effect, uh, during testing, uh,

671
00:30:36.935 --> 00:30:39.335
that were not fully understood, um,

672
00:30:39.755 --> 00:30:42.605
before the actual mishap mishap flight.

673
00:30:43.655 --> 00:30:47.215
A confirmation bias is probably, uh, is, is probably one

674
00:30:47.215 --> 00:30:48.455
of the most common biases in life.

675
00:30:48.455 --> 00:30:49.575

It's certainly one of the, uh,

676
00:30:49.575 --> 00:30:51.175
most common biases in flight tests.

677
00:30:51.555 --> 00:30:54.855
Uh, seeking contrary data, uh, is an attempt to counter

678
00:30:54.965 --> 00:30:56.175
that confirmation bias.

679
00:30:56.755 --> 00:30:58.695
You have to actively seek data

680
00:30:58.695 --> 00:31:01.855
that disproves your hypothesis instead of confirming it.

681
00:31:02.115 --> 00:31:03.575
Uh, so again, going back to the challenge

682
00:31:03.575 --> 00:31:04.895
of launch decision, you know,

683
00:31:05.135 --> 00:31:07.975
sampling on the dependent variable here is gonna give you an

684
00:31:07.975 --> 00:31:10.495
answer that, uh, you know, so you have to go out

685
00:31:10.495 --> 00:31:14.055
and seek, uh, ultimate, uh, explanations.

686
00:31:14.155 --> 00:31:17.255
You know, the same type of thing with the confirmation bias

687
00:31:17.835 --> 00:31:22.175
occurs when you've, you know, when you've completed 95%

688
00:31:22.715 --> 00:31:25.815
of the, uh, flight test envelope, um, you are still

689
00:31:25.875 --> 00:31:27.975
as uncertain about this remaining 5%,

690
00:31:28.235 --> 00:31:29.415
uh, as you were before.

691
00:31:29.475 --> 00:31:31.855
So continue to seek that contrary information.

692
00:31:32.575 --> 00:31:34.535
Continue to look for places where, hey,

693
00:31:34.535 --> 00:31:36.255
maybe we don't fully understand this.

694
00:31:37.435 --> 00:31:41.215
And then one of the best methods for

695
00:31:42.825 --> 00:31:45.275
keeping your finger on the pulse of, you know,

696
00:31:45.295 --> 00:31:48.595
how risk aware are we, is, how many surprises are there?

697
00:31:49.315 --> 00:31:51.395
Surprises are warnings, surprise,

698
00:31:51.415 --> 00:31:54.155
or warnings that either you do not understand the system

699
00:31:54.815 --> 00:31:58.035
or that you've covered un previously unappreciated

700
00:31:58.105 --> 00:31:59.595
uncertainty, um,

701
00:32:00.095 --> 00:32:02.595
or perhaps that the organization has drifted.

702
00:32:03.765 --> 00:32:05.665

So in the five minutes leading up

703
00:32:05.665 --> 00:32:08.985
to the X 31 air data mishap, there are at least three

704
00:32:09.985 --> 00:32:13.225
recognized surprises by the test team, uh, that indicated

705
00:32:13.485 --> 00:32:15.985
or should have indicated that they didn't understand

706
00:32:16.015 --> 00:32:18.025
what was happening to the system and what was going on.

707
00:32:18.045 --> 00:32:21.625
So those surprises are warnings to call timeout and,

708
00:32:22.045 --> 00:32:24.385
and start to build your appreciation, your knowledge,

709
00:32:24.385 --> 00:32:25.425
your understanding of the system.

710
00:32:26.785 --> 00:32:30.045
So up to now, we've been looking at accidents with, uh,

711
00:32:30.155 --> 00:32:33.325
with crystal clear real world 2020 hindsight.

712
00:32:33.825 --> 00:32:37.485
Um, and so here are some two examples of

713
00:32:37.485 --> 00:32:42.325
where risk awareness, um, helped, uh, with a direct mindset.

714
00:32:42.705 --> 00:32:47.085
Uh, so we developed a risk awareness, uh, while I was, uh,

715
00:32:47.085 --> 00:32:49.005
commander of a test group, uh, several years ago.

716
00:32:49.505 --> 00:32:53.765
Um, and so this first story is, is one that was long

717
00:32:53.765 --> 00:32:54.885
after I'd left, uh,

718
00:32:54.905 --> 00:32:56.365
but I heard about it from the squadron

719
00:32:56.365 --> 00:32:57.485
commander of a squadron.

720
00:32:57.585 --> 00:33:00.205
So, uh, there was a, uh, a test group

721
00:33:00.205 --> 00:33:01.645
that was doing a, a test.

722
00:33:01.785 --> 00:33:04.845
Uh, it was actually in support of an operational test,

723
00:33:05.935 --> 00:33:09.515
and the A 10 pilot, the, uh, the weapons school, uh,

724
00:33:09.805 --> 00:33:12.115
patch wear flight, uh, flight briefer.

725
00:33:12.375 --> 00:33:15.195
Um, and of course, one of the, the flight test engineer

726
00:33:15.195 --> 00:33:18.515
that was in charge of the test, uh, had been, uh, in one

727
00:33:18.515 --> 00:33:19.835
of the squadrons that was in my organization.

728
00:33:21.715 --> 00:33:23.895
So the, uh, the, the A 10 pilot says, Hey,

729
00:33:23.895 --> 00:33:26.295

we've got this new tactic, uh, that we want to test out.

730
00:33:26.955 --> 00:33:31.365
And, and the young engineer, um, you know,

731
00:33:31.475 --> 00:33:34.165
just a young captain, you know, stands up to the, uh,

732
00:33:34.185 --> 00:33:37.445
you know, the major, um, weapons school, you know,

733
00:33:37.645 --> 00:33:38.685
a 10 driver and,

734
00:33:38.705 --> 00:33:40.045
and says, well, you know, have you,

735
00:33:40.315 --> 00:33:41.885
have you done a time safety margin?

736
00:33:41.905 --> 00:33:44.085
You know, he, what? He recognizes that, Hey, wait a second.

737
00:33:44.085 --> 00:33:45.965
This is, this is something I don't know about.

738
00:33:46.045 --> 00:33:47.525
I don't know about this. Um,

739
00:33:47.755 --> 00:33:50.005
have you done the time safety margin analysis

740
00:33:50.625 --> 00:33:51.765
and the, uh, the A 10?

741
00:33:52.005 --> 00:33:53.645
I was like, what? What's that? Um,

742
00:33:55.095 --> 00:33:57.035
and, you know, so the FT tries to explain,

743
00:33:57.055 --> 00:33:58.515
and he is like, nah, we don't need to do that.

744
00:33:58.735 --> 00:34:00.635
And so then the ft, you know, he's like, well,

745
00:34:00.855 --> 00:34:02.195
is is the tactic you wanna try?

746
00:34:02.195 --> 00:34:04.395
Is it in three dash one? And they attend pilot?

747
00:34:04.495 --> 00:34:06.275
And he was like, are you kidding me?

748
00:34:06.275 --> 00:34:07.435
We write three dash one.

749
00:34:07.575 --> 00:34:09.315
If this works, we're gonna put it in three dash one.

750
00:34:09.855 --> 00:34:11.855
We don't need. So they went back and forth.

751
00:34:11.875 --> 00:34:13.575
The FTE stood his ground, uh,

752
00:34:13.575 --> 00:34:16.175
because he recognized that there was reducible ignorance,

753
00:34:16.175 --> 00:34:17.295
there's something that we could do.

754
00:34:17.355 --> 00:34:19.375
We could do the time safety margin analysis.

755
00:34:20.515 --> 00:34:21.695
Uh, the squadron commander

756
00:34:21.695 --> 00:34:22.815

says, Hey, we're not gonna fly that.

757
00:34:22.825 --> 00:34:24.615
We're not gonna fly that mission until we do it.

758
00:34:24.955 --> 00:34:26.495
Uh, which turned out to be the right call,

759
00:34:26.495 --> 00:34:28.975
because when they did the time safety margin analysis,

760
00:34:28.975 --> 00:34:31.415
it turned out that there was a negative time safety margin

761
00:34:31.995 --> 00:34:34.135
for the maneuver that the a 10 pilot wanted to fly.

762
00:34:34.835 --> 00:34:37.415
Now, does that actually mean that the A 10 would've crashed?

763
00:34:37.735 --> 00:34:39.495
Probably not because the pilot, uh,

764
00:34:39.495 --> 00:34:40.575
when he got in the airplane

765
00:34:40.675 --> 00:34:41.775
and he got the ground rush,

766
00:34:41.835 --> 00:34:42.695
he probably would've done

767
00:34:42.695 --> 00:34:43.895
something, he would've terminated the maneuver.

768
00:34:44.275 --> 00:34:45.815
Uh, but the point remains is that

769
00:34:46.235 --> 00:34:48.455
by consciously thinking about risk awareness

770
00:34:48.515 --> 00:34:50.615
and identifying, well, where are the things

771
00:34:50.615 --> 00:34:54.215
that we don't know, and is it possible to know more about

772
00:34:54.215 --> 00:34:55.975
that thing before we go and do this test?

773
00:34:56.155 --> 00:34:58.415
That's the concept of reducing reducible ignorance.

774
00:34:58.875 --> 00:35:00.535
We have a responsibility to do that.

775
00:35:01.235 --> 00:35:04.335
And, and maybe just maybe in this ca case, we actually

776
00:35:04.925 --> 00:35:08.455
avoided a mishap very similar to, uh, some of the other ones

777
00:35:08.455 --> 00:35:11.055
that we've seen in ot, um, since then.

778
00:35:12.345 --> 00:35:15.285
Uh, this is a, um, an example.

779
00:35:15.545 --> 00:35:18.405
Uh, another preceptive risk awareness is that we want

780
00:35:18.405 --> 00:35:22.065
to compare what we think should be happening with

781
00:35:22.065 --> 00:35:23.625
what is actually happening in the real world.

782
00:35:24.315 --> 00:35:27.455
Um, so the, uh, the four 11 flight test squadron out

783
00:35:27.455 --> 00:35:32.055

to Edwards, the F 22, uh, test squadron, uh, they have a,

784
00:35:33.065 --> 00:35:36.995
there's a mathematical model, um, uh, of the, uh, of the,

785
00:35:37.125 --> 00:35:40.085
of the flight dynamics, um, the same model

786
00:35:40.085 --> 00:35:41.445
that's run to the flight simulator.

787
00:35:41.905 --> 00:35:43.645
And of course you've got realtime tm.

788
00:35:43.705 --> 00:35:47.925
So what they have now is realtime simulation,

789
00:35:48.705 --> 00:35:51.005
um, of, of the model.

790
00:35:51.065 --> 00:35:55.485
And you can compare overlay what the aircraft is doing with

791
00:35:55.725 --> 00:35:59.565
what the, what the model says should be happening.

792
00:35:59.945 --> 00:36:01.845
And by comparing these two results,

793
00:36:01.985 --> 00:36:03.045
and by seeing a real time,

794
00:36:03.305 --> 00:36:05.685
you can immediately get feedback on, well,

795
00:36:05.685 --> 00:36:06.845
where is our model accurate?

796
00:36:06.845 --> 00:36:08.085
Or where is our model inaccurate?

797
00:36:08.105 --> 00:36:09.565
And this has done two things. You know, one,

798
00:36:09.565 --> 00:36:11.845
it's enhanced safety, again, because of risk awareness.

799
00:36:11.965 --> 00:36:13.925
'cause it, it's, it's a warning sign of when, well,

800
00:36:13.925 --> 00:36:16.045
wait a second, the airplane's not doing, you know,

801
00:36:16.045 --> 00:36:17.645
the airplane's real, um,

802
00:36:18.225 --> 00:36:20.765
but the airplane's not doing what we thought it was going

803
00:36:20.765 --> 00:36:22.885
to do based on the modeling that we did ahead of time.

804
00:36:23.505 --> 00:36:24.965
And it's also actually increased

805
00:36:24.965 --> 00:36:26.165
their efficiency and throughput.

806
00:36:26.365 --> 00:36:28.245
'cause now for flying science missions,

807
00:36:28.245 --> 00:36:31.045
they can move much more quickly, uh, through this.

808
00:36:32.455 --> 00:36:34.835
So let's, let's put it all together now and, and,

809
00:36:34.835 --> 00:36:37.275
and talk about how STPA fits into this, uh,

810
00:36:37.275 --> 00:36:38.355

which is the theme of, uh,

811
00:36:38.355 --> 00:36:39.835
of this flight test safety workshop.

812
00:36:40.255 --> 00:36:44.435
Um, and, and John in his, uh, discussion with Ben, uh, kind

813
00:36:44.435 --> 00:36:46.075
of hit upon that a little bit.

814
00:36:47.015 --> 00:36:50.035
Um, that this is another tool in the toolbox.

815
00:36:50.175 --> 00:36:54.675
And, and there's two primary mechanisms, two great benefits

816
00:36:54.675 --> 00:36:56.675
that I see for test teams with STPA.

817
00:36:57.135 --> 00:37:00.195
Uh, the first is, is the mere fact

818
00:37:00.375 --> 00:37:02.075
of having a functional control diagram.

819
00:37:02.815 --> 00:37:05.955
Uh, there have been multiple times when you get people all

820
00:37:05.955 --> 00:37:07.395
sitting around the table and start

821
00:37:07.395 --> 00:37:10.355
to sketch out the functional control diagram for a system

822
00:37:10.765 --> 00:37:11.955
where, you know, someone will

823
00:37:11.955 --> 00:37:13.075
say, well, that's not how that works.

824
00:37:13.145 --> 00:37:14.275
It's supposed to work this way. And

825
00:37:14.395 --> 00:37:15.555
somebody's like, no, that's not how it works.

826
00:37:15.895 --> 00:37:18.995
So immediately you start just by having to go

827
00:37:18.995 --> 00:37:20.355
through and model it.

828
00:37:20.775 --> 00:37:24.595
You immediately identify where different understandings of

829
00:37:24.595 --> 00:37:26.395
what the system is doing is supposed to do.

830
00:37:27.015 --> 00:37:31.115
Um, that is, uh, you know, one component of starting

831
00:37:31.135 --> 00:37:32.475
to shine the light on

832
00:37:32.645 --> 00:37:34.555
where are we ignorant about the system.

833
00:37:35.455 --> 00:37:37.115
Uh, the second, and,

834
00:37:37.135 --> 00:37:39.995
and probably even more important, uh, I, I mean,

835
00:37:39.995 --> 00:37:41.795
the functional control dynamic is incredibly useful.

836
00:37:42.135 --> 00:37:43.755
Uh, hopefully we get that right.

837
00:37:44.215 --> 00:37:48.115

Um, but the second one is that STPA gives you a methodical,

838
00:37:48.485 --> 00:37:50.675
systematic way of thinking through

839
00:37:51.335 --> 00:37:52.875
and developing loss scenarios.

840
00:37:52.875 --> 00:37:54.035
And I've got a couple examples,

841
00:37:54.135 --> 00:37:55.275
uh, that I'll show you for that.

842
00:37:55.575 --> 00:37:59.435
Uh, I do want to quickly though walk through, uh, two kind

843
00:37:59.435 --> 00:38:03.315
of cautionary notes, uh, with regard to STPA and, and,

844
00:38:03.315 --> 00:38:04.995
and John kind of hit on these a little bit.

845
00:38:06.025 --> 00:38:10.635
Um, and, and the first is I is, uh,

846
00:38:10.865 --> 00:38:13.275
it's not really an inherent issue of STPA, uh,

847
00:38:13.335 --> 00:38:17.475
but it's a, it's, it's a problem with complex systems, which

848
00:38:17.735 --> 00:38:19.715
of course we are dealing with in the 21st century.

849
00:38:20.295 --> 00:38:22.515
Uh, and this, uh, the cursive complexity is a very,

850
00:38:22.515 --> 00:38:24.555
very easy trap to fall into.

851
00:38:25.215 --> 00:38:29.275
And, and STPA might give you a false sense of security, um,

852
00:38:30.015 --> 00:38:32.555
if you are not careful and not deliberate.

853
00:38:32.555 --> 00:38:36.165
So, uh, it goes back to Air France 4 47 7 from, uh, 2009.

854
00:38:36.195 --> 00:38:40.085
This was the, uh, the Airbus, uh, three 30 that, uh,

855
00:38:40.105 --> 00:38:41.445
was en route from Rio to Paris

856
00:38:42.185 --> 00:38:44.045
and flew into some, uh,

857
00:38:44.045 --> 00:38:45.805
some weather autopilot got kicked out.

858
00:38:45.875 --> 00:38:47.645
Copilot, who's flying, uh,

859
00:38:47.735 --> 00:38:49.285
mishandles the aircraft in the attempt

860
00:38:49.285 --> 00:38:50.845
to roll the wings level, uh,

861
00:38:50.845 --> 00:38:52.125
gets the nose up a little bit high.

862
00:38:53.105 --> 00:38:56.685
Um, they then get the, uh, uh,

863
00:38:56.785 --> 00:38:58.285
the aircraft starts descending.

864
00:38:58.585 --> 00:39:00.485

Uh, so he pulls back on the stick more.

