```
WEBVTT

1
00:00:01.315 --> 00:00:02.285
From Lucid Arrow.

2
00:00:02.875 --> 00:00:05.605
Noam is a, uh, has a degree in electrical, robotics

3
00:00:05.625 --> 00:00:06.925
and aerospace engineering.

4
00:00:07.555 --> 00:00:10.525
He's, uh, led a varied existence as aerospace engineer,

5
00:00:10.525 --> 00:00:12.565
project lead, ferry pilot flight instructor,

6
00:00:12.565 --> 00:00:14.925
maintenance test pilot, amongst other things.

7
00:00:15.035 --> 00:00:18.045
With this, uh, with flight experience in over 160 different

8
00:00:18.445 --> 00:00:21.325
aircraft types and engineering experience across a

9
00:00:21.325 --> 00:00:22.365
wide range of programs.

10
00:00:23.155 --> 00:00:25.885
He's, uh, real interested in the interplay between design,

11
00:00:25.885 --> 00:00:27.605
test, safety and human factors.

12
00:00:28.315 --> 00:00:31.325
Done some recent work at MIT focusing on bridging the gap

13
00:00:31.325 --> 00:00:33.965
between the industry and academia on flight test safety.
```

14
00:00:34.715 --> 00:00:38.965
What I'm really hoping is that he can explain it STPA so

15
00:00:38.965 --> 00:00:42.965
that even I can understand it, it's gonna give us a, uh,

16
00:00:42.965 --> 00:00:46.765
presentation on the introduction to STPA in a flight,

17
00:00:46.785 --> 00:00:48.685
in a test hazard management context.

18
00:00:51.945 --> 00:00:56.085
It Alright.

19
00:00:56.385 --> 00:00:58.685
Um, just so I can have a feel for the room.

20
00:00:59.915 --> 00:01:01.395
Everyone's heard of STPA

21
00:01:01.515 --> 00:01:02.835
'cause it was mentioned earlier today.

22
00:01:03.135 --> 00:01:05.715
Who, who's used? STPA.

23
00:01:08.195 --> 00:01:11.525
Okay. Who knows more

24
00:01:11.525 --> 00:01:13.445
or less maybe how it works,

25
00:01:13.545 --> 00:01:14.965
but has never had the opportunity.

26
00:01:17.055 --> 00:01:20.305
Okay. Is there anyone here who doesn't know how THA works?

27
00:01:21.995 --> 00:01:24.265

Great. That's what you like to hear. Okay.

28
00:01:24.685 --> 00:01:26.585
So we've, people of

29
00:01:26.585 --> 00:01:29.265
before me today have talked about complexity

30
00:01:29.605 --> 00:01:31.105
and the problems with it,

31
00:01:31.165 --> 00:01:34.385
and maybe some directions we can go

32
00:01:34.405 --> 00:01:35.785
and it's all kind of abstract.

33
00:01:35.805 --> 00:01:38.185
And my goal is to bring this all to Earth in a way

34
00:01:38.185 --> 00:01:40.265
that makes it actionable and usable.

35
00:01:41.165 --> 00:01:44.705
Um, and I like to motivate it with the, uh, Gulf Stream

36
00:01:45.235 --> 00:01:46.865
crash because it's one where

37
00:01:47.805 --> 00:01:50.265
the NTSB even concluded contributing

38
00:01:50.265 --> 00:01:51.865
to the accident was a failure to ensure

39
00:01:51.865 --> 00:01:54.345
that potential hazards have been fully identified.

40
00:01:54.885 --> 00:01:56.185
That's not a new problem.

41
00:01:56.285 --> 00:01:57.785
And we've talked about this problem.

42
00:01:57.965 --> 00:01:59.505
It goes all the way back to the beginning.

43
00:01:59.885 --> 00:02:03.225
Um, Wilbur Wright wrote to his father, um, that

44
00:02:03.225 --> 00:02:04.665
to keep the problem long enough

45
00:02:04.665 --> 00:02:06.105
to really learn anything positively,

46
00:02:06.105 --> 00:02:07.545
one must not take dangerous risks.

47
00:02:07.745 --> 00:02:10.425
Carelessness and overconfidence are usually more dangerous

48
00:02:10.425 --> 00:02:12.145
than deliberately accepted risks.

49
00:02:12.885 --> 00:02:16.025
And that right there is the whole key to test,

50
00:02:16.365 --> 00:02:17.545
uh, risk management.

51
00:02:19.245 --> 00:02:20.745
The process looks something like this.