865
00:39:00.945 --> 00:39:04.045
Uh, it, long story short, uh, after about two

866
00:39:04.045 --> 00:39:06.365
and a half minutes of having the aircraft in a deep stall,

867
00:39:06.745 --> 00:39:08.205
it flies in the ocean a perfectly

868
00:39:09.525 --> 00:39:12.775
operating airplane engines operating fully well.

869
00:39:12.935 --> 00:39:15.175
But it hits the ocean, uh, at a very,

870
00:39:15.175 --> 00:39:17.295
very steep flight path angle, uh, at close

871
00:39:17.295 --> 00:39:18.895
to 50 degrees angle of attack.

872
00:39:19.355 --> 00:39:21.815
Uh, all because the copilot was, was

873
00:39:22.335 --> 00:39:24.735
applying tic brushing you once, once they got into descent,

874
00:39:24.835 --> 00:39:26.975
he was trying to, uh, um, you know,

875
00:39:26.975 --> 00:39:28.495
bring the nose up to stop the descent.

876
00:39:30.395 --> 00:39:33.015
It would be tempting as an engineer

877
00:39:33.195 --> 00:39:36.785
to look at a system like this and say, huh, you know what?

878
00:39:36.805 --> 00:39:39.585
We could design a system so that the pilot can't do that.

879
00:39:40.375 --> 00:39:43.635
Uh, wouldn't it be great if we had a system

880
00:39:43.705 --> 00:39:46.435
that if the pilot got the nose up too high, uh,

881
00:39:46.575 --> 00:39:47.755
and we got into a deep stall,

882
00:39:47.755 --> 00:39:50.715
that the aircraft automatically pushed the nose down?

883
00:39:52.115 --> 00:39:55.975
Um, and so tomorrow we actually have an STPA analysis

884
00:39:56.595 --> 00:39:57.735
of, uh, MAS.

885
00:39:57.735 --> 00:40:00.855
Uh, I don't want to imply by any means that STPA was, uh,

886
00:40:01.275 --> 00:40:02.615
was, was the problem with MCAS,

887
00:40:02.615 --> 00:40:06.225
but merely to highlight the fact that it,

888
00:40:06.405 --> 00:40:10.545
as you add more and more things to systems, uh, more

889
00:40:10.665 --> 00:40:13.985
and more controllers, uh, you have increased the complexity

890
00:40:13.985 --> 00:40:14.985
of the system, uh,

891
00:40:15.005 --> 00:40:17.985

and you make the system more difficult to understand.

892
00:40:18.125 --> 00:40:21.265
So, so it is a risk, uh, to be cognizant of.

893
00:40:22.455 --> 00:40:25.435
Uh, the other cautionary note is, is, is closer to the, uh,

894
00:40:25.435 --> 00:40:27.875
the, the fact, uh, of what we do in flight test.

895
00:40:28.455 --> 00:40:30.155
Uh, so, uh,

896
00:40:30.215 --> 00:40:34.715
and that's SDP is, is built around this, uh, this, this,

897
00:40:34.865 --> 00:40:36.555
this concept of, you know, we're going

898
00:40:36.615 --> 00:40:37.635
to control the system.

899
00:40:37.815 --> 00:40:39.675
We have a control process, we have this model.

900
00:40:40.415 --> 00:40:42.875
It is deeply, deeply dependent on this model.

901
00:40:43.295 --> 00:40:44.795
And what we're doing in flight test

902
00:40:45.495 --> 00:40:47.035
is we're actually building this model.

903
00:40:47.135 --> 00:40:51.955
So we don't really know what the system is, is, is doing.

904
00:40:52.215 --> 00:40:54.755
Uh, and that's what we're doing in flight test,

905
00:40:54.775 --> 00:40:56.395
is we're actually characterizing this model.

906
00:40:56.495 --> 00:40:58.715
We are building this model in flight test.

907
00:40:58.815 --> 00:41:01.755
So uncertainty about this system makes it difficult.

908
00:41:01.755 --> 00:41:03.755
If you don't actually know what the system's supposed to do,

909
00:41:03.755 --> 00:41:05.155
it's very difficult to control it.

910
00:41:06.015 --> 00:41:08.355
Uh, so if, you know, if you're about

911
00:41:08.695 --> 00:41:11.915
to have the biggest airplane that's ever flown by wingspan,

912
00:41:11.915 --> 00:41:15.595
take off, um, how certain are you that

913
00:41:16.185 --> 00:41:18.915
what we historically know about aircraft, uh, and,

914
00:41:19.055 --> 00:41:20.795
and how things scale, rentals, numbers,

915
00:41:20.855 --> 00:41:22.115
and flight dynamics, um,

916
00:41:22.295 --> 00:41:24.435
how certain are we about that for the system?

917
00:41:24.495 --> 00:41:27.235
So, just a another cautionary note, as you apply

918
00:41:27.235 --> 00:41:30.395

or as you seek to apply, SDPA, uh, is recognize that

919
00:41:31.725 --> 00:41:33.725
we are building that model.

920
00:41:34.065 --> 00:41:37.085
Uh, and so model uncertainty, you still need.

921
00:41:37.845 --> 00:41:41.225
So where it comes into its own though, is the,

922
00:41:41.245 --> 00:41:43.425
and the real utility for the test team is

923
00:41:43.425 --> 00:41:44.465
in the scenario planning.

924
00:41:44.525 --> 00:41:47.105
So part of what we do in, in, in risk management

925
00:41:47.105 --> 00:41:50.985
and safety planning is try to develop those scenarios, uh,

926
00:41:50.985 --> 00:41:52.345
that will lead to losses.

927
00:41:52.885 --> 00:41:55.185
And STPA once you have that functional control diagram,

928
00:41:55.595 --> 00:41:57.905
gives you a very methodical way

929
00:41:57.905 --> 00:41:59.105
of stepping through the system.

930
00:41:59.965 --> 00:42:04.905
In theory, every single possible scenario that could lead

931
00:42:04.905 --> 00:42:07.105
to a loss is embedded in here.

932
00:42:08.175 --> 00:42:09.715
Now, it doesn't do your thinking for you,

933
00:42:09.775 --> 00:42:11.115
you still have to think.

934
00:42:11.895 --> 00:42:15.555
Um, but their framework is here and the tool is here.

935
00:42:16.335 --> 00:42:19.275
And the example that really highlights this is the one

936
00:42:19.275 --> 00:42:21.275
that made me a believer in STPA.

937
00:42:22.595 --> 00:42:24.935
Uh, so when I was first starting to try

938
00:42:24.935 --> 00:42:29.535
to under understand STPA, um, not unlike, uh,

939
00:42:29.535 --> 00:42:30.735
the homework assignment that,

940
00:42:30.735 --> 00:42:32.055
that you've been given to do tonight.

941
00:42:32.055 --> 00:42:33.575
And, and I certainly encourage you to do

942
00:42:33.575 --> 00:42:34.815
that just like I do with all my students.

943
00:42:35.655 --> 00:42:37.955
Uh, you get far more outta the course if you do the

944
00:42:38.075 --> 00:42:39.115
homework, uh,

945
00:42:39.255 --> 00:42:40.435

and come back with questions about

946
00:42:40.455 --> 00:42:41.515
the things you didn't understand.

947
00:42:42.055 --> 00:42:44.795
Uh, so I did a very similar homework assignment, uh,

948
00:42:44.895 --> 00:42:47.035
and I applied it to the Spaceship two mishap, uh,

949
00:42:47.035 --> 00:42:48.635
from October of 2014.

950
00:42:49.665 --> 00:42:53.355
Um, and this is the one that that made, that convinced me

951
00:42:53.355 --> 00:42:55.275
of the utility in scenario planning.

952
00:42:55.455 --> 00:42:58.875
So, uh, I, I think most people are probably familiar with,

953
00:42:58.895 --> 00:43:00.035
uh, with what happened here.

954
00:43:00.575 --> 00:43:02.595
Um, I, I don't wanna discredit, uh,

955
00:43:03.105 --> 00:43:04.395
Mike Alsbury many alsbury.

956
00:43:04.895 --> 00:43:07.915
Uh, I, I count him as a, as a, as a friend.

957
00:43:08.495 --> 00:43:11.155
Um, in fact, uh, his, his patch is still right here.

958
00:43:11.815 --> 00:43:13.365
Um, uh,

959
00:43:13.625 --> 00:43:17.605
but the, uh, the, the, the, the immediate cause, uh,

960
00:43:17.665 --> 00:43:19.565
the precipitate cause of the mishap was, uh,

961
00:43:19.565 --> 00:43:22.405
when he early unlocked, uh, the, uh, the feather locks.

962
00:43:22.585 --> 00:43:27.365
Um, so trans sonically, uh, because of the scarf nozzle, uh,

963
00:43:27.425 --> 00:43:31.085
and because the, uh, uh, the, the lift hasn't shifted aft,

964
00:43:31.085 --> 00:43:32.125
uh, once you're supersonic

965
00:43:32.125 --> 00:43:34.805
and the center of lift, the center of pressure moves aft uh,

966
00:43:34.825 --> 00:43:38.045
so there's an, there's an upload on the vertical tail, um,

967
00:43:38.385 --> 00:43:40.965
that's much larger than the actuators.

968
00:43:41.065 --> 00:43:44.405
The feather actuators can, uh, uh, can resist.

969
00:43:44.465 --> 00:43:46.805
So for that reason, there are some locks.

970
00:43:46.905 --> 00:43:48.805
Uh, there's, there's some feather locks here on the leading

971
00:43:48.805 --> 00:43:50.045
edge of the tail boom.

972
00:43:51.665 --> 00:43:53.965

If you walk through an STPA analysis

973
00:43:54.265 --> 00:43:56.525
of just the feather unlocked feature,

974
00:43:58.265 --> 00:44:00.045
it highlights exactly X.

975
00:44:00.045 --> 00:44:02.805
And of course, there's always hindsight bias

976
00:44:02.865 --> 00:44:06.365
and risk of, uh, of, of the 2020 clarity looking back.

977
00:44:06.905 --> 00:44:09.285
Um, but this is particularly telling for me.

978
00:44:09.425 --> 00:44:13.405
So, so in the process model in in mini's head, uh, he had,

979
00:44:13.425 --> 00:44:14.685
he had three things that he had to do.

980
00:44:14.985 --> 00:44:16.605
Uh, this is a very dynamic situation.

981
00:44:16.605 --> 00:44:18.485
They like the motor, he confirms motor lawn light.

982
00:44:18.785 --> 00:44:22.605
Uh, he calls out 0.8 mock in order to alert, uh, Pete, uh,

983
00:44:22.605 --> 00:44:25.125
Seabold, who's flying that, Hey, we're about to in,

984
00:44:25.145 --> 00:44:26.325
you know, enter the transonic

985
00:44:26.345 --> 00:44:27.205
and there's gonna be some trend

986
00:44:27.205 --> 00:44:28.325
changes to the transonic region.

987
00:44:28.325 --> 00:44:29.525
There's gonna be some transonic buffer.

988
00:44:30.105 --> 00:44:33.885
Uh, then at 1.4 mock, uh, is when Minnie is supposed to, uh,

989
00:44:33.945 --> 00:44:37.485
to unlock, uh, the feathers, uh, at 1.5 mock.

990
00:44:37.825 --> 00:44:39.605
If they are not unlocked yet, there's going

991
00:44:39.605 --> 00:44:40.805
to be a warning light that comes on

992
00:44:40.805 --> 00:44:42.405
because you have to abort the burn.

993
00:44:42.905 --> 00:44:44.805
Uh, so this is on powered flight four.

994
00:44:45.225 --> 00:44:47.645
Uh, the other things that Minnie might be a mini's mine,

995
00:44:47.645 --> 00:44:49.645
you know, we're, we can only guess here is

996
00:44:49.645 --> 00:44:52.025
that on powered flight two and three, um,

997
00:44:52.245 --> 00:44:54.825
we had unlocked the feathers at 1.2 and 1.3.

998
00:44:55.325 --> 00:44:57.625
Uh, so if we go through all the control actions here,

999
00:44:57.925 --> 00:44:59.345

and then look at what are the safe

1000
00:44:59.405 --> 00:45:01.545
and the unsafe control actions, uh,

1001
00:45:01.765 --> 00:45:04.945
and how does providing the feather unlock, uh,

1002
00:45:04.955 --> 00:45:07.385
cause a hazard if you apply it to early,

1003
00:45:07.445 --> 00:45:10.105
if you apply it too late, uh, if you don't provide it,

1004
00:45:10.845 --> 00:45:15.765
and the one where providing it causes a hazard, uh, so,

1005
00:45:15.865 --> 00:45:18.445
you know, if you, if you unlock early

1006
00:45:18.445 --> 00:45:21.365
through the transonic region, the, the up, uh,

1007
00:45:21.505 --> 00:45:23.645
the tail up arrow loads are gonna overcome the actuator

1008
00:45:23.845 --> 00:45:27.185
resistance, uh, which is gonna result in a, um, you know,

1009
00:45:27.185 --> 00:45:28.985
catastrophic breakup, which is exactly what happened.

1010
00:45:29.455 --> 00:45:31.185
This quote down here in the bottom right hand

1011
00:45:31.185 --> 00:45:34.025
and corner is, is gym ties.

1012
00:45:34.365 --> 00:45:37.425
Uh, one of the most brilliant Aaron ACO engineers, uh,

1013
00:45:37.425 --> 00:45:41.625
that I have, uh, I've ever met, uh, testimony to the NTSB,

1014
00:45:41.645 --> 00:45:42.865
uh, is that early unlocking

1015
00:45:42.865 --> 00:45:45.465
of the feather system was not considered as a what if, uh,

1016
00:45:45.625 --> 00:45:47.105
they, they just hadn't thought about that.

1017
00:45:47.105 --> 00:45:49.825
There was no warning in the pilot operating handbook, uh,

1018
00:45:49.835 --> 00:45:51.465
about unlocking the feathers early.

1019
00:45:52.165 --> 00:45:55.345
Um, if the test team,

1020
00:45:55.445 --> 00:45:57.265
and again, if you know, hindsight bias,

1021
00:45:57.325 --> 00:45:59.345
but if they had walked through, uh,

1022
00:45:59.345 --> 00:46:03.385
this feather unlock scenario, um, it,

1023
00:46:03.605 --> 00:46:04.825
it, it, at least it's there.

1024
00:46:04.925 --> 00:46:06.105
The framework is there

1025
00:46:06.105 --> 00:46:07.985
to actually consider all the different

1026
00:46:08.505 --> 00:46:11.665

possible actu actuations that could lead to an unsafe act.

1027
00:46:11.805 --> 00:46:13.145
And that might've said, you know,

1028
00:46:13.185 --> 00:46:15.225
might've highlighted the fact like, Hey, by the way,

1029
00:46:15.715 --> 00:46:18.065
don't unlock feathers, uh, one around the transonic region

1030
00:46:18.065 --> 00:46:19.065
because the arrow loads are higher.

1031
00:46:19.285 --> 00:46:21.585
Uh, the air, the aeronautics folks knew that,

1032
00:46:21.645 --> 00:46:25.265
but clearly the pilots, uh, were not aware of that risk.

1033
00:46:27.475 --> 00:46:28.855
So one of the first things we have

1034
00:46:28.855 --> 00:46:30.935
to do in developing risk awareness is identify

1035
00:46:30.935 --> 00:46:32.175
and characterize what is unknown.

1036
00:46:32.175 --> 00:46:33.615
That's what we've been talking about. Uh,

1037
00:46:33.635 --> 00:46:35.535
and there's this whole spectrum of uncertainty,

1038
00:46:36.075 --> 00:46:37.775
and we've got this cloud of ignorance.

1039
00:46:37.955 --> 00:46:39.695
And what we're doing as part

1040
00:46:39.695 --> 00:46:42.135
of our test planning is we are reducing

1041
00:46:42.165 --> 00:46:43.415
that reduceable ignorance.

1042
00:46:44.355 --> 00:46:45.495
Um, and,

1043
00:46:45.495 --> 00:46:47.575
and this is where I think the, uh, the,

1044
00:46:47.575 --> 00:46:50.935
the 2D risk matrix really kind of, uh, does us a disservice.

1045
00:46:51.375 --> 00:46:54.895
'cause we've probably all been there, we've abused it.

1046
00:46:54.955 --> 00:46:56.295
We, we know we don't wanna,

1047
00:46:56.795 --> 00:46:58.095
you know, you know, we manipulate it.

1048
00:46:58.175 --> 00:47:00.535
'cause like, well, you know, if we play with the likelihood

1049
00:47:00.535 --> 00:47:02.695
of occurrence or, you know, that's unlikely,

1050
00:47:02.965 --> 00:47:04.655
even though it's gonna be a catastrophic loss.

1051
00:47:04.795 --> 00:47:06.735
So it's medium risk, um,

1052
00:47:06.735 --> 00:47:08.695
because we know the answer that we wanna get to.

1053
00:47:09.115 --> 00:47:13.255

Uh, so in communicating to the risk authorities,

1054
00:47:14.615 --> 00:47:17.505
it's not a very effective way for communicating risk,

1055
00:47:17.725 --> 00:47:20.505
nor is it helpful as we're in the testing for,

1056
00:47:20.525 --> 00:47:22.705
for shaping our analysis.

1057
00:47:23.205 --> 00:47:24.385
So the safety planning

1058
00:47:24.385 --> 00:47:26.985
and the safety review process should really be looking at

1059
00:47:27.045 --> 00:47:30.005
and, and characterizing what don't we know about the system?

1060
00:47:31.095 --> 00:47:33.025
What tests didn't we do?

1061
00:47:33.165 --> 00:47:35.425
We did CFD, but we didn't do wind tunnel,

1062
00:47:35.565 --> 00:47:38.025
or we, we, we did media speed taxi,

1063
00:47:38.325 --> 00:47:40.105
but we didn't do the medium high speed taxi.

1064
00:47:40.685 --> 00:47:42.545
Um, where are the gaps in the knowledge?

1065
00:47:42.565 --> 00:47:44.905
You know, where have we been surprised by the model so far?

1066
00:47:45.325 --> 00:47:48.065
You know, the wind tunnel said that this should happen,

1067
00:47:48.245 --> 00:47:50.105
or CFD said that this should happen,

1068
00:47:50.685 --> 00:47:52.745
but when we did the rotation test

1069
00:47:52.765 --> 00:47:55.865
or the control authority test, we were off by 10 knots.

1070
00:47:55.975 --> 00:47:57.145
Well, can't we explain that?

1071
00:47:57.245 --> 00:47:58.945
So where are the model surprises been so far?

1072
00:47:59.555 --> 00:48:01.305
Let's put, you know, for the things that we think

1073
00:48:01.305 --> 00:48:02.385
that we know about the system,

1074
00:48:02.965 --> 00:48:05.305
can you characterize the confidence intervals on that?

1075
00:48:05.885 --> 00:48:08.025
Um, the test that we're about to do?

1076
00:48:08.025 --> 00:48:09.705
What does that test inform?

1077
00:48:10.325 --> 00:48:11.985
And then equally important, again,

1078
00:48:11.985 --> 00:48:14.265
from the drift standpoint is do we have

1079
00:48:14.545 --> 00:48:15.585
sufficient schedule to learn?

1080
00:48:15.965 --> 00:48:18.065

And this is one of the things that it's really helpful

1081
00:48:18.165 --> 00:48:20.465
for testers in communicating with program managers

1082
00:48:20.465 --> 00:48:22.945
where a lot of that pressure for drift comes from is,

1083
00:48:23.885 --> 00:48:24.905
is not pushing us.

1084
00:48:25.005 --> 00:48:27.745
So, so let's put it all together in a,

1085
00:48:27.765 --> 00:48:29.025
in a real quick example.

1086
00:48:29.965 --> 00:48:33.225
Uh, so let's say that you're about to do, um, some V two,

1087
00:48:33.405 --> 00:48:36.185
uh, testing, uh, for a new new design.

1088
00:48:36.685 --> 00:48:38.905
Uh, and so you start to characterize, you go

1089
00:48:38.905 --> 00:48:40.225
through the process of characterizing what we know.

1090
00:48:40.225 --> 00:48:42.865
Well, we know that our, our V two needs to be a minimum

1091
00:48:43.085 --> 00:48:47.425
of 13%, uh, over, uh, over the, uh, stall reference speed,

1092
00:48:47.765 --> 00:48:49.025
uh, stall reference speed.

1093
00:48:49.485 --> 00:48:51.505
Do we know that? Yeah, we've, we've done some flight tests.

1094
00:48:51.525 --> 00:48:53.185
We did flight tests at 15,000 feet

1095
00:48:53.445 --> 00:48:54.945
as billed down to 10,000 feet.

1096
00:48:54.945 --> 00:48:57.665
We've got, uh, we've got seal max data from, um,

1097
00:48:57.895 --> 00:49:00.785
from 15,000 feet and 10,000 feet.

1098
00:49:00.805 --> 00:49:01.905
We can adjust the pressure.

1099
00:49:02.025 --> 00:49:04.265
We know that, uh, let's see weight. Do we know the weight?

1100
00:49:04.335 --> 00:49:06.025
Yeah, we can, we can measure the weight.

1101
00:49:06.285 --> 00:49:08.025
Uh, we know weight to within 2%.

1102
00:49:08.525 --> 00:49:09.945
Uh, we know density on the test.

1103
00:49:10.025 --> 00:49:11.705
A, we know c max from the stall testing.

1104
00:49:12.545 --> 00:49:15.275
Alright, so what is different about 10,000 feet

1105
00:49:15.275 --> 00:49:17.755
and what we're about to do, uh, in our V two testing here.

1106
00:49:18.415 --> 00:49:19.995
Uh, okay, so we're close to the ground.

1107
00:49:19.995 --> 00:49:23.635

Does that have a difference? Uh, well, yeah, maybe it does.

1108
00:49:23.635 --> 00:49:25.595
There's this, uh, ground effect thing, uh,

1109
00:49:25.695 --> 00:49:28.275
and the fact that, uh, our wing, uh,

1110
00:49:28.295 --> 00:49:30.955
our finite wing looks a lot more like an infinite

1111
00:49:30.955 --> 00:49:32.115
wing when we're in ground effect.

1112
00:49:32.415 --> 00:49:34.115
Um, what effect does that have?

1113
00:49:34.115 --> 00:49:35.355
Well, that's gonna reduce our drag.

1114
00:49:35.615 --> 00:49:37.155
Uh, so that means we're gonna get a little bit more thrust.

1115
00:49:37.155 --> 00:49:39.675
We actually didn't show the, uh, the thrust effect up here,

1116
00:49:39.735 --> 00:49:41.435
but as we rotate to a pitch angle,

1117
00:49:41.435 --> 00:49:42.875
there's gonna be a component of the thrust vector

1118
00:49:42.875 --> 00:49:44.835
that's going to decrease our weight, uh,

1119
00:49:44.835 --> 00:49:46.315
which is gonna help us with stall speed.

1120
00:49:46.895 --> 00:49:50.075
Uh, what else does that do? Well, that, wait a second.

1121
00:49:50.105 --> 00:49:52.515
That that also changes the lift curve slope.

1122
00:49:53.095 --> 00:49:54.995
Uh, we have,

1123
00:49:54.995 --> 00:49:56.995
because our wing acts more like an infinite wing.

1124
00:49:57.455 --> 00:50:00.235
Uh, we have a steeper lift curve slope.

1125
00:50:00.775 --> 00:50:02.715
So now our CL max

1126
00:50:03.535 --> 00:50:06.155
is gonna occur at a lower angle of attack.

1127
00:50:06.745 --> 00:50:09.395
Well, that's, that's interesting.

1128
00:50:09.615 --> 00:50:12.995
So now we start to question our assumptions.

1129
00:50:13.535 --> 00:50:16.635
Is CL max the same that it is,

1130
00:50:17.375 --> 00:50:18.835
uh, in ground effect?

1131
00:50:18.855 --> 00:50:21.195
So in this diagram we've shown right here is we're

1132
00:50:21.195 --> 00:50:22.275
predicting a new angle attack,

1133
00:50:22.275 --> 00:50:23.715
which we can now use to set a pitch angle.

1134
00:50:24.475 --> 00:50:27.585

Is our seal max the same in ground effect effect?

1135
00:50:27.585 --> 00:50:29.265
Well, I don't know. Is that a good assumption or not?

1136
00:50:29.475 --> 00:50:31.785
Could we do some analysis? Could we do some CFD?

1137
00:50:31.815 --> 00:50:34.745
Yeah, actually, that's a pretty easy CFD problem to do.

1138
00:50:35.245 --> 00:50:40.165
So if you go through this, uh, you quickly start

1139
00:50:40.225 --> 00:50:41.445
to, uh, to realize

1140
00:50:41.985 --> 00:50:44.165
and characterize what you know and what you don't know.

1141
00:50:44.985 --> 00:50:47.405
Um, and I think many

1142
00:50:47.405 --> 00:50:49.445
of you are probably familiar with this one.

1143
00:50:49.475 --> 00:50:52.685
This is a, a, again, a, a a somewhat simplified version.

1144
00:50:53.185 --> 00:50:57.495
Um, the, uh, the G six team actually knew quite a bit, um,

1145
00:50:57.835 --> 00:50:59.255
and, and actually made some corrections.

1146
00:50:59.255 --> 00:51:00.295
They just made some incorrect

1147
00:51:00.295 --> 00:51:01.535
corrections for the lift curve slope.

1148
00:51:01.995 --> 00:51:04.255
Uh, it's a fascinating TSB report to read.

1149
00:51:04.795 --> 00:51:06.015
Um, uh,

1150
00:51:06.015 --> 00:51:09.575
but there are some failures, uh, in understanding the system

1151
00:51:09.635 --> 00:51:11.015
and characterizing and, and,

1152
00:51:11.015 --> 00:51:13.785
and making assumptions, um, that going

1153
00:51:13.785 --> 00:51:16.625
through the safety planning process, uh, would clearly have.

1154
00:51:17.285 --> 00:51:22.105
Um, so, so, so some final thoughts here, um, on,

1155
00:51:22.365 --> 00:51:26.025
on how, you know, how what, and this is, this is just seed.

1156
00:51:26.045 --> 00:51:27.945
You know, we haven't really gotten to the point of

1157
00:51:27.965 --> 00:51:30.305
how can we communicate this differently than a 2D risk

1158
00:51:30.305 --> 00:51:32.425
matrix, a 2D risk risk matrix.

1159
00:51:32.725 --> 00:51:34.945
We use it in program management, we use it in flight test,

1160
00:51:35.285 --> 00:51:37.905
uh, but it doesn't really communicate to the risk authority,

1161
00:51:38.205 --> 00:51:39.985

nor does it help drive us as a test team.

1162
00:51:40.485 --> 00:51:42.785
Uh, so here are some thoughts on what we can do, you know,

1163
00:51:43.105 --> 00:51:44.425
identifying what we truly know

1164
00:51:44.765 --> 00:51:46.825
and putting confidence intervals on what we know.

1165
00:51:47.505 --> 00:51:50.285
Um, and then once we've identified what we know,

1166
00:51:50.305 --> 00:51:52.525
we can now identify what we don't know,

1167
00:51:53.145 --> 00:51:54.485
and then we can characterize, well,

1168
00:51:54.485 --> 00:51:55.725
what is the nature of that unknown?

1169
00:51:56.065 --> 00:51:57.805
Is it a random type of unknown

1170
00:51:57.865 --> 00:52:01.325
or is it a, an an ignorance type of unknown

1171
00:52:01.425 --> 00:52:03.485
and uncertainty, a knowledge type of unknown?

1172
00:52:04.115 --> 00:52:08.215
What kind of tests can we do to reduce that ignorance?

1173
00:52:08.595 --> 00:52:11.535
Um, and if not, then, uh, then, uh,

1174
00:52:12.315 --> 00:52:14.295
or, you know, let's line out all the tests

1175
00:52:14.435 --> 00:52:16.615
and then we'll make a deliberate decisions about which ones,

1176
00:52:17.115 --> 00:52:20.015
uh, we don't have the time or we don't have the money to do,

1177
00:52:20.015 --> 00:52:21.495
and let's make a deliberate decision about that.

1178
00:52:21.595 --> 00:52:23.095
But let's look at all the tests that we're,

1179
00:52:23.095 --> 00:52:25.165
that we're not going to do, um,

1180
00:52:25.385 --> 00:52:27.205
and let's identify the tests that weren't done.

1181
00:52:27.385 --> 00:52:29.325
We need to communicate that to the risk authority,

1182
00:52:29.345 --> 00:52:31.405
the risk manager, the, the person that makes the decision

1183
00:52:31.945 --> 00:52:32.965
so that they're aware of that.

1184
00:52:33.585 --> 00:52:35.085
Uh, you know, in the Gulf Stream mishap,

1185
00:52:35.085 --> 00:52:36.925
they didn't do the CFD in ground effect.

1186
00:52:37.265 --> 00:52:39.325
Um, that was, you know, that was decision.

1187
00:52:39.665 --> 00:52:41.965
Um, again, the, the risk manager said, you know what?

1188
00:52:42.015 --> 00:52:43.725

Let's, let's go ahead and do that analysis

1189
00:52:43.745 --> 00:52:47.325
before we, we go, uh, what surprises have we had so far?

1190
00:52:47.785 --> 00:52:49.125
And then what does the test inform?

1191
00:52:49.145 --> 00:52:50.645
You know, are we actually learning something

1192
00:52:50.865 --> 00:52:53.165
and do we have a sufficient schedule?

1193
00:52:53.545 --> 00:52:56.765
Uh, that was also a factor in, in the G six mishap, uh, is

1194
00:52:56.765 --> 00:52:58.125
that there just wasn't enough time

1195
00:52:58.125 --> 00:52:59.645
to analyze the data from previous tests.

1196
00:53:01.515 --> 00:53:04.295
Um, so, and, and then probably the bottom line,

1197
00:53:04.295 --> 00:53:05.855
and this is where SDPA comes in,

1198
00:53:06.195 --> 00:53:09.495
is rather than the risk matrix pushes us to this, uh,

1199
00:53:09.765 --> 00:53:11.375
probability kind of thing,

1200
00:53:11.375 --> 00:53:15.775
and I think that's the wrong, uh, the wrong mindset in risk

1201
00:53:16.295 --> 00:53:20.255
planning, uh, we should really be thinking about what is

1202
00:53:20.855 --> 00:53:22.695
possible, what could possibly happen,

1203
00:53:23.595 --> 00:53:25.765
not necessarily is it likely to happen?

1204
00:53:25.825 --> 00:53:28.525
Is it plausible or is it probable that's downstream.

1205
00:53:28.625 --> 00:53:32.725
But if there is a scenario by which something is possible,

1206
00:53:32.725 --> 00:53:33.805
something could possibly happen,

1207
00:53:34.195 --> 00:53:35.405
well, let's talk about that.

1208
00:53:35.865 --> 00:53:38.165
Uh, and that's again, where STPA gives you

1209
00:53:38.165 --> 00:53:41.565
that very deliberate, methodical way of looking at

1210
00:53:42.365 --> 00:53:44.765
functional frameworks in, in defining

1211
00:53:44.795 --> 00:53:46.445
what could possibly happen to the system.

1212
00:53:46.635 --> 00:53:50.365
That is how we slowly build risk awareness over time.

1213
00:53:50.845 --> 00:53:55.835
Ultimately, flight test is about, you know, suppressing,

1214
00:53:55.895 --> 00:53:59.675
uh, mankind's, uh, inclination towards hubris, um, and,

1215
00:53:59.675 --> 00:54:01.715

and showing that, uh, that humility and,

1216
00:54:01.715 --> 00:54:04.115
and to the extent that we can move our,

1217
00:54:04.215 --> 00:54:06.315
our flight test safety process

1218
00:54:06.455 --> 00:54:10.715
and reviews to an inquiry versus an advocacy, uh, basis.

1219
00:54:11.695 --> 00:54:13.275
Uh, I, I think we're in good shape.

1220
00:54:13.855 --> 00:54:16.955
Um, so, so, uh, is it, is it back over to Ben?

1221
00:54:17.155 --> 00:54:20.195
I, I talked two minutes more than, uh, than I was allotted.

1222
00:54:21.015 --> 00:54:22.115
That's perfect. Baker. I

1223
00:54:22.115 --> 00:54:23.515
Think it's either, uh, either Ben

1224
00:54:23.515 --> 00:54:25.995
or Tom is, uh, is, is back up here.

1225
00:54:26.355 --> 00:54:28.555
I I would've been getting the eye contact from,

1226
00:54:28.585 --> 00:54:30.715
from them, uh, in real place. Hey, Ben.

1227
00:54:31.325 --> 00:54:35.725
Hello. Oh, thank you. That's, uh, always fabulous.

1228
00:54:35.985 --> 00:54:38.245
Uh, really instructive. I love the way you put, uh,

1229
00:54:38.695 --> 00:54:42.005
complexity positioned our world within a,

1230
00:54:42.005 --> 00:54:43.165
within the complexity space,

1231
00:54:43.165 --> 00:54:44.805
and then showed us how SCPA can

1232
00:54:45.745 --> 00:54:46.925
can provide us a way through.

1233
00:54:46.945 --> 00:54:48.005
So that's, that's great.

1234
00:54:49.185 --> 00:54:52.145
You spoke about functional diagrams, uh,

1235
00:54:52.205 --> 00:54:54.105
and the, the value in sitting down as a group

1236
00:54:54.245 --> 00:54:55.985
and building a functional diagram.

1237
00:54:58.305 --> 00:55:00.765
How successful has that been in real life, uh,

1238
00:55:00.965 --> 00:55:02.685
I can almost see the eye rolling coming

1239
00:55:02.685 --> 00:55:03.685
through the question panel.

1240
00:55:04.545 --> 00:55:07.885
Uh, is there any hints on how to do that?

1241
00:55:08.305 --> 00:55:10.605
How much resources is that gonna take for us?

1242
00:55:11.645 --> 00:55:13.335

What, what can we expect in that activity?

1243
00:55:15.565 --> 00:55:17.785
The, uh, so this is actually one of the things we,

1244
00:55:17.845 --> 00:55:20.505
we are trying to, to do in the Air Force.

1245
00:55:20.725 --> 00:55:23.705
Uh, I, I, I, there, there have been some, um,

1246
00:55:24.705 --> 00:55:29.105
a couple papers at SEP symposium, uh, a couple notes in the,

1247
00:55:29.905 --> 00:55:32.585
about the experiment we did at Edwards about 18 months ago,

1248
00:55:33.125 --> 00:55:38.025
um, is, is pushing some of this,

1249
00:55:38.245 --> 00:55:40.025
uh, further upstream in the program.