52
00:02:21.285 --> 00:02:24.065
Uh, you identify hazards, you analyze them,

53
00:02:24.285 --> 00:02:26.225
you evaluate them, you mitigate them,

54
00:02:26.245 --> 00:02:28.865

and then you can decide if you accept them or, or not.

55
00:02:28.885 --> 00:02:30.985
And, you know, there's, there's twists and turns in there,

56
00:02:30.985 --> 00:02:32.665
but that's the overall process.

57
00:02:33.365 --> 00:02:35.545
As an industry. We've gotten quite good at

58
00:02:35.845 --> 00:02:36.985
the later parts of this.

59
00:02:37.235 --> 00:02:39.305
We're pretty good at analyzing, evaluating,

60
00:02:39.305 --> 00:02:40.905
mitigating, and deciding.

61
00:02:41.365 --> 00:02:42.865
But you can't do any of those things

62
00:02:43.085 --> 00:02:45.305
unless you've identified the hazards in the first place.

63
00:02:46.045 --> 00:02:49.545
And some of the ways we do that now fall down on the job.

64
00:02:50.765 --> 00:02:53.345
If you look at it another way, on the left,

65
00:02:53.365 --> 00:02:55.625
you have all the initial hazards in your whole program,

66
00:02:56.205 --> 00:02:58.785
and the goal is to identify all of them so

67
00:02:58.785 --> 00:03:00.805
that you can decide maybe they're unacceptable,

```
68
00:03:00.805 --> 00:03:01.805
you're gonna eliminate them.

69
00:03:02.485 --> 00:03:04.725
Unacceptable. You're gonna control them and,

70
00:03:04.905 --> 00:03:07.125
and accept the, the mitigated hazards.

71
00:03:07.715 --> 00:03:10.845
That use of the word control is the risk

72
00:03:11.135 --> 00:03:12.645
management use of the word.

73
00:03:12.645 --> 00:03:14.685
And I'm going to use that in a totally different

74
00:03:14.685 --> 00:03:16.165
way for everything else.

75
00:03:16.305 --> 00:03:19.445
So just be aware of that. Um, you might accept them.

76
00:03:20.665 --> 00:03:23.005
If you don't identify them though, that's

77
00:03:23.005 --> 00:03:24.605
where you end up with problems, right?

78
00:03:24.605 --> 00:03:26.645
These are your unknown unknowns and they bite.

79
00:03:28.875 --> 00:03:30.165
Okay, how do we do it right now?

80
00:03:30.385 --> 00:03:32.045
We get a bunch of experts in a room together

81
00:03:32.465 --> 00:03:34.805
```

and we say, imagine all the things

82
00:03:34.805 --> 00:03:36.325
that could go wrong with this program.

83
00:03:36.415 --> 00:03:39.045
Think about other programs you've been on that are similar

84
00:03:39.265 --> 00:03:41.965
and, you know, lean on that experience and, and,

85
00:03:42.105 --> 00:03:43.765
and what could be wrong here?

86
00:03:44.185 --> 00:03:47.285
Or we will copy and paste a previous program and revise

87
00:03:47.705 --> 00:03:51.245
and you end up in a situation with, uh, you know,

88
00:03:51.345 --> 00:03:52.605
spotty coverage of hazards.

89
00:03:52.605 --> 00:03:54.725
You have no way of knowing whether you've found them all.

90
00:03:55.945 --> 00:03:59.365
Um, depending who shows up on any given day to the meeting

91
00:03:59.425 --> 00:04:01.765
or who's part of that team, it can change

92
00:04:01.765 --> 00:04:03.525
what hazards you manage to identify.

93
00:04:04.555 --> 00:04:07.405
There's no framework that unifies this whole thing.

94
00:04:07.645 --> 00:04:09.285
Everyone uses the mental model in their own head

95
00:04:09.665 --> 00:04:12.485
and comes up with, as you know, the best they can,

96
00:04:12.705 --> 00:04:16.125
but sometimes hard to talk across disciplines or whatever.

97
00:04:16.325 --> 00:04:17.605
'cause you imagine it differently

98
00:04:18.385 --> 00:04:21.045
and it's extremely susceptible to novelty.

99
00:04:22.435 --> 00:04:26.175
It relies on our prior experience with quote similar, right?

100
00:04:26.675 --> 00:04:29.855
Uh, programs and complexity.

101
00:04:31.045 --> 00:04:33.475
Complexity is something people have talked about a bunch.

102
00:04:33.585 --> 00:04:34.995
I'll talk about it more in a second.