1250
00:55:40.525 --> 00:55:45.155
Um, so the functional control diagrams, it would be,

1251
00:55:45.615 --> 00:55:48.035
you know, that that should be a deliverable, um,

1252
00:55:48.265 --> 00:55:50.155
from the program, uh, from the engineers.

1253
00:55:50.575 --> 00:55:52.195
Uh, and that's actually one of the, one

1254
00:55:52.195 --> 00:55:54.115
of the things we've got a tomorrow you're,

1255
00:55:54.115 --> 00:55:56.475
we're gonna hear from, uh, major Poncho summers.

1256
00:55:56.645 --> 00:55:59.355
Sarah Summers, um, who,

1257
00:55:59.575 --> 00:56:02.995
who studied SP under Nancy Levison at MIT, um,

1258
00:56:03.935 --> 00:56:08.435
was out at the, the, the, uh, uh, test, uh,

1259
00:56:08.505 --> 00:56:11.755
test center, uh, and is now a PIM up at the Pentagon.

1260
00:56:11.815 --> 00:56:15.035
And, and she is driving an effort to try to drive some

1261
00:56:15.035 --> 00:56:16.595
of this upstream to program so

1262
00:56:16.595 --> 00:56:19.035
that programs are developing functional control diagrams

1263
00:56:19.305 --> 00:56:24.045
that test teams can then use the, the level of, of,

1264
00:56:24.065 --> 00:56:27.165
of detail that the test team, you know, ultimately produces.

1265
00:56:27.505 --> 00:56:29.385
You know, to,

1266
00:56:29.485 --> 00:56:32.385
to my mind what's important is not necessarily the

1267
00:56:32.625 --> 00:56:35.225
functional control diagram, it's the intellectual energy

1268
00:56:35.225 --> 00:56:37.585
that goes into creating it or into understanding it

1269
00:56:37.965 --> 00:56:39.025

and, and discussing it.

1270
00:56:39.685 --> 00:56:41.825
So, you know, the test team sitting around there, if,

1271
00:56:41.825 --> 00:56:42.945
if the program doesn't have one

1272
00:56:42.945 --> 00:56:45.745
and the test team has to create one on their own, you know,

1273
00:56:45.745 --> 00:56:47.345
it's very illustrative when you start

1274
00:56:47.345 --> 00:56:50.305
to throw stuff up on a whiteboard or on a big tabletop

1275
00:56:50.305 --> 00:56:54.345
and tabletop this, um, it, it really starts to highlight

1276
00:56:54.915 --> 00:56:58.105
where different impressions of what the system do are, and,

1277
00:56:58.105 --> 00:56:59.545
and, and that's the real value.

1278
00:57:00.485 --> 00:57:03.035
Um, you know, it helps get

1279
00:57:03.035 --> 00:57:04.235
around some of the group think things.

1280
00:57:04.335 --> 00:57:09.025
And, and also as a, you know, now that, um, you know, I,

1281
00:57:09.365 --> 00:57:11.705
I'm a couple years removed from being the guy down in the

1282
00:57:11.745 --> 00:57:12.985
trenches, getting to do the, uh, with,

1283
00:57:12.985 --> 00:57:14.785
with the pencil, uh, getting to do the work.

1284
00:57:15.205 --> 00:57:18.395
Uh, but it gives you a sense for, Hey, wait a second.

1285
00:57:18.395 --> 00:57:21.795
There's, there's a, there's a big disparity in understanding

1286
00:57:22.365 --> 00:57:23.755
among the people here

1287
00:57:23.755 --> 00:57:25.675
that should be the experts on the system.

1288
00:57:26.025 --> 00:57:27.635
Yeah. To me, as a, as a leader,

1289
00:57:27.635 --> 00:57:29.755
that's a warning that, wait a second.

1290
00:57:29.815 --> 00:57:33.335
We, we may not understand this as, as well as we should. Um,

1291
00:57:34.775 --> 00:57:35.935
A sizable part of the,

1292
00:57:36.675 --> 00:57:38.975
the flight test community is now involved

1293
00:57:38.995 --> 00:57:40.135
in smaller startups.

1294
00:57:40.715 --> 00:57:43.895
And we, and I'm aware that they, they really don't have

1295
00:57:43.895 --> 00:57:46.655
that, that reach back to a program office

1296
00:57:46.655 --> 00:57:49.175

that's been working this for a number of years

1297
00:57:49.195 --> 00:57:50.775
and then provides them with a,

1298
00:57:51.435 --> 00:57:52.935
an executable flight test program.

1299
00:57:52.935 --> 00:57:55.415
They need to build this as they go along. Yep.

1300
00:57:56.115 --> 00:57:59.735
Do you have any, any favorite STPA

1301
00:58:01.135 --> 00:58:05.055
mindsets, any favorite STPA questions that you would use to,

1302
00:58:05.055 --> 00:58:06.935
that you would recommend as, as a go-to?

1303
00:58:07.635 --> 00:58:10.255
So if you haven't got the, the resources

1304
00:58:10.275 --> 00:58:12.815
or the, the years timeframe of a program,

1305
00:58:14.125 --> 00:58:16.495
what changed in your mindset to enable you

1306
00:58:16.495 --> 00:58:18.815
to implement STPA on more of a day-to-day

1307
00:58:19.835 --> 00:58:21.185
extra tool in your tool bag?

1308
00:58:23.865 --> 00:58:27.735
The, uh, so the real, I, you know, I,

1309
00:58:27.775 --> 00:58:29.775
I certainly understand the, uh, the, the,

1310
00:58:29.775 --> 00:58:31.295
the challenges inherent with a small team.

1311
00:58:31.555 --> 00:58:34.015
Uh, there's also some advantages with that small team.

1312
00:58:34.755 --> 00:58:39.545
Uh, it's a lot easier, um, to have a,

1313
00:58:40.525 --> 00:58:44.105
uh, a more cohesive and more unified understanding.

1314
00:58:44.125 --> 00:58:45.705
You're, you're less likely to end up

1315
00:58:45.705 --> 00:58:47.665
with stovepipe knowledge that's not

1316
00:58:48.985 --> 00:58:50.595
filtering across the organization.

1317
00:58:51.985 --> 00:58:56.365
Uh, again, that's one of the kind of the key things for, uh,

1318
00:58:56.505 --> 00:59:01.325
the managers, um, you know, to kind of keep the pulse on is,

1319
00:59:01.465 --> 00:59:03.005
you know, how well is information

1320
00:59:03.005 --> 00:59:04.165
flowing across an organization?

1321
00:59:04.505 --> 00:59:07.285
You know, are there pockets of knowledge on one side

1322
00:59:07.285 --> 00:59:08.365
that aren't known by another?

1323
00:59:08.425 --> 00:59:12.045

So, so smaller teams actually have the advantage in that,

1324
00:59:12.825 --> 00:59:17.365
um, you have much, uh, more fluid information flow that's a,

1325
00:59:17.365 --> 00:59:19.085
you know, also a, a challenge.

1326
00:59:20.575 --> 00:59:24.395
The, I, I guess the simple answer to your question, Ben, is,

1327
00:59:24.395 --> 00:59:27.875
uh, is, is do the best that you can, um, you know,

1328
00:59:27.875 --> 00:59:30.675
take a stab at it, uh, every time that you go through this,

1329
00:59:31.375 --> 00:59:33.395
uh, whether it be SDPA or whether or not,

1330
00:59:33.455 --> 00:59:36.035
or whether it's, you know, just doing a scenario planning,

1331
00:59:36.655 --> 00:59:40.685
uh, every time you go through that exercise, uh, you start

1332
00:59:40.685 --> 00:59:42.725
to uncover things, uh,

1333
00:59:42.785 --> 00:59:46.085
and discover things that were were previously unknown.

1334
00:59:46.545 --> 00:59:48.685
Um, and, and that's where the real value lies.

1335
00:59:49.225 --> 00:59:51.165
Um, you know, it's, you know,

1336
00:59:51.165 --> 00:59:53.005
what I tell my students now when they, you know, they've,

1337
00:59:53.005 --> 00:59:54.285
they've got a problem and they're like, sir,

1338
00:59:54.285 --> 00:59:55.405
I have no idea where to start with this.

1339
00:59:55.585 --> 00:59:56.845
I'm like, well, what do you know?

1340
00:59:57.185 --> 00:59:59.845
Um, you know, start writing down things that, you know, um,

1341
01:00:00.425 --> 01:00:02.605
and start building that roadmap between where you want

1342
01:00:02.605 --> 01:00:03.925
to get to and what you know right now.

1343
01:00:04.865 --> 01:00:06.485
And, and, and, you know, just,

1344
01:00:06.715 --> 01:00:08.005
just start putting the pencil on the paper.

1345
01:00:08.005 --> 01:00:10.805
Just start doing it, I guess is the, uh, is the simple, uh,

1346
01:00:10.805 --> 01:00:12.725
short answer is just do it. Um,

1347
01:00:13.035 --> 01:00:14.765
Yeah, the one I, I don't

1348
01:00:14.765 --> 01:00:15.685
Think we can, that's probably already

1349
01:00:15.685 --> 01:00:16.325
trademarked, isn't it?

1350
01:00:17.705 --> 01:00:19.165

The one I look for from, uh,

1351
01:00:19.795 --> 01:00:22.005
John Thomas' brief earlier is I look for the, the points

1352
01:00:22.005 --> 01:00:23.005
of control now,

1353
01:00:23.065 --> 01:00:25.725
and now they, they flagged me as a, as somewhere

1354
01:00:25.725 --> 01:00:26.965
to work and look for hazards.

1355
01:00:27.225 --> 01:00:28.325
That's one of the other questions.

1356
01:00:28.325 --> 01:00:29.925
That's excellent point, because those are the seams,

1357
01:00:29.925 --> 01:00:31.885
those are the interfaces, and that's, that's often

1358
01:00:31.885 --> 01:00:35.165
where you see information flow breakdown is between those,

1359
01:00:35.455 --> 01:00:36.805
those interfaces and, and,

1360
01:00:36.805 --> 01:00:39.005
and seems between organizations or between systems.

1361
01:00:39.145 --> 01:00:41.565
So that's, that's actually a, a, a very good point. Ben,

1362
01:00:42.035 --> 01:00:44.485
I've had a couple of questions come in, uh, asking

1363
01:00:44.545 --> 01:00:47.025
how this relates the, the relationship

1364
01:00:47.025 --> 01:00:49.025
between STPA and, and 2D matrix.

1365
01:00:49.765 --> 01:00:51.025
So I'll give that one to you,

1366
01:00:51.605 --> 01:00:53.625
but can I frame it with awareness

1367
01:00:53.625 --> 01:00:57.745
that I believe the USAF are now ruling out, uh, it's kind

1368
01:00:57.745 --> 01:01:01.425
of changed their 2D matrix so that everything that is, uh,

1369
01:01:01.585 --> 01:01:05.505
catastrophic is now, uh, is kind of a vertical red

1370
01:01:06.285 --> 01:01:08.745
bar on one side instead of the progression across the chart.

1371
01:01:09.445 --> 01:01:11.145
Are you able to explain the logic behind that

1372
01:01:11.485 --> 01:01:13.345
and tell us how that's been working

1373
01:01:14.165 --> 01:01:15.745
and tie that into an STPA?

1374
01:01:15.845 --> 01:01:17.705
So people are saying, how does this all,

1375
01:01:18.455 --> 01:01:20.065
I've got a 2D matrix that I have to use.

1376
01:01:20.925 --> 01:01:21.945
How can I make that better?

1377
01:01:22.205 --> 01:01:23.985

Is STPA the way I make that better?

1378
01:01:24.365 --> 01:01:25.585
Or are these two different things?

1379
01:01:27.485 --> 01:01:29.465
The, um, yeah, so this is, this is,

1380
01:01:29.465 --> 01:01:33.025
this is not the air force's, um, opinion.

1381
01:01:33.025 --> 01:01:35.225
This is beaker's opinion. Um, okay.

1382
01:01:36.685 --> 01:01:37.785
That's, That's even worse

1383
01:01:37.785 --> 01:01:38.985
than putting lipstick on a pig.

1384
01:01:39.245 --> 01:01:42.305
Um, you know, making it, uh, you know,

1385
01:01:42.755 --> 01:01:46.105
color coding catastrophic as automatically red, um,

1386
01:01:47.125 --> 01:01:49.585
is merely providing a perverse incentive to do something,

1387
01:01:49.605 --> 01:01:51.025
you know, to continue playing the games.

1388
01:01:51.725 --> 01:01:54.385
Um, okay, the, the 2D matrix is,

1389
01:01:54.465 --> 01:01:55.545
I mean, we've got it right now.

1390
01:01:55.645 --> 01:01:57.785
Uh, and until we come up, you know, until we

1391
01:01:57.785 --> 01:01:59.265
as a community come up with something better,

1392
01:01:59.845 --> 01:02:01.065
uh, it's what we're stuck with.

1393
01:02:01.525 --> 01:02:05.425
Um, and so it's, it's the, the presentation methodology.

1394
01:02:06.325 --> 01:02:10.995
So my advice to teams would be, do let

1395
01:02:10.995 --> 01:02:13.275
that be the very, very last thing you do, you know,

1396
01:02:13.335 --> 01:02:14.395
do everything else.

1397
01:02:15.135 --> 01:02:17.475
And then if the boss wants to see a 2D matrix

1398
01:02:17.495 --> 01:02:19.660
and wants to see everything plotted out in the 2D matrix,

1399
01:02:20.075 --> 01:02:22.625
take all of the work that you've done, uh,

1400
01:02:22.725 --> 01:02:24.705
and communicate it in the best way that you can,

1401
01:02:25.365 --> 01:02:29.125
and then put it on the 2D matrix, uh, at the very end.

1402
01:02:29.385 --> 01:02:32.045
Um, and until we come up with a better way

1403
01:02:32.045 --> 01:02:33.525
of communicating risk, uh,

1404
01:02:33.585 --> 01:02:35.045

and that's, that's part of what, you know,

1405
01:02:35.085 --> 01:02:36.845
I I really want everybody to start thinking about.

1406
01:02:37.585 --> 01:02:42.125
Um, we'll, actually at a I A A aviation, uh, next month, uh,

1407
01:02:42.125 --> 01:02:43.525
we're having a special session on this.

1408
01:02:43.625 --> 01:02:45.405
Tom Huff is actually, uh, participating.

1409
01:02:45.945 --> 01:02:49.045
Um, NASA has started to think along these lines as well.

1410
01:02:49.185 --> 01:02:51.645
And it's beyond just flight test, safety, uh, you know,

1411
01:02:51.845 --> 01:02:53.005
aviation and, and programs.

1412
01:02:53.025 --> 01:02:56.285
Uh, there's, there's a lot of kind of discontent with, um,

1413
01:02:57.875 --> 01:03:01.205
just how traditionally abused the, uh, the risk matrix is.

1414
01:03:01.665 --> 01:03:04.005
Um, and again, you know, there's not, there's not a better,

1415
01:03:04.185 --> 01:03:05.285
if we had something better right

1416
01:03:05.285 --> 01:03:06.365
now, we'd, we'd be using it.

1417
01:03:06.745 --> 01:03:08.885
And so we'll have to continue using it

1418
01:03:08.885 --> 01:03:09.965
until we come up with something better.

1419
01:03:09.985 --> 01:03:11.485
And the, the challenges on us,

1420
01:03:11.905 --> 01:03:13.285
and I think we're the ones to do it, you know,

1421
01:03:13.425 --> 01:03:16.405
flight testers are professional risk managers.

1422
01:03:16.435 --> 01:03:17.805
This is what we do for a living.

1423
01:03:18.465 --> 01:03:20.245
Um, and so that there's the challenge.

1424
01:03:20.585 --> 01:03:22.815
Um, there's some bright young people out there.

1425
01:03:22.855 --> 01:03:24.375
I, I hope that come up with a,

1426
01:03:24.575 --> 01:03:25.615
a better way of communicating.

1427
01:03:25.815 --> 01:03:26.975
'cause that's ultimately what it is, is

1428
01:03:26.975 --> 01:03:28.215
how do we communicate uncertainty.

1429
01:03:28.725 --> 01:03:33.195
Yeah. Susan was, uh, John Thomas available

1430
01:03:33.215 --> 01:03:37.155
to rejoin us for our joint q and A at the end.

1431
01:03:43.385 --> 01:03:44.625

I believe he's about to pop up.

1432
01:03:51.745 --> 01:03:54.115
Alright, well, what we, uh, continue learning how to use,

1433
01:03:54.215 --> 01:03:59.035
uh, go to webinar, we can take a chance

1434
01:03:59.155 --> 01:04:00.275
for another question with bika.

1435
01:04:01.295 --> 01:04:04.275
Um, you mentioned, uh,

1436
01:04:04.505 --> 01:04:07.035
deviation from your mental model manifesting

1437
01:04:07.035 --> 01:04:08.155
itself as surprises.

1438
01:04:09.015 --> 01:04:11.475
So whether or not you formally have a mental model

1439
01:04:11.495 --> 01:04:14.315
or not, I think most of us are familiar with the idea

1440
01:04:14.315 --> 01:04:16.155
of surprise, which kind of implies

1441
01:04:16.155 --> 01:04:17.555
that you actually did have a mental

1442
01:04:17.635 --> 01:04:18.835
model, you just weren't aware of it.

1443
01:04:19.375 --> 01:04:22.555
Uh, and that, that deviation, uh,

1444
01:04:25.155 --> 01:04:30.135
how, how are you using STPA to build that mental model?

1445
01:04:34.035 --> 01:04:38.735
So the, one of the first steps in SDPA is to have that,

1446
01:04:38.735 --> 01:04:39.775
uh, functional control diagram.

1447
01:04:40.985 --> 01:04:44.365
Um, you know, so, so that helps, you know, and,

1448
01:04:44.505 --> 01:04:48.725
and, um, it probably, you know, one thing that I, I,

1449
01:04:48.845 --> 01:04:51.765
I am realizing as a, as I've moved into, uh,

1450
01:04:51.765 --> 01:04:53.085
thinking about pedagogy

1451
01:04:53.085 --> 01:04:54.485
and how different people see the world

1452
01:04:54.505 --> 01:04:56.045
and understand things is,

1453
01:04:56.065 --> 01:04:57.485
is I tend to be a graphical person.

1454
01:04:57.665 --> 01:05:00.165
Uh, I, I tend to think, um, you know,

1455
01:05:00.235 --> 01:05:01.845
spatially and, and graphically.

1456
01:05:02.545 --> 01:05:07.055
Um, so, you know, one of the first steps for me is, is start

1457
01:05:07.075 --> 01:05:09.495
to, you know, draw, you know, you know, put things,

1458
01:05:09.595 --> 01:05:11.935

you know, draw a diagram, draw a relationship out on people

1459
01:05:11.935 --> 01:05:13.895
about how things interact on paper, about

1460
01:05:13.895 --> 01:05:15.055
how things interact with each other.

1461
01:05:15.595 --> 01:05:19.205
Um, that then you becomes more formal, uh, in the form

1462
01:05:19.265 --> 01:05:20.645
of a functional control diagram.

1463
01:05:21.265 --> 01:05:24.285
Uh, you can't really do STPA until you have that, uh,

1464
01:05:24.285 --> 01:05:27.325
until you've kind of identified, you know, what is the,

1465
01:05:27.385 --> 01:05:30.125
the plant being controlled, what is the controller, um,

1466
01:05:30.435 --> 01:05:33.605
what, what feedback is available from the

1467
01:05:34.495 --> 01:05:36.285
plant back to the controller.

1468
01:05:36.785 --> 01:05:40.005
Um, okay. So it's model first, then STPA,

1469
01:05:40.585 --> 01:05:42.285
not s st a to build the model

1470
01:05:42.795 --> 01:05:44.285
That Is, or is that too simplistic?

1471
01:05:44.465 --> 01:05:45.765
Um, yep. And,

1472
01:05:45.825 --> 01:05:48.885
and, uh, you know, John, if he, if he, there he is, John,

1473
01:05:49.385 --> 01:05:53.285
he could certainly, uh, uh, offer can far more, uh,

1474
01:05:53.825 --> 01:05:55.525
you know, enlightened perspective on that,

1475
01:05:55.545 --> 01:05:58.525
but I don't see how you could do STPA if you don't,

1476
01:05:58.545 --> 01:06:01.605
if you haven't started thinking about, um, you know,

1477
01:06:02.405 --> 01:06:04.525
modeling the system and how the, uh, how the interactions

1478
01:06:04.625 --> 01:06:06.805
and, and, and maybe as a result of that,

1479
01:06:06.825 --> 01:06:07.845
you actually add some.

1480
01:06:13.415 --> 01:06:16.345
John, do you have any thoughts on, on which came first,

1481
01:06:16.785 --> 01:06:19.625
STPA or the, or the functional system diagram?

1482
01:06:25.955 --> 01:06:28.615
Check your audio settings. You on mute?

1483
01:06:36.115 --> 01:06:38.105
Susan, are you able to check John's audio, please?

1484
01:06:40.635 --> 01:06:42.145
There we go. Thank you. Yep.

1485
01:06:43.145 --> 01:06:44.945

I confused just a little slow I was getting there.

1486
01:06:45.785 --> 01:06:47.505
I, yeah, great point.

1487
01:06:48.005 --> 01:06:52.425
Uh, the control structure is certainly central to STPA.

1488
01:06:52.885 --> 01:06:54.665
You can't have one without the other.

1489
01:06:55.325 --> 01:06:58.065
Um, and it's, it is interesting

1490
01:06:58.335 --> 01:07:01.505
that you mentioned the question about, uh, using STPA

1491
01:07:01.505 --> 01:07:03.585
to build a shared mental model.

1492
01:07:04.085 --> 01:07:05.585
One of the first applications

1493
01:07:05.585 --> 01:07:08.585
of STPA about 15 years ago now,

1494
01:07:09.005 --> 01:07:10.745
was the ballistic missile defense system.

1495
01:07:11.605 --> 01:07:15.985
And in that application, uh, right away, even

1496
01:07:16.005 --> 01:07:18.385
before the analysis was finished, when they

1497
01:07:19.065 --> 01:07:21.465
revealed the control structure on one slide,

1498
01:07:21.525 --> 01:07:23.145
now this was a high level control structure.

1499
01:07:23.485 --> 01:07:25.945
You can imagine this is an incredibly complex system.

1500
01:07:26.405 --> 01:07:29.025
The comment was, whoa, you did it.

1501
01:07:29.245 --> 01:07:31.425
And we said, what did, what, what do you mean?

1502
01:07:31.425 --> 01:07:33.385
They say, you've got it on one page.

1503
01:07:33.635 --> 01:07:35.505
We've been trying for a long time

1504
01:07:35.565 --> 01:07:37.065
to get this complex system.

1505
01:07:37.295 --> 01:07:40.105
Best we've got is a stack of pages like this, uh,

1506
01:07:40.105 --> 01:07:41.865
with incredibly detailed diagrams,

1507
01:07:41.885 --> 01:07:43.465
but this is what we've been missing.

1508
01:07:43.695 --> 01:07:46.545
This is the systems view, uh, of the thing.

1509
01:07:46.805 --> 01:07:49.905
And what they started doing is conversing just about

1510
01:07:50.005 --> 01:07:51.305
the control structure.

1511
01:07:51.375 --> 01:07:54.665
They realized some mental models were a little different

1512
01:07:54.665 --> 01:07:57.665

between how different folks thought the system worked at

1513
01:07:57.665 --> 01:07:59.505
that level of abstraction.

1514
01:07:59.505 --> 01:08:03.705
So they found just drawing the thing was incredibly useful.

1515
01:08:04.165 --> 01:08:05.905
Um, at that point, they were almost like,

1516
01:08:05.905 --> 01:08:06.905
forget the other steps.

1517
01:08:07.435 --> 01:08:08.665
Let's just draw this thing.

1518
01:08:08.845 --> 01:08:10.545
Uh, but then of course, you know, after,

1519
01:08:10.715 --> 01:08:13.185
after you do that, um, which has value,

1520
01:08:13.535 --> 01:08:14.985
then you start saying, all right, let's,

1521
01:08:15.150 --> 01:08:16.910
let's do better than just talk about it.

1522
01:08:16.975 --> 01:08:20.005
Let's, we need a rigorous way to actually go through this

1523
01:08:20.005 --> 01:08:21.405
and make sure we don't miss anything.

1524
01:08:21.825 --> 01:08:24.445
Um, and those are the following steps in STPA.

1525
01:08:26.445 --> 01:08:28.615
Okay. One of the, uh, one of the questions

1526
01:08:28.615 --> 01:08:30.135
that just popped up as you were speaking there was,

1527
01:08:31.235 --> 01:08:34.975
can you use STPA to, to fault check itself?

1528
01:08:35.595 --> 01:08:38.895
So, can you use STPA to, to ensure

1529
01:08:38.895 --> 01:08:40.735
that your mental model ensure that your,

1530
01:08:40.925 --> 01:08:43.675
your functional diagram is whole?

1531
01:08:43.895 --> 01:08:47.155
Is it complete? One of the, one of the issues for,

1532
01:08:47.415 --> 01:08:48.795
for program managers, for the,

1533
01:08:48.855 --> 01:08:52.555
the risk acceptance authorities is simply an assessment

1534
01:08:52.575 --> 01:08:55.675
of the breadth, breadth of the risk that's being presented.

1535
01:08:55.695 --> 01:08:58.315
And do we know how broad it goes?

1536
01:08:59.215 --> 01:09:01.235
Can s STPA a check itself?

1537
01:09:02.665 --> 01:09:04.555
Well, I mean, not, not directly.

1538
01:09:04.575 --> 01:09:06.035
And then you would say, how do you check that?

1539
01:09:06.035 --> 01:09:07.715

We'll do STPA again to check that

1540
01:09:07.935 --> 01:09:09.475
and just keep going all the way down.

1541
01:09:10.215 --> 01:09:12.955
Uh, but we do something similar. Actually.

1542
01:09:13.415 --> 01:09:16.115
Um, the folks who are applying STPA, they're,

1543
01:09:16.115 --> 01:09:18.715
they're basically performing a process to come up

1544
01:09:18.715 --> 01:09:21.675
with requirements and constraints and recommendations.

1545
01:09:22.385 --> 01:09:24.035
That is a control action.

1546
01:09:24.455 --> 01:09:26.435
And they're sitting, you know, engineers, uh,

1547
01:09:26.435 --> 01:09:27.755
flight test planners and so on,

1548
01:09:27.785 --> 01:09:31.555
they're sitting in a larger control structure themselves.

1549
01:09:32.105 --> 01:09:35.595
They may provide, uh, may have some errors

1550
01:09:35.595 --> 01:09:38.955
or some mistakes in the information they provide.

1551
01:09:38.975 --> 01:09:41.715
The decisions they make, those would be maybe unsafe

1552
01:09:41.715 --> 01:09:43.435
or undesirable control actions, of course,

1553
01:09:43.495 --> 01:09:44.555
not maliciously usually.

1554
01:09:44.975 --> 01:09:47.675
Um, but we can say, use the SDPA framework to say,

1555
01:09:47.815 --> 01:09:49.915
why are we making this mistake?

1556
01:09:49.925 --> 01:09:51.275
Maybe we've made, you know,

1557
01:09:51.595 --> 01:09:53.715
mistakes maybe once a month for the last 10 years.

1558
01:09:54.015 --> 01:09:56.875
And on the surface, superficially they might look like

1559
01:09:56.905 --> 01:09:57.955
very different mistakes.

1560
01:09:58.015 --> 01:10:01.235
You know, we had, you know, an alert that comes on too soon,

1561
01:10:01.335 --> 01:10:03.875
uh, for this feature, or over here, you know, we, we've got,

1562
01:10:03.875 --> 01:10:04.875
uh, you know, something wrong with

1563
01:10:04.875 --> 01:10:05.955
the power supply over there.

1564
01:10:06.115 --> 01:10:07.275
I mean, they look different on the surface.

1565
01:10:07.495 --> 01:10:10.595
But if you model this in SDPA, you say, okay, alright, look,

1566
01:10:10.615 --> 01:10:13.595

the specific control action, the exact requirement

1567
01:10:13.595 --> 01:10:16.395
that we missed is different on all these progre programs.

1568
01:10:16.815 --> 01:10:20.675
But the structure around our test planners

1569
01:10:20.815 --> 01:10:23.835
and around our pilots is largely the same.

1570
01:10:24.135 --> 01:10:27.355
What's wrong with the structure? What are the patterns here?

1571
01:10:27.425 --> 01:10:30.715
What kinds of beliefs do we have gaps in when we're making

1572
01:10:31.035 --> 01:10:32.955
decisions about requirements and recommendations?

1573
01:10:32.975 --> 01:10:34.995
And maybe when we're performing STPA

1574
01:10:35.015 --> 01:10:37.875
or any other method, really, what are, um,

1575
01:10:38.015 --> 01:10:41.475
the feedback sources that we're providing to the engineers?

1576
01:10:41.515 --> 01:10:45.275
A lot of times what happens is the system evolves while

1577
01:10:45.275 --> 01:10:47.235
we're doing these planning activities,

1578
01:10:47.415 --> 01:10:48.875
and we don't close the loop.

1579
01:10:48.975 --> 01:10:52.315
We don't notify, you know, the, the flight test planners

1580
01:10:52.315 --> 01:10:55.075
or engineers or the, or the pilots of some of these changes.

1581
01:10:55.225 --> 01:10:57.235
It's happened on almost every project, really,

1582
01:10:57.615 --> 01:10:58.635
um, what we need.

1583
01:10:58.635 --> 01:10:59.995
That's a structural problem.

1584
01:11:00.235 --> 01:11:02.275
I mean, the, the realization of

1585
01:11:02.275 --> 01:11:03.835
that might be slightly different every time,

1586
01:11:04.055 --> 01:11:07.395
but we've gotta identify the gaps in the control structure

1587
01:11:07.535 --> 01:11:10.315
around our engineers, around our pilots, and so on.

1588
01:11:10.315 --> 01:11:11.915
And that's where we see the patterns.

1589
01:11:12.185 --> 01:11:14.005
That also means it's incredibly effective.

1590
01:11:14.225 --> 01:11:17.005
If you fix, you know, you, you've realized that you,

1591
01:11:17.075 --> 01:11:18.885
there's an operational event that occurred,

1592
01:11:18.885 --> 01:11:20.125
and we didn't tell the pilot about that.

1593
01:11:20.125 --> 01:11:22.125

Well go tell the pilot about that operational event,

1594
01:11:22.125 --> 01:11:24.085
but that prevents exactly one problem.

1595
01:11:24.705 --> 01:11:27.445
If you find the structural issue about why all

1596
01:11:27.445 --> 01:11:30.005
of these types of events are not being provided,

1597
01:11:30.105 --> 01:11:31.445
and we're not following up

1598
01:11:31.445 --> 01:11:35.245
and closing the loop, then you prevent lots of accidents.

1599
01:11:35.245 --> 01:11:37.725
So, so it's much more powerful actually to do that.

1600
01:11:38.075 --> 01:11:42.685
Yeah. So it encourages you to convey, uh, it relates

1601
01:11:42.685 --> 01:11:43.845
to one of the questions that come up here.

1602
01:11:43.845 --> 01:11:46.365
They're conveying the, the procedures

1603
01:11:46.365 --> 01:11:49.005
and the system descriptions, uh, through the, uh,

1604
01:11:49.005 --> 01:11:50.365
through the aircraft manuals.

1605
01:11:51.125 --> 01:11:52.365
I wonder if you can spend, uh, John,

1606
01:11:52.405 --> 01:11:55.545
I wonder if you can spend a minute or two relating to us

1607
01:11:55.605 --> 01:11:57.465
how STPA relates to fika.

1608
01:11:57.465 --> 01:12:00.265
There's been some, uh, guess sort of addressing a,

1609
01:12:00.305 --> 01:12:01.305
a different community within,

1610
01:12:01.685 --> 01:12:03.265
within the flight test safety committee.

1611
01:12:03.275 --> 01:12:06.505
We've got some of the, the very small startups, small teams,

1612
01:12:06.565 --> 01:12:08.705
but some of our bigger industry players

1613
01:12:08.765 --> 01:12:12.265
and some of the big, uh, the big defense projects, uh,

1614
01:12:12.265 --> 01:12:14.305
mandate the use of fika and, uh,

1615
01:12:14.305 --> 01:12:19.265
and if, uh, functional, uh, uh, F-F-M-E-A

1616
01:12:19.445 --> 01:12:22.345
as well as the fika, how do these relate?

1617
01:12:22.965 --> 01:12:25.665
Is S-T-P-A-A-A different flavor of the same ice cream,

1618
01:12:25.685 --> 01:12:26.785
or are we, or is it,

1619
01:12:28.445 --> 01:12:29.665
Uh, well differ?

1620
01:12:30.025 --> 01:12:33.145

I, now that you've asked question, I have to answer it,

1621
01:12:33.225 --> 01:12:35.305
I think, uh, I usually try to avoid that.

1622
01:12:35.465 --> 01:12:37.865
I try to just stick to S tpa. A Oh,

1623
01:12:37.865 --> 01:12:39.785
You, you, you can't avoid coming out your,

1624
01:12:39.895 --> 01:12:40.895
It's a natural question.

1625
01:12:41.445 --> 01:12:43.665
Uh, the problem is sometimes, I mean, we've got a lot

1626
01:12:43.665 --> 01:12:45.785
of folks on the, on the call, I interact with

1627
01:12:45.805 --> 01:12:47.665
so many different, uh, mindsets.

1628
01:12:47.975 --> 01:12:49.625
Some folks will probably feel like, yeah,

1629
01:12:49.715 --> 01:12:51.225
let's do SDPA tonight.

1630
01:12:51.685 --> 01:12:54.945
Um, some folk, I've met other folks that, that come

1631
01:12:54.945 --> 01:12:57.425
to me on day one of A-S-T-P-A class,

1632
01:12:57.445 --> 01:12:58.745
and they say, I just want you to know,

1633
01:12:59.085 --> 01:13:03.025
the reason I'm here is because I am a fika expert,

1634
01:13:03.605 --> 01:13:07.465
and I'm here to prove to you that we can, uh, do more

1635
01:13:07.465 --> 01:13:09.545
with FIKA than you can with STPA.