103
00:04:35.055 --> 00:04:38.435
But complexity can very easily put you in novelty

104
00:04:39.265 --> 00:04:40.855
maybe without even realizing it.

105
00:04:41.885 --> 00:04:45.775
There's kind of four big, uh, aspects of complexity.

106
00:04:46.275 --> 00:04:49.255
One is emergence. So the overall behavior

107
00:04:49.315 --> 00:04:52.695
of your system is not necessarily readily predictable

108
00:04:52.715 --> 00:04:55.935

by decompositional analysis of its constituent parts.

109
00:04:56.655 --> 00:04:59.055
I give you a car and a driver

110
00:04:59.195 --> 00:05:00.655
and I say, here's how they drive.

111
00:05:01.395 --> 00:05:03.415
And then I say, okay, put a bunch of them on the highway.

112
00:05:04.475 --> 00:05:07.175
Can you tell me that the traffic is gonna develop with this,

113
00:05:07.475 --> 00:05:11.975
uh, like wave, uh, pressure wave that flows backwards

114
00:05:12.865 --> 00:05:14.055
maybe in a simulation,

115
00:05:14.155 --> 00:05:16.815
but not, not just by thinking about it, right?

116
00:05:16.815 --> 00:05:18.775
That's an emergent property of the system.

117
00:05:20.745 --> 00:05:21.775
Non-linear behavior.

118
00:05:22.715 --> 00:05:25.335
You have pieces tied together all sorts of different ways,

119
00:05:25.835 --> 00:05:27.935
and the interaction amongst the elements

120
00:05:28.135 --> 00:05:30.975
of the system produce behaviors that are way more complex

121
00:05:31.605 --> 00:05:35.215
than the events that initiated the the behavior, right?

122
00:05:35.595 --> 00:05:38.055
You may also end up with time varying behaviors

123
00:05:38.055 --> 00:05:39.095
and non-determinism.

124
00:05:39.675 --> 00:05:43.415
Um, and this isn't non-linear, like you have a curve

125
00:05:43.415 --> 00:05:44.655
and it's not straight, right?

126
00:05:44.655 --> 00:05:47.775
You can represent that curve as a linear sum

127
00:05:47.775 --> 00:05:49.215
of curved basis elements.

128
00:05:49.215 --> 00:05:50.375
This is like non-linear.

129
00:05:50.375 --> 00:05:52.335
Like we don't really even know we're

130
00:05:52.335 --> 00:05:53.815
extrapolating so far away.

131
00:05:53.815 --> 00:05:57.285
We, we can't tell sensitivity to changes.

132
00:05:57.355 --> 00:05:59.405
This is where the novelty can really get you.

133
00:05:59.595 --> 00:06:02.845
Even tiny changes in the design of some little piece

134
00:06:02.845 --> 00:06:05.965
of a system can change the entire behavior

135
00:06:06.025 --> 00:06:09.365

of the system overall sometimes for the, for the worse.

136
00:06:10.225 --> 00:06:12.485
Um, and non failure hazards, right?

137
00:06:12.485 --> 00:06:14.645
We're quite good at saying, okay, what if this piece fails?

138
00:06:14.645 --> 00:06:16.445
What if that piece fails? What if that piece fails?

139
00:06:16.825 --> 00:06:19.325
You can have systems, especially where they involve software

140
00:06:19.425 --> 00:06:21.725
or people or you know, organizations.

141
00:06:22.785 --> 00:06:25.885
You can have systems where every single piece operates

142
00:06:25.915 --> 00:06:29.605
exactly as designed and you still get a bad outcome.

143
00:06:30.975 --> 00:06:34.335
Okay, what can we do about it?

144
00:06:35.115 --> 00:06:36.135
And I wanna back up

145
00:06:36.675 --> 00:06:38.975
and start from a more useful accident model.

146
00:06:39.125 --> 00:06:42.135
Overall, if we know how you have an accident,

147
00:06:42.135 --> 00:06:44.095
maybe we can know how to not have an accident.

148
00:06:45.185 --> 00:06:47.295
We're used to thinking linearly, dominoes,

```
149
00:06:47.295 --> 00:06:49.415
they fall on each other, this cascade of events.

150
00:06:49.475 --> 00:06:50.975
And next thing you know, you have an accident.

151
00:06:52.355 --> 00:06:53.415
In retrospect, fine,

152
00:06:53.415 --> 00:06:55.535
we can tell ourselves a nice story in prospect,

153
00:06:55.535 --> 00:06:56.575
where are the dominoes

154
00:06:56.915 --> 00:06:58.575
and which ones fall on which other ones

155
00:06:58.575 --> 00:07:01.135
and what are the outcomes not super useful.

156
00:07:02.965 --> 00:07:04.935
Similarly, we have an accident, the idea

157
00:07:04.935 --> 00:07:08.655
of an accident chain and like day of, you know,

158
00:07:08.915 --> 00:07:12.055
in in the air you can say, okay, I'm three links in.

159
00:07:12.055 --> 00:07:14.055
It's usually seven links. It's time to knock it off.

160
00:07:14.115 --> 00:07:17.135
But in prospect, I can give you a system

161
00:07:17.135 --> 00:07:18.375
and say, where's the chain?

162
00:07:18.585 --> 00:07:23.435
```

Right? Okay. So we say, okay, it's this bigger thing.

163
00:07:23.645 --> 00:07:25.475
Swiss cheese, lots of layers.

164
00:07:26.375 --> 00:07:28.105
There's holes when they line up

165
00:07:28.105 --> 00:07:30.385
and the latent failure goes through all the holes.

166
00:07:30.765 --> 00:07:34.585
You get an accident, which is a nice concept for maybe how

167
00:07:34.585 --> 00:07:36.425
to imagine something.

168
00:07:36.845 --> 00:07:39.385
But where are the holes? How big are they?

169
00:07:39.445 --> 00:07:41.705
How do they align? And what are the latent hazards?

170
00:07:41.705 --> 00:07:43.385
Like, tell me in prospect what,

171
00:07:43.385 --> 00:07:44.585
what's gonna happen with the system.

172
00:07:46.885 --> 00:07:50.065
We know aviation is a big social sociotechnical system.

173
00:07:50.085 --> 00:07:53.065
We have technology, we have, you know, hardware and people

174
00:07:53.325 --> 00:07:55.865
and procedures and all of these things,

175
00:07:55.865 --> 00:07:57.505
and they all come together to hopefully

176
00:07:57.505 --> 00:07:59.025
produce a safe outcome.

177
00:07:59.765 --> 00:08:00.985
How do we tie that all together?

178
00:08:01.845 --> 00:08:03.425
And that's where systems theory comes in.

179
00:08:03.765 --> 00:08:08.265
So if I give you this ball of string, I give you a string

180
00:08:08.265 --> 00:08:09.385
and I let you play with it,

181
00:08:09.605 --> 00:08:11.145
and we put them together into a ball,

182
00:08:11.685 --> 00:08:13.425
and I ask you, okay, I'm gonna toss the ball.

183
00:08:13.445 --> 00:08:17.675
How high will it bounce? Who knows, right?

184
00:08:18.365 --> 00:08:20.155
Again, decompositional analysis,

185
00:08:20.215 --> 00:08:24.235
but instead we can structure it in a way

186
00:08:24.235 --> 00:08:26.955
that we can consider the whole system as a whole, not just

187
00:08:27.335 --> 00:08:29.075
as the parts put together.

188
00:08:30.055 --> 00:08:33.715
We can find out its emergent properties, right?

189
00:08:33.775 --> 00:08:35.875

The things that happen from the interactions among them.

190
00:08:36.535 --> 00:08:40.275
And we can capture this holistic, non-linear system

191
00:08:41.175 --> 00:08:42.395
as a coherent way of thinking.

192
00:08:44.885 --> 00:08:46.075
Stamp the system.

193
00:08:46.075 --> 00:08:49.195
Theoretic accident model and process is where that comes in.

194
00:08:49.295 --> 00:08:51.755
We can take these things and we can structure them.

195
00:08:52.775 --> 00:08:54.515
And now we're back in engineering land

196
00:08:54.775 --> 00:08:55.845
and we're all happy again.

197
00:08:55.845 --> 00:08:58.685
We can take a big, big deep breath sigh of relief,

198
00:08:59.065 --> 00:09:00.765
and we have new tools that we can use.

199
00:09:03.105 --> 00:09:06.255
First we're gonna say an accident

200
00:09:07.475 --> 00:09:09.735
is when the system behavior as a whole, right?

201
00:09:09.915 --> 00:09:11.695
All of everything that happens in the system, the,

202
00:09:11.755 --> 00:09:12.775
the emergent behavior

203
00:09:12.775 --> 00:09:16.895
of the system is unsafe in the context, right?