1636
01:13:09.655 --> 01:13:13.585
Like, wow, what, what, what kind of mindset is that?

1637
01:13:13.845 --> 01:13:17.305
Um, uh, I mean, so, uh, they're different.

1638
01:13:17.305 --> 01:13:18.345
They're different methods.

1639
01:13:18.765 --> 01:13:23.105
Uh, um, one of the differences is, um, uh,

1640
01:13:23.575 --> 01:13:27.025
fika and FIA are designed, uh, first, they're,

1641
01:13:27.025 --> 01:13:28.745
they're designed kind of for a different problem.

1642
01:13:28.985 --> 01:13:31.145
I, I think that's a pretty strong argument to make.

1643
01:13:31.295 --> 01:13:32.705
They're developed, believe it

1644
01:13:32.705 --> 01:13:36.065
or not, in the 1940s, a lot of folks are using this

1645
01:13:36.065 --> 01:13:37.065
as the go-to method,

1646
01:13:37.125 --> 01:13:39.545
but they, they don't realize, uh, how old it is.

1647
01:13:39.845 --> 01:13:41.105

It that doesn't make it bad.

1648
01:13:41.205 --> 01:13:42.505
It just means it's developed

1649
01:13:42.505 --> 01:13:45.865
for something a little different than we, than, um, we've,

1650
01:13:45.865 --> 01:13:47.225
we've had new problems since then.

1651
01:13:47.935 --> 01:13:49.865
It's basically looks at components.

1652
01:13:50.165 --> 01:13:51.345
And one of the strengths

1653
01:13:51.345 --> 01:13:53.905
of the method is it's really good at finding single point

1654
01:13:53.905 --> 01:13:54.945
component failures.

1655
01:13:55.605 --> 01:13:57.505
Now, the word failure can be defined.

1656
01:13:57.525 --> 01:13:59.265
If you look different standards,

1657
01:13:59.265 --> 01:14:01.185
they have slightly different, uh, definitions.

1658
01:14:01.285 --> 01:14:05.225
But it's essentially considered, uh, uh, the definition

1659
01:14:05.225 --> 01:14:07.665
of component failure is when a component does not

1660
01:14:07.665 --> 01:14:08.985
operate as specified.

1661
01:14:09.485 --> 01:14:11.025
You can change out a couple of those words,

1662
01:14:11.225 --> 01:14:13.325
but it essentially comes back to some notion

1663
01:14:13.325 --> 01:14:15.885
of a component not operating the way it's supposed to.

1664
01:14:16.345 --> 01:14:18.485
And that is not the entire problem.

1665
01:14:18.705 --> 01:14:19.765
It is part of the problem.

1666
01:14:19.995 --> 01:14:22.165
It's an important part, and we've gotta look at those.

1667
01:14:22.845 --> 01:14:24.205
STPA looks at those two, by the way.

1668
01:14:24.425 --> 01:14:27.605
Uh, but lots of methods, look at those. FMEA is ones fault.

1669
01:14:27.605 --> 01:14:30.125
TREE is another approach, and there are lots of others.

1670
01:14:30.625 --> 01:14:35.085
Um, however, what we've seen in the last 10 years, um, with,

1671
01:14:35.105 --> 01:14:38.565
you know, a ziana and, uh, air France 4, 4, 7,

1672
01:14:38.625 --> 01:14:40.845
and almost any accident you look at, um,

1673
01:14:41.855 --> 01:14:43.485
there might be a component that fails.

1674
01:14:43.485 --> 01:14:45.125

Sometimes there's no component failure,

1675
01:14:45.305 --> 01:14:48.085
but there are almost always interactions

1676
01:14:48.385 --> 01:14:51.805
beyond the failure if it occurred, that really matter.

1677
01:14:51.815 --> 01:14:54.045
Where pilots are following procedures,

1678
01:14:54.465 --> 01:14:56.725
and the procedures have gaps or limitations,

1679
01:14:57.025 --> 01:15:00.005
or pilots deviate from procedures, which happens every day,

1680
01:15:00.005 --> 01:15:01.205
by the way, for good reasons.

1681
01:15:01.665 --> 01:15:03.285
Uh, but they didn't have the information needed

1682
01:15:03.285 --> 01:15:05.405
to know when it was a good thing, when it was a bad thing,

1683
01:15:05.585 --> 01:15:08.525
or, uh, automation, uh, and sensors

1684
01:15:08.525 --> 01:15:10.565
and other things working exactly as designed.

1685
01:15:11.145 --> 01:15:13.485
That's one of the sweet spots for STPA.

1686
01:15:13.635 --> 01:15:17.165
It's really good at finding the non failure cases, uh,

1687
01:15:17.165 --> 01:15:19.045
that you typically, there's no failure mode.

1688
01:15:19.065 --> 01:15:20.685
So you, you would not be looking for

1689
01:15:20.685 --> 01:15:22.485
that in something like in FMEA.

1690
01:15:22.945 --> 01:15:25.965
Now, I, I feel like I should say something about FMEA, uh,

1691
01:15:25.995 --> 01:15:28.405
once I, I interacted with somebody, he wasn't so happy

1692
01:15:28.405 --> 01:15:31.605
with SDPA, um, he said, I still prefer FMEA.

1693
01:15:31.645 --> 01:15:34.445
I said, why? He was in a regulatory, uh, framework.

1694
01:15:34.445 --> 01:15:36.645
And he said, what I like about FMEA, number one,

1695
01:15:36.645 --> 01:15:37.965
the regulator requires it.

1696
01:15:38.305 --> 01:15:42.405
And number two, um, I know, uh, all I have to do is go

1697
01:15:42.405 --> 01:15:44.165
through every component and show

1698
01:15:44.195 --> 01:15:46.645
that I've considered the single failure of that component,

1699
01:15:46.705 --> 01:15:48.605
and I know, uh, that I'm done.

1700
01:15:48.915 --> 01:15:50.885
It's a, it doesn't require a lot of thinking,

1701
01:15:51.305 --> 01:15:52.525

uh, to get through the process.

1702
01:15:53.065 --> 01:15:54.765
Um, and he says, STPA,

1703
01:15:55.045 --> 01:15:57.605
although it probably is the right thing to do, uh, it,

1704
01:15:57.605 --> 01:15:58.605
it probably would be useful.

1705
01:15:58.825 --> 01:16:00.405
Uh, it's not required by the regulator,

1706
01:16:00.625 --> 01:16:03.965
and it looks like it, it might take, uh, more out

1707
01:16:03.965 --> 01:16:06.925
of the box, uh, thinking than, than going through an FMBA.

1708
01:16:06.925 --> 01:16:10.005
So he didn't prefer, um, STPA, uh,

1709
01:16:10.185 --> 01:16:13.445
but anyway, I mean, it, STPA came out of accidents.

1710
01:16:13.445 --> 01:16:16.685
It came out of that crack that currently exists out

1711
01:16:16.685 --> 01:16:19.005
of the stuff that we are missing, uh,

1712
01:16:19.005 --> 01:16:20.365
in our current framework.

1713
01:16:20.425 --> 01:16:21.885
It doesn't mean it's the only tool.

1714
01:16:21.885 --> 01:16:23.205
It doesn't mean it's the only solution,

1715
01:16:23.205 --> 01:16:25.325
but it's very, very good at what it does.

1716
01:16:26.725 --> 01:16:28.685
Okay. Thank you, John.

1717
01:16:29.745 --> 01:16:33.445
Uh, one of the, I'm not sure what, where to pitch this one

1718
01:16:33.465 --> 01:16:35.685
to, to Doug or to or to John.

1719
01:16:35.995 --> 01:16:37.165
This idea of software.

1720
01:16:37.665 --> 01:16:39.925
Um, and I came up with, uh,

1721
01:16:40.235 --> 01:16:42.645
with John's presentation very early on, the idea that

1722
01:16:43.445 --> 01:16:44.885
software doesn't make errors.

1723
01:16:44.885 --> 01:16:48.285
It just does what it's told, um, or how it's coded in.

1724
01:16:48.345 --> 01:16:51.285
And, and Doug, you had featured software within your

1725
01:16:51.695 --> 01:16:53.805
complexity, uh, discussion.

1726
01:16:54.825 --> 01:16:57.485
If that is the case, if the software is not making errors,

1727
01:16:58.505 --> 01:17:01.725
how would we model that inside an STPA framework?

1728
01:17:03.065 --> 01:17:06.685

Oh, very easily in the 2D matrix, we, we fudge and we hedge,

1729
01:17:06.745 --> 01:17:09.085
and we, we assume a probability knowing

1730
01:17:09.165 --> 01:17:11.325
that the probability is a one or a zero.

1731
01:17:11.505 --> 01:17:13.205
So we've immediately broken our own model.

1732
01:17:14.145 --> 01:17:16.165
How would we do that in an STPA context?

1733
01:17:17.275 --> 01:17:20.325
Well, there's kind of two, I hear two questions in there

1734
01:17:20.325 --> 01:17:21.605
that maybe I'll try to figure it out.

1735
01:17:21.745 --> 01:17:22.765
One is, uh,

1736
01:17:22.785 --> 01:17:26.005
how do we model software errors in an STA framework?

1737
01:17:26.005 --> 01:17:29.205
That's, uh, I think I can answer that easily, maybe.

1738
01:17:29.865 --> 01:17:32.405
Um, the other question is how do we rank

1739
01:17:32.465 --> 01:17:33.525
and prioritize things?

1740
01:17:33.545 --> 01:17:36.125
And that's the 2D matrix that you ma the risk matrix.

1741
01:17:36.785 --> 01:17:38.765
Um, how do, how do we prioritize?

1742
01:17:38.765 --> 01:17:40.565
And those are two separate questions in my view.

1743
01:17:40.905 --> 01:17:42.365
Uh, they're related of course, but, um,

1744
01:17:42.925 --> 01:17:45.925
software errors are not hard to model an SD tpa

1745
01:17:46.165 --> 01:17:47.645
'cause you don't actually need to know

1746
01:17:48.185 --> 01:17:50.405
how the software works, or if an error exists.

1747
01:17:50.985 --> 01:17:52.565
You can apply STPA

1748
01:17:52.565 --> 01:17:54.525
with almost no information about the software.

1749
01:17:54.545 --> 01:17:55.885
We treat it as a black box.

1750
01:17:56.545 --> 01:17:59.765
Uh, we just, like we did in all the examples in my lecture

1751
01:17:59.945 --> 01:18:02.045
now, now we took some shortcuts just to be clear.

1752
01:18:02.545 --> 01:18:05.485
Um, but that, that part is normal.

1753
01:18:05.585 --> 01:18:08.125
We normally would not pull up a, you know, a thousand lines

1754
01:18:08.125 --> 01:18:10.445
of software code in order to perform STPA.

1755
01:18:10.705 --> 01:18:12.125

We would say, alright, forget

1756
01:18:12.125 --> 01:18:13.445
that it might be right, might be wrong.

1757
01:18:13.625 --> 01:18:15.085
Uh, we don't even have to look at that yet.

1758
01:18:15.195 --> 01:18:17.085
Tell me, what are the outputs from the software?

1759
01:18:17.675 --> 01:18:18.965
What are the control actions?

1760
01:18:19.295 --> 01:18:20.565
Those are definable even

1761
01:18:20.565 --> 01:18:23.445
before the software is written or after.

1762
01:18:23.955 --> 01:18:25.085
What are the control actions?

1763
01:18:25.305 --> 01:18:26.725
And then tell me what,

1764
01:18:26.795 --> 01:18:29.125
when are the control actions safe or unsafe?

1765
01:18:29.545 --> 01:18:30.645
We don't answer that question

1766
01:18:30.645 --> 01:18:32.245
by looking at this, what the software says.

1767
01:18:32.505 --> 01:18:34.525
So we don't go to prove the software.

1768
01:18:34.885 --> 01:18:36.925
Whatever they wrote is correct. We say, let's look

1769
01:18:36.925 --> 01:18:38.045
outside of the software.

1770
01:18:38.385 --> 01:18:41.005
Forget what they wrote. Let's look outside the software,

1771
01:18:41.005 --> 01:18:42.605
because that's what's gonna decide

1772
01:18:42.755 --> 01:18:44.645
what control actions are safe or unsafe.

1773
01:18:44.905 --> 01:18:45.925
So pitch up command,

1774
01:18:45.925 --> 01:18:48.045
pitch down command software code doesn't determine,

1775
01:18:48.045 --> 01:18:49.365
determine if that's safe or not.

1776
01:18:49.475 --> 01:18:51.365
What determines that's safe is the effect it has in the

1777
01:18:51.525 --> 01:18:53.245
aircraft and the situation you're providing it in.

1778
01:18:53.505 --> 01:18:56.965
So we define the unsafe control actions that if

1779
01:18:57.365 --> 01:18:59.125
provided by whatever software you come up

1780
01:18:59.125 --> 01:19:00.645
with would be unsafe.

1781
01:19:00.705 --> 01:19:03.565
We declare those, we write them, we review them,

1782
01:19:03.585 --> 01:19:05.685

we talk about them, and we put requirements in

1783
01:19:05.685 --> 01:19:07.325
place to prevent them.

1784
01:19:07.785 --> 01:19:10.085
And then towards the end of the process,

1785
01:19:10.985 --> 01:19:13.205
if software becomes available to review,

1786
01:19:13.395 --> 01:19:14.885
then you might open up the hood

1787
01:19:14.885 --> 01:19:17.565
and say, all right, here's what STPA says it needs to do

1788
01:19:17.585 --> 01:19:18.725
to prevent an accident.

1789
01:19:18.725 --> 01:19:20.045
Does it match what they came up

1790
01:19:20.045 --> 01:19:21.365
with in their solution space?

1791
01:19:21.785 --> 01:19:23.845
So we never start with a solution.

1792
01:19:23.865 --> 01:19:26.605
We never start with an error or a perfect solution.

1793
01:19:26.605 --> 01:19:27.885
We start with a black box

1794
01:19:28.385 --> 01:19:30.365
and postulate what we need to prevent

1795
01:19:30.465 --> 01:19:31.685
and put requirements in place.

1796
01:19:31.865 --> 01:19:34.205
And so on. Your other question about ranking

1797
01:19:34.265 --> 01:19:39.085
and prioritizing, um, scenarios and ucas and other artifacts

1798
01:19:39.085 --> 01:19:40.725
and STPA, we do that all the time.

1799
01:19:40.785 --> 01:19:43.645
Now. We don't use a risk matrix that kind of, the,

1800
01:19:43.825 --> 01:19:47.245
the problem with the risk matrix is it really has really old

1801
01:19:47.375 --> 01:19:51.005
roots and foundations similar to FMEA.

1802
01:19:51.225 --> 01:19:52.885
It, it was developed a long,

1803
01:19:52.885 --> 01:19:55.645
long time ago when component failures stuff breaking,

1804
01:19:55.765 --> 01:19:57.885
especially mechanical connections on aircraft

1805
01:19:57.885 --> 01:19:59.445
and things like that were breaking.

1806
01:19:59.705 --> 01:20:04.285
Um, and over time, and we found a great way to model that.

1807
01:20:04.465 --> 01:20:06.205
The risk matrix. The problem is

1808
01:20:06.205 --> 01:20:09.245
what we're having now is requirements, um,

1809
01:20:09.585 --> 01:20:11.325

are being satisfied correctly.

1810
01:20:12.105 --> 01:20:14.245
100% of the time.

1811
01:20:14.425 --> 01:20:16.365
The software is satisfying the requirements,

1812
01:20:16.465 --> 01:20:17.605
and it brings down the plane

1813
01:20:17.635 --> 01:20:19.725
because it met its requirements.

1814
01:20:20.425 --> 01:20:23.245
Um, we see that in a lot of recent events, uh, uh,

1815
01:20:23.245 --> 01:20:24.645
right on the tip of our tongues, right?

1816
01:20:25.385 --> 01:20:28.285
Um, the software wasn't, didn't have an error at all.

1817
01:20:28.805 --> 01:20:30.285
Arguably, you go through the software engineers

1818
01:20:30.285 --> 01:20:31.645
and say, why'd you write this line of code?

1819
01:20:31.645 --> 01:20:33.765
They'll say, because you told me to. That's why.

1820
01:20:34.025 --> 01:20:36.485
And it passed every single component level test,

1821
01:20:36.485 --> 01:20:38.405
every single verification and so on.

1822
01:20:38.785 --> 01:20:40.565
The problem is the interaction and the system level.

1823
01:20:40.625 --> 01:20:43.005
So probability kind of breaks down

1824
01:20:43.385 --> 01:20:45.005
as a distinguishing measure.

1825
01:20:45.475 --> 01:20:46.965
It's not a universal measure.

1826
01:20:47.185 --> 01:20:50.165
It does work very good for what it was originally intended

1827
01:20:50.305 --> 01:20:51.685
for, for a component.

1828
01:20:51.715 --> 01:20:53.845
Certain types of component failures maybe.

1829
01:20:54.025 --> 01:20:56.265
But for this requirements problem,

1830
01:20:57.185 --> 01:20:59.105
re reliability either is not applicable

1831
01:20:59.105 --> 01:21:00.785
or it's unknowable When you,

1832
01:21:00.975 --> 01:21:02.985
when you have a flawed requirement, I mean,

1833
01:21:02.985 --> 01:21:04.625
if we knew the requirement was flawed,

1834
01:21:04.725 --> 01:21:07.665
we wouldn't waste any time putting a, a probability on it.

1835
01:21:07.735 --> 01:21:09.065
We'd just fix the requirement, right?

1836
01:21:09.125 --> 01:21:11.465

As engineers or put mitigation in place.

1837
01:21:11.965 --> 01:21:14.385
So, but that's okay. That's not the end of the day.

1838
01:21:14.525 --> 01:21:16.865
We just need a different solution than probability

1839
01:21:16.925 --> 01:21:17.945
for these types of problems.

1840
01:21:18.365 --> 01:21:20.105
And there are lots of them.

1841
01:21:20.585 --> 01:21:22.785
Severity is one that's part of the risk matrix,

1842
01:21:22.885 --> 01:21:24.745
and it still works for these new problems.

1843
01:21:24.985 --> 01:21:27.785
Severity is a great one. Another one is controllability,

1844
01:21:27.785 --> 01:21:30.385
which is actually proposed in mill standard 8 82.

1845
01:21:30.685 --> 01:21:32.625
The risk matrix, a lot of people don't know this.

1846
01:21:32.845 --> 01:21:35.225
It is inside mill standard 8 82,

1847
01:21:35.445 --> 01:21:39.065
but, um, guess what's in appendix A for software?

1848
01:21:39.805 --> 01:21:42.705
The standard says there's an alternative risk matrix

1849
01:21:42.775 --> 01:21:44.545
that may be more useful for you.

1850
01:21:44.845 --> 01:21:47.625
And what they do is replace the probability dimension

1851
01:21:47.625 --> 01:21:50.545
completely by something they call controllability.

1852
01:21:50.605 --> 01:21:52.065
And they've got five measures

1853
01:21:52.325 --> 01:21:53.865
of controllability to put in there.

1854
01:21:54.025 --> 01:21:55.185
I don't think that's perfect either.

1855
01:21:55.445 --> 01:21:56.985
Uh, but at least it's doable

1856
01:21:57.165 --> 01:21:59.625
for something like a, a requirements problem.

1857
01:21:59.855 --> 01:22:01.745
Another one to look at is cost.

1858
01:22:02.045 --> 01:22:03.705
Now, I hesitate to say that

1859
01:22:03.705 --> 01:22:06.145
because you can, you can use that in the wrong way.

1860
01:22:06.145 --> 01:22:08.225
You can only fix the low cost problems

1861
01:22:08.225 --> 01:22:09.705
and leave the most expensive ones.

1862
01:22:09.705 --> 01:22:11.145
That's not good. That's not a good answer.

1863
01:22:11.415 --> 01:22:14.505

However, it, it might be one factor to consider,

1864
01:22:14.505 --> 01:22:18.585
because so many of these requirements problems, the cost

1865
01:22:18.725 --> 01:22:21.785
to fix them, especially if you find it early, uh,

1866
01:22:21.785 --> 01:22:23.545
before operation, it may be

1867
01:22:23.545 --> 01:22:26.345
before you actually go out on your flight test early in

1868
01:22:26.625 --> 01:22:28.785
planning, if you get flight test engineers involved early

1869
01:22:28.785 --> 01:22:30.865
during development, which you absolutely should,

1870
01:22:31.405 --> 01:22:34.145
you can catch this when it's almost free

1871
01:22:34.805 --> 01:22:36.145
to fix these problems.

1872
01:22:36.485 --> 01:22:38.305
You just changed the requirement you wrote down.

1873
01:22:38.385 --> 01:22:39.545
I mean, how long does it take to,

1874
01:22:39.565 --> 01:22:40.625
to type a different answer?

1875
01:22:40.905 --> 01:22:42.185
I mean, I'm exaggerating slightly,

1876
01:22:42.485 --> 01:22:43.985
but the cost is almost nothing.

1877
01:22:44.335 --> 01:22:47.825
Literally talking, the time you would spend talking about,

1878
01:22:48.205 --> 01:22:51.025
uh, doing a risk assessment is longer than just

1879
01:22:51.045 --> 01:22:52.185
fixing the problem.

1880
01:22:52.525 --> 01:22:55.905
It is. So, so we can use cost maybe as a way

1881
01:22:55.905 --> 01:22:57.305
to identify low hanging fruit.

1882
01:22:57.485 --> 01:22:59.305
And there are other measures that we can look at.

1883
01:23:00.005 --> 01:23:02.945
I'm hearing that SDPA is a, is an extra tool

1884
01:23:02.945 --> 01:23:05.065
that we can use at that FME level too.

1885
01:23:05.515 --> 01:23:08.405
It's for a d for me, focusing on the components.

1886
01:23:09.765 --> 01:23:11.205
TPA throws a wider net

1887
01:23:11.305 --> 01:23:13.565
and starts including including the

1888
01:23:13.565 --> 01:23:14.725
humans and the way we operate.

1889
01:23:15.265 --> 01:23:17.525
That's right. Another thing I've been talking about,

1890
01:23:17.525 --> 01:23:19.245

component failure, kind of talking to the engineers.

1891
01:23:19.245 --> 01:23:21.165
I guess another thing that it can find the analog

1892
01:23:21.165 --> 01:23:23.485
for human behavior is that the procedures are wrong.

1893
01:23:24.185 --> 01:23:29.125
Mm-hmm. SDPA will nail down procedure 1.6 0.2 is

1894
01:23:29.135 --> 01:23:32.885
wrong because it's going to cause a, a loss of thrust.

1895
01:23:32.905 --> 01:23:35.045
In this case. You don't want that procedure.

1896
01:23:35.365 --> 01:23:37.205
I mean, what's the probability of the procedure is wrong?

1897
01:23:37.205 --> 01:23:38.445
Well, once you find it, the

1898
01:23:38.445 --> 01:23:39.485
probability is a hundred percent.

1899
01:23:39.555 --> 01:23:41.925
What, what do you mean probability of a procedure

1900
01:23:41.925 --> 01:23:43.525
that's wrong once you find it.

1901
01:23:44.265 --> 01:23:45.405
Um, it's, it,

1902
01:23:45.405 --> 01:23:48.005
the probability comes way for certain problems. Yeah.

1903
01:23:48.955 --> 01:23:52.285
Another real challenge software is, uh,

1904
01:23:52.625 --> 01:23:54.805
is there's a trend right now towards, uh,

1905
01:23:54.815 --> 01:23:56.045
agile software development.

1906
01:23:56.745 --> 01:23:58.845
Um, you know, it goes by a lot of different names.

1907
01:23:59.145 --> 01:24:00.845
And, um,

1908
01:24:02.225 --> 01:24:05.205
and there's, you know, the, the frequency with which, uh,

1909
01:24:05.415 --> 01:24:08.845
agile is changing puts a lot of pressure on us as testers.

1910
01:24:09.705 --> 01:24:13.045
Um, and, you know, in terms of what, you know,

1911
01:24:13.045 --> 01:24:14.165
what is the state of the system

1912
01:24:14.345 --> 01:24:15.965
and what is, uh, you know, what has been changed

1913
01:24:16.105 --> 01:24:18.045
and what has been changed without us doing it.

1914
01:24:19.075 --> 01:24:20.775
And to the, to the extent, extent

1915
01:24:20.775 --> 01:24:24.575
that flight critical things are separated away from, uh,

1916
01:24:24.795 --> 01:24:25.935
you know, the agile pieces.

1917
01:24:26.835 --> 01:24:28.695

Um, I I is helpful,

1918
01:24:28.915 --> 01:24:33.135
but it's, you know, necessary but not sufficient. Um, okay.

1919
01:24:34.115 --> 01:24:35.455
Um, I'm not aware of

1920
01:24:35.455 --> 01:24:37.575
how much flight tests is AC actually gets

1921
01:24:37.575 --> 01:24:38.735
done at the USAF Academy.

1922
01:24:39.615 --> 01:24:41.215
I know you were previously, uh,

1923
01:24:41.415 --> 01:24:43.935
a commander out at the Edwards base.

1924
01:24:45.195 --> 01:24:46.375
Was there an example from there

1925
01:24:46.375 --> 01:24:49.575
where STPA was employed on at a tactical level?

1926
01:24:50.895 --> 01:24:54.915
Uh, there was, and, um, uh, poncho, uh,

1927
01:24:54.915 --> 01:24:57.635
major Summers is gonna be, uh, uh, presenting tomorrow.

1928
01:24:57.855 --> 01:24:59.035
She was part of that effort.

1929
01:24:59.175 --> 01:25:01.995
Um, they, they actually ran side by side, uh,

1930
01:25:02.045 --> 01:25:03.715
about a half dozen different programs.

1931
01:25:04.965 --> 01:25:06.545
Um, and, and compared, you know,

1932
01:25:06.545 --> 01:25:10.705
the traditional test planning with, uh, with SDPA, um,

1933
01:25:12.435 --> 01:25:15.485
unfortunately the, uh, we learned some

1934
01:25:15.485 --> 01:25:16.805
of the wrong lessons from that

1935
01:25:16.805 --> 01:25:20.965
because we, we picked programs, uh, which had, you know,

1936
01:25:20.965 --> 01:25:22.765
you could pull the binder off the shelf, uh,

1937
01:25:22.765 --> 01:25:25.365
that had all the, uh, PHAs and GMCs

1938
01:25:25.385 --> 01:25:27.285
and, um, you know, you,

1939
01:25:27.505 --> 01:25:29.005
you first had to blow the dust off of it.

1940
01:25:29.675 --> 01:25:31.355
'cause we've been using it for, for two decades.

1941
01:25:32.175 --> 01:25:36.715
Um, but, you know, so some of the conclusions that the, the,

1942
01:25:36.935 --> 01:25:40.355
the, the folks in the, in the test center safety office came

1943
01:25:40.355 --> 01:25:41.435
to was that, well, yep.

1944
01:25:41.975 --> 01:25:44.555

Uh, that was an awful lot of work to do the SPPA thing.

1945
01:25:44.975 --> 01:25:46.235
Uh, and I didn't learn anything else.

1946
01:25:46.285 --> 01:25:47.875
Which again, I think is, uh,

1947
01:25:47.895 --> 01:25:49.155
you know, kind of misses the point because,

1948
01:25:50.175 --> 01:25:52.635
So is it fair to say then that stpa is a,

1949
01:25:52.755 --> 01:25:53.915
a tool in your tool bag,

1950
01:25:53.975 --> 01:25:58.075
but it's, it's kind of a hind glass break here in case of,

1951
01:25:58.295 --> 01:25:59.515
of extra complexity?

1952
01:26:01.255 --> 01:26:02.555
It, it is definitely a tool.

1953
01:26:02.615 --> 01:26:05.965
It, it, I see it as a framework for, uh,

1954
01:26:05.965 --> 01:26:07.245
thinking about systems.

1955
01:26:08.065 --> 01:26:11.125
Um, and it's, and it's particularly useful

1956
01:26:11.125 --> 01:26:14.925
and applicable as systems and system interactions.

1957
01:26:14.925 --> 01:26:17.245
And system of systems. Um, you know,

1958
01:26:17.245 --> 01:26:21.415
as we increasingly test those, uh, to, to really kind of

1959
01:26:22.115 --> 01:26:23.455
wr out the interfaces

1960
01:26:23.455 --> 01:26:26.255
and ring out the interactions, you know, a a lot

1961
01:26:26.255 --> 01:26:29.135
of the failures that we're seeing are, um, are

1962
01:26:29.155 --> 01:26:30.255
of an emergent nature.

1963
01:26:31.555 --> 01:26:34.895
Uh, and, and so that's where SBA comes, uh, you know,

1964
01:26:34.895 --> 01:26:36.655
becomes a, a, a very useful tool

1965
01:26:36.675 --> 01:26:39.055
and framework, uh, for approaching those types

1966
01:26:39.055 --> 01:26:40.335
of problems and those types of systems.

1967
01:26:41.035 --> 01:26:42.255
Uh, it is hard work.

1968
01:26:42.415 --> 01:26:44.735
I mean, it, it doesn't, it doesn't do the thinking for you,

1969
01:26:44.755 --> 01:26:47.255
you know, there's no, there's no SDPA algorithm

1970
01:26:47.255 --> 01:26:48.935
that you can just say, okay, here's all the data

1971
01:26:49.235 --> 01:26:50.455

and spit me out an answer.

1972
01:26:51.155 --> 01:26:53.935
Um, you know, the, the intellectual energy

1973
01:26:54.475 --> 01:26:57.335
and calories that go into coming up with, uh, you know,

1974
01:26:57.335 --> 01:27:00.855
thinking about the system and what could go wrong, uh,

1975
01:27:01.035 --> 01:27:02.695
are are still you.

1976
01:27:02.695 --> 01:27:03.975
That heavy lifting is still there.

1977
01:27:04.315 --> 01:27:06.455
Yep. Is there a natural stopping point?

1978
01:27:07.235 --> 01:27:09.255
So we go through this analysis

1979
01:27:09.255 --> 01:27:10.815
through all the, the functional diagram.

1980
01:27:11.035 --> 01:27:12.215
We ask the questions at each

1981
01:27:12.215 --> 01:27:13.335
of the point of points of control.

1982
01:27:14.115 --> 01:27:16.055
Is that the end of R-S-T-P-A?

1983
01:27:16.805 --> 01:27:20.085
I don't think so. Um, uh, I I think it's a,

1984
01:27:20.085 --> 01:27:21.765
it's a continuous and iterative process,

1985
01:27:21.765 --> 01:27:23.045
particularly in flight test.

1986
01:27:23.505 --> 01:27:25.845
Uh, 'cause we're constantly learning about the system.

1987
01:27:26.145 --> 01:27:27.525
And the system is, you know,

1988
01:27:27.565 --> 01:27:29.445
I understand the system is constantly being updated

1989
01:27:30.025 --> 01:27:31.045
as we go through flight tests.

1990
01:27:31.065 --> 01:27:33.525
So I, you know, I I don't think it's, you know, two times

1991
01:27:33.525 --> 01:27:35.005
through the loop or three times through the loop.

1992
01:27:35.045 --> 01:27:36.605
I, I think you're constantly doing it.

1993
01:27:37.025 --> 01:27:41.085
And when you start to see a, a growing divergence between

1994
01:27:41.115 --> 01:27:42.445
what you thought was going to happen

1995
01:27:42.465 --> 01:27:46.085
and what is happening, uh, that's probably a, a sign that,

1996
01:27:46.105 --> 01:27:47.725
Hey, we need to go do this again now.

1997
01:27:49.105 --> 01:27:53.635
Okay. I, I, I agree with beaker, by the way.

1998
01:27:53.895 --> 01:27:56.195

Uh, I will also add, uh,

1999
01:27:56.485 --> 01:28:00.275
there is a stopping rule on a per,

2000
01:28:00.855 --> 01:28:02.075
uh, issue basis.

2001
01:28:02.735 --> 01:28:05.755
Um, it, it doesn't change anything you just said, um,

2002
01:28:05.775 --> 01:28:08.355
but it might be more satisfactory to some folks out there.

2003
01:28:08.735 --> 01:28:10.515
Um, on a per issue basis,

2004
01:28:10.515 --> 01:28:14.955
basically the stopping rule is you want to interleave STPA

2005
01:28:15.465 --> 01:28:17.635
with, uh, with engineering

2006
01:28:17.775 --> 01:28:19.835
and with, uh, your mitigation efforts.

2007
01:28:20.215 --> 01:28:23.555
So when STPA identifies an issue at a high level,

2008
01:28:23.975 --> 01:28:26.875
if you can eliminate that, if you can identify a,

2009
01:28:27.075 --> 01:28:29.635
a solution at a high level that completely eliminates it,

2010
01:28:30.135 --> 01:28:34.195
or a satisfactory, uh, uh, addresses it,

2011
01:28:34.625 --> 01:28:35.715
then you're done.

2012
01:28:35.895 --> 01:28:39.315
You don't need to examine in much more detail

2013
01:28:39.345 --> 01:28:40.595
that particular issue.

2014
01:28:40.595 --> 01:28:43.555
You can move on when you find an issue at a high level

2015
01:28:43.555 --> 01:28:46.035
that you cannot completely eliminate just

2016
01:28:46.035 --> 01:28:47.315
by making a simple little change.

2017
01:28:47.735 --> 01:28:51.435
That's your cue to iterate that issue in more detail

2018
01:28:51.435 --> 01:28:55.275
with STPA in the future, um, until you can get

2019
01:28:55.335 --> 01:28:56.795
to a solution that you can implement.

2020
01:28:56.795 --> 01:28:58.035
Okay. So

2021
01:29:00.125 --> 01:29:03.015
Can't tolerate, Yeah, interleave it with this.

2022
01:29:03.615 --> 01:29:05.495
STB is kind of the problem space.

2023
01:29:05.645 --> 01:29:09.175
Finding things that go wrong, you really need to interleave

2024
01:29:09.175 --> 01:29:10.895
that with a solution space, which,

2025
01:29:10.905 --> 01:29:14.535

which is providing requirements and recommendations and,

2026
01:29:14.535 --> 01:29:15.655
and actions to mitigate.

2027
01:29:15.915 --> 01:29:19.295
And that helps you identify, uh, what issues you need

2028
01:29:19.455 --> 01:29:22.455
to look more at and what issues are, uh,

2029
01:29:22.525 --> 01:29:23.535
have been addressed.

2030
01:29:25.475 --> 01:29:27.485
Alright, gentlemen, I think I have to, uh,

2031
01:29:27.665 --> 01:29:29.325
to wrap it there and give it back to our chairman.

2032
01:29:30.555 --> 01:29:31.885
It's, uh, I've been giving you two

2033
01:29:31.885 --> 01:29:35.325
and a half minutes, so, uh, thank you, John.

2034
01:29:35.325 --> 01:29:39.245
Thank you, Doug. They're, uh, really fabulous input

2035
01:29:39.345 --> 01:29:40.525
and, uh, a privilege for me

2036
01:29:40.525 --> 01:29:42.005
to get a chance to talk to you both.

2037
01:29:42.255 --> 01:29:43.255
Thank you.

2038
01:29:44.495 --> 01:29:47.605
Great job, Ben. And again, thank you, uh, Dr. Thomas

2039
01:29:47.905 --> 01:29:51.645
and Colonel Weer really captivating presentations,

2040
01:29:51.675 --> 01:29:52.725
thought provoking,

2041
01:29:53.065 --> 01:29:55.805
and I've just, uh, watching the questions coming in as well.

2042
01:29:56.345 --> 01:30:00.285
And I think I share, uh, probably sentiments of many

2043
01:30:00.285 --> 01:30:02.325
that are out there and that we're trying to

2044
01:30:03.105 --> 01:30:06.685
see in our own minds by how we, we overcome the headwinds.

2045
01:30:07.035 --> 01:30:10.085
Because as John made perfectly clear earlier in the program,

2046
01:30:10.985 --> 01:30:12.885
um, this is something that you need

2047
01:30:12.885 --> 01:30:15.685
to have some experience using in order for it

2048
01:30:15.685 --> 01:30:18.245
to unleash the real potentials.

2049
01:30:18.865 --> 01:30:23.765
Um, so I guess, uh, I'll leave you with just, uh, my hope

2050
01:30:23.765 --> 01:30:26.565
that maybe this provides a stimulus to try

2051
01:30:26.625 --> 01:30:28.965
to do some further research

2052
01:30:29.145 --> 01:30:32.525

and participate in the workshops that, uh, John offers

2053
01:30:32.945 --> 01:30:37.005
and, um, try to, uh, get smarter on STPA

2054
01:30:37.005 --> 01:30:38.925
and how it might apply to your operations.

2055
01:30:39.025 --> 01:30:42.205
But, um, uh, I think it's a very powerful tool

2056
01:30:42.425 --> 01:30:44.285
and, uh, hopefully this is providing some

2057
01:30:44.285 --> 01:30:45.405
incentive to look into it further.

2058
01:30:46.145 --> 01:30:48.445
Hey, Tom, can we mention, uh, the slides

2059
01:30:48.445 --> 01:30:50.525
that I gave are ready to post

2060
01:30:50.625 --> 01:30:54.485
and may may already be posted for folks Absolutely.

2061
01:30:54.485 --> 01:30:55.645
Who might go work on the homework.

2062
01:30:56.225 --> 01:30:59.485
Yep. So, if, if, uh, Susan would go to the next slide

2063
01:30:59.585 --> 01:31:01.125
for me, that's a great segue.

2064
01:31:01.255 --> 01:31:05.085
Thank you, John. Uh, so in addition to the homework, uh,

2065
01:31:05.085 --> 01:31:06.445
we're gonna post John's slides

2066
01:31:06.445 --> 01:31:08.405
because, uh, people have been asking, um,

2067
01:31:08.665 --> 01:31:09.965
if the slides are gonna be available,

2068
01:31:10.065 --> 01:31:13.805
and he's kindly allow that to happen in a convenient PDF.

2069
01:31:13.805 --> 01:31:17.325
And so we'll get that, um, posted to the website.

2070
01:31:17.545 --> 01:31:20.725
I'm not sure exactly which prob maybe under STPA resources,

2071
01:31:21.425 --> 01:31:25.685
uh, or under a 2020 flight test safety workshop repository.

2072
01:31:26.425 --> 01:31:28.175
So, uh, and,

2073
01:31:28.275 --> 01:31:30.735
and again, if you haven't downloaded the handout,

2074
01:31:30.875 --> 01:31:33.135
now is the time to do it in the last minute

2075
01:31:33.135 --> 01:31:34.175
before we close the webinar,

2076
01:31:34.485 --> 01:31:36.375
because once we close the webinar, then

2077
01:31:36.375 --> 01:31:37.855
that word document's no longer available.

2078
01:31:38.275 --> 01:31:41.615
And please, we're, this isn't about trying to be perfect

2079
01:31:41.765 --> 01:31:43.615

with the homework exercise, we're,

2080
01:31:43.615 --> 01:31:45.095
it's a self grading exercise.

2081
01:31:45.345 --> 01:31:46.975
We're here to do shared learning.

2082
01:31:47.515 --> 01:31:50.295
Uh, even if it's incomplete, we're not gonna grade it

2083
01:31:50.295 --> 01:31:51.575
as incomplete or complete.

2084
01:31:51.875 --> 01:31:53.175
Uh, just put something down,

2085
01:31:53.245 --> 01:31:55.295
even if you do it on a bar napkin later

2086
01:31:55.395 --> 01:31:57.775
and take a an iPhone picture of it

2087
01:31:57.995 --> 01:31:59.845
and email it into that, uh,

2088
01:31:59.845 --> 01:32:02.565
Google Drive repository, that's fine too.

2089
01:32:03.095 --> 01:32:05.325
We'll still consider you eligible for the Ralph

2090
01:32:05.545 --> 01:32:07.885
for some Starbucks coffee later on.

2091
01:32:08.425 --> 01:32:11.325
Um, further, I wanted to just make sure

2092
01:32:11.325 --> 01:32:12.365
that people understood

2093
01:32:12.365 --> 01:32:16.205
that the flight test safety.org website is your website

2094
01:32:16.985 --> 01:32:18.405
for flight test professionals.

2095
01:32:18.665 --> 01:32:20.885
And we go to great lengths of trying to host

2096
01:32:20.985 --> 01:32:23.885
as much information as we possibly can on this

2097
01:32:23.915 --> 01:32:25.245
website for your use.

2098
01:32:25.715 --> 01:32:29.365
Next chart, Susan. So each of the, the

2099
01:32:30.525 --> 01:32:32.045
workshops we video cast,

2100
01:32:32.225 --> 01:32:36.685
and if the presenters provide us the permissions to, uh,

2101
01:32:36.875 --> 01:32:39.765
host their video cast on the website, we do so.

2102
01:32:40.265 --> 01:32:42.165
So shortly after this event, uh,

2103
01:32:42.265 --> 01:32:44.805
we will host those recordings that we have.

2104
01:32:45.165 --> 01:32:46.685
'cause this is, this is being recorded.

2105
01:32:47.505 --> 01:32:49.805
Uh, we recently completed an airshow guide.

2106
01:32:49.805 --> 01:32:51.685

This is a very extensive document for those

2107
01:32:51.785 --> 01:32:53.925
who organizations that might find themselves

2108
01:32:54.575 --> 01:32:56.765
doing dynamic airshow work.

2109
01:32:57.025 --> 01:32:58.845
Uh, we understand that testers get tapped

2110
01:32:58.845 --> 01:32:59.885
to do this type of thing.

2111
01:33:00.465 --> 01:33:03.005
Um, so we went to the best in the business,

2112
01:33:03.065 --> 01:33:04.605
the most highly experienced guys

2113
01:33:05.145 --> 01:33:07.205
to critique our work on this airshow guide.

2114
01:33:07.275 --> 01:33:09.445
It's now available on the website.

2115
01:33:09.995 --> 01:33:12.965
There's, uh, tons of SMS resources.

2116
01:33:13.665 --> 01:33:16.285
Um, we also added some COVID-19 guides.

2117
01:33:16.285 --> 01:33:18.085
Now, these are just suggestions.

2118
01:33:18.705 --> 01:33:20.605
Um, every organization is different,

2119
01:33:20.605 --> 01:33:22.605
and we wanna make sure people are paying attention to

2120
01:33:22.605 --> 01:33:25.165
what the CDC and your local, state

2121
01:33:25.185 --> 01:33:28.365
and federal governments are, are putting in place.

2122
01:33:28.665 --> 01:33:31.085
But, um, these are some things that you may want

2123
01:33:31.085 --> 01:33:33.565
to consider if you're, if you're continuing operations,

2124
01:33:33.565 --> 01:33:36.325
maybe scaled back, maybe you've cease operations

2125
01:33:36.665 --> 01:33:37.885
and you're going to restart.

2126
01:33:38.075 --> 01:33:39.965
There's some information that's available to you.

2127
01:33:40.345 --> 01:33:41.445
And like I mentioned earlier,

2128
01:33:41.555 --> 01:33:44.165
there's a whole STPA resources tab in there

2129
01:33:44.165 --> 01:33:45.805
that includes the handbook.

2130
01:33:46.225 --> 01:33:49.165
Um, and I think I've included the March, 2018 version,

2131
01:33:49.165 --> 01:33:52.765
which John, I believe that is the most, uh, recent version.

2132
01:33:54.635 --> 01:33:57.295
Um, and there is more stuff on, on the website as well.

2133
01:33:57.355 --> 01:33:59.975

So I encourage everybody to go there and, uh, take a look.

2134
01:34:00.125 --> 01:34:04.945
Next slide, please. So we have not

2135
01:34:04.945 --> 01:34:06.865
pulled the plug on our European

2136
01:34:06.865 --> 01:34:08.185
Flight Test safety workshops.

2137
01:34:08.185 --> 01:34:09.225
So we are still scheduled

2138
01:34:09.225 --> 01:34:12.545
for mid-October in London at the Royal Aeronautical Society.

2139
01:34:12.565 --> 01:34:14.585
And the team that's putting this together is

2140
01:34:15.355 --> 01:34:18.785
going over the top with this event, um,

2141
01:34:19.405 --> 01:34:21.505
to include technical tours and social events.

2142
01:34:21.875 --> 01:34:24.745
Buckingham Palace, I heard is in the mix, um,

2143
01:34:25.945 --> 01:34:29.005
and some incredible aviation museum tours.

2144
01:34:29.745 --> 01:34:33.625
Uh, we're gonna do safety risk management is the theme.

2145
01:34:33.845 --> 01:34:35.505
Uh, the call for papers has gone out.

2146
01:34:35.555 --> 01:34:39.025
We're holding back on the registration until we have, um,

2147
01:34:39.525 --> 01:34:41.625
you know, better information, which to make a decision.

2148
01:34:41.685 --> 01:34:43.385
But like I mentioned in the beginning, uh,

2149
01:34:43.385 --> 01:34:45.225
we're not gonna put people safety at risk.

2150
01:34:45.325 --> 01:34:48.025
But, uh, we're currently continuing the planning

2151
01:34:48.165 --> 01:34:50.065
for an in-person workshop.

2152
01:34:50.445 --> 01:34:52.785
And we're also discussing whether we'll do a remote.

2153
01:34:52.965 --> 01:34:55.025
So in either case, we ask

2154
01:34:55.025 --> 01:34:57.205
that you at least block your calendars for the 14

2155
01:34:57.465 --> 01:34:58.685
to 16 timeframe.

2156
01:34:59.185 --> 01:35:02.045
Um, and we will make our decision on where we go from there.

2157
01:35:02.315 --> 01:35:02.885
Next chart,

2158
01:35:07.145 --> 01:35:08.925
We are going to be in Denver next year.

2159
01:35:09.265 --> 01:35:10.925
I'm gonna stay very confident.

2160
01:35:10.925 --> 01:35:12.285

We're gonna talk about safety promotion.

2161
01:35:12.285 --> 01:35:15.085
And by the way, what you're doing right now is safety

2162
01:35:15.085 --> 01:35:16.925
promotion, so you should take credit for it.

2163
01:35:17.345 --> 01:35:19.645
Um, boom Supersonic is still gonna be the host.

2164
01:35:20.105 --> 01:35:22.605
Um, they're getting very close to a flight test campaign,

2165
01:35:22.625 --> 01:35:24.965
so we're still hoping that they can accommodate us in the

2166
01:35:24.965 --> 01:35:27.765
same way that they were, uh, planning for this year.

2167
01:35:28.105 --> 01:35:30.325
But that's what we're, we're currently, uh, marching toward.

2168
01:35:30.355 --> 01:35:35.145
Next slide. Um,

2169
01:35:36.125 --> 01:35:37.465
I'm, I'm hoping that people are,

2170
01:35:37.645 --> 01:35:40.265
are seeing the Flight test Safety Fact newsletter.

2171
01:35:40.845 --> 01:35:42.505
We, we do put a lot of work into these.

2172
01:35:43.085 --> 01:35:47.425
Um, it's meant to be a forum to have opposing point of view,

2173
01:35:47.855 --> 01:35:50.705
talk about things that maybe are a little bit different.

2174
01:35:51.045 --> 01:35:52.905
Uh, we have talked about STPA in the past.

2175
01:35:53.645 --> 01:35:56.625
Uh, Mark Jones, I gotta throw major props his way

2176
01:35:57.085 --> 01:36:00.745
for being the incentive to get this, uh, off the ground.

2177
01:36:01.165 --> 01:36:03.625
And so we've been successful in having a flight test safety

2178
01:36:03.625 --> 01:36:06.265
fact newsletter every month this year so far.

2179
01:36:06.885 --> 01:36:09.825
Um, and really the credit is his, he just keeps pestering me

2180
01:36:09.825 --> 01:36:12.505
to do my Chairman's corner, which I really do

2181
01:36:12.505 --> 01:36:13.945
because I think it's that important.

2182
01:36:14.785 --> 01:36:18.105
A you have topics, you have subject that you would like

2183
01:36:18.105 --> 01:36:19.345
to see in this newsletter.

2184
01:36:19.655 --> 01:36:22.625
There's an email at the bottom of that thing that comes to,

2185
01:36:22.685 --> 01:36:26.905
to me, um, and we'll, we'll consider it, uh, turbo.

2186
01:36:26.905 --> 01:36:29.785
Thomasetti took the, the bull by the horns

2187
01:36:29.845 --> 01:36:32.345

and, uh, set up our podcasting effort.

2188
01:36:33.165 --> 01:36:34.425
So usually a week

2189
01:36:34.425 --> 01:36:36.785
after the issuance of our flight test safety fact,

2190
01:36:36.785 --> 01:36:40.425
at the beginning of every month, turbo Cuts a new podcast

2191
01:36:41.545 --> 01:36:43.705
covering some of the highlights in the, the newsletter,

2192
01:36:43.805 --> 01:36:44.865
and then some new content.

2193
01:36:45.525 --> 01:36:49.705
So we encourage people to, um, sign up for those podcasts.

2194
01:36:49.805 --> 01:36:53.665
And, you know, even earlier, I wasn't doing much in the way

2195
01:36:53.665 --> 01:36:57.785
of podcasting, but now I sign up for those, download 'em,

2196
01:36:57.785 --> 01:36:59.705
and then I just play 'em through my hands-free device

2197
01:36:59.705 --> 01:37:00.785
in the car on the way to work.

2198
01:37:01.285 --> 01:37:02.865
And I find that I don't get distracted,

2199
01:37:02.865 --> 01:37:05.305
but I still pay attention to what, what Turbo is, uh,

2200
01:37:05.765 --> 01:37:07.465
is preaching, which is all good stuff.

2201
01:37:07.975 --> 01:37:12.545
Next slide. So with that,

2202
01:37:12.925 --> 01:37:15.955
um, I wanted to just remind people

2203
01:37:15.955 --> 01:37:17.635
that we're gonna start at the same time

2204
01:37:18.375 --> 01:37:20.035
and same channel, uh, tomorrow.

2205
01:37:20.655 --> 01:37:22.435
Uh, you can use the same hot link.

2206
01:37:22.695 --> 01:37:24.275
So we encourage everybody to come in.

2207
01:37:24.355 --> 01:37:28.395
I think I noted that our high water mark was 390 attendees.

2208
01:37:29.575 --> 01:37:32.675
That's, that's amazing. We had 555 registered.

2209
01:37:32.755 --> 01:37:35.995
I believe the cap is at 500. So some people were waitlisted.

2210
01:37:35.995 --> 01:37:38.475
We hope those that were waitlisted, uh,

2211
01:37:38.475 --> 01:37:39.995
may have had opportunity to come on in.

2212
01:37:39.995 --> 01:37:42.875
But we look forward to everybody. Buddy, join us tomorrow.

2213
01:37:43.205 --> 01:37:44.875
We've got another impactful day

2214
01:37:44.905 --> 01:37:46.235

with some great presentations,

2215
01:37:46.615 --> 01:37:48.555
and I can't thank you enough for tuning in.

2216
01:37:48.975 --> 01:37:51.955
So with that, I wanna wish you all well, uh, I hope that,

2217
01:37:52.055 --> 01:37:53.875
uh, you, your families

2218
01:37:54.015 --> 01:37:57.255
and your organizational teammates are all staying healthy

2219
01:37:57.715 --> 01:37:59.295
and doing well with that.

2220
01:37:59.295 --> 01:37:59.775
Thanks again.