204
00:09:16.965 --> 00:09:19.215
It's not unsafe for an airplane

205
00:09:19.315 --> 00:09:22.375
to make a rapid descent if you're high,

206
00:09:22.755 --> 00:09:24.855
it is quite unsafe if the context is

207
00:09:24.855 --> 00:09:26.375
that we're right next to the ground to begin with.

208
00:09:26.675 --> 00:09:31.565
So context matters and then we can look inside the system

209
00:09:32.225 --> 00:09:36.005
and capture all of the behaviors that happen on the inside

210
00:09:36.065 --> 00:09:38.365
to figure out how could it cause the bad

211
00:09:38.365 --> 00:09:39.405
events on the outside.

212
00:09:40.585 --> 00:09:43.525
So I'm gonna take our risk management process

213
00:09:44.105 --> 00:09:48.005
and I'm gonna pre-end a step, understand the system.

214
00:09:48.435 --> 00:09:51.485
This starts to give us a framework, right?

215
00:09:51.915 --> 00:09:53.045
This is now our first step.

216
00:09:53.045 --> 00:09:56.985

Understand it and identify the hazards. Okay?

217
00:09:57.435 --> 00:09:59.665
Stamp thinks in terms of control.

218
00:09:59.685 --> 00:10:02.665
And this is control like flight controls,

219
00:10:02.665 --> 00:10:05.385
like applying control to something to make it do something.

220
00:10:06.165 --> 00:10:08.465
You have a controller, it has

221
00:10:09.265 --> 00:10:11.185
a control algorithm and a process model.

222
00:10:11.205 --> 00:10:13.385
The process model is what does it think is going on.

223
00:10:13.525 --> 00:10:15.745
And the control algorithm is what should I do about it?

224
00:10:16.245 --> 00:10:20.905
And it issues control actions to some controlled process,

225
00:10:21.275 --> 00:10:23.545
takes the control actions does whatever it does,

226
00:10:23.565 --> 00:10:24.905
it might be an airplane and it flies

227
00:10:24.905 --> 00:10:26.785
or who knows some piece of the system

228
00:10:27.685 --> 00:10:31.985
and it's gonna give feedback together.

229
00:10:32.485 --> 00:10:36.225
You can end up with a control loop. Okay? That's two pieces.

230
00:10:36.485 --> 00:10:37.545
Put in a bigger system.

231
00:10:37.965 --> 00:10:40.745
Now you can look at every set of pieces

232
00:10:41.125 --> 00:10:42.345
and what they might do together.

233
00:10:42.345 --> 00:10:44.065
And you can start to trace control loops

234
00:10:44.535 --> 00:10:47.225
that don't necessarily go through just two pieces, right?

235
00:10:47.225 --> 00:10:49.985
There's a small one, there's a bigger one,

236
00:10:50.005 --> 00:10:51.105
and you can start to look at

237
00:10:51.105 --> 00:10:52.585
what the system does as a whole.

238
00:10:53.395 --> 00:10:56.345
Great. When does that go bad?

239
00:10:57.925 --> 00:10:59.305
We look at the control actions

240
00:10:59.655 --> 00:11:01.305
that the controllers can issue

241
00:11:01.805 --> 00:11:06.705
and we say, under what conditions would it be unsafe to,

242
00:11:06.965 --> 00:11:08.825
to make given control actions?

243
00:11:09.005 --> 00:11:11.345

And there's kind of four archetypes under what, uh,

244
00:11:11.345 --> 00:11:13.425
conditions would it be unsafe to give

245
00:11:14.025 --> 00:11:17.325
x control action under what conditions?

246
00:11:17.385 --> 00:11:19.245
To not give x control action

247
00:11:19.245 --> 00:11:21.405
that should have been given too early, too late, too long,

248
00:11:21.405 --> 00:11:23.325
too short, oops.

249
00:11:23.465 --> 00:11:26.005
And you start to put this together.

250
00:11:26.185 --> 00:11:27.925
So like I said earlier,

251
00:11:28.945 --> 00:11:32.205
to provide a pitch down control, right?

252
00:11:33.775 --> 00:11:35.725
Under what context is that unsafe?

253
00:11:35.905 --> 00:11:37.205
If you're near the ground, under

254
00:11:37.205 --> 00:11:38.605
what context would it be unsafe

255
00:11:38.605 --> 00:11:40.405
to not give a pitch down control?

256
00:11:40.705 --> 00:11:42.245
Say you're approaching stall, right?

257
00:11:43.845 --> 00:11:48.345
In other conditions though, you had better issue the the

258
00:11:49.085 --> 00:11:50.705
or better not issue the the pitch

259
00:11:50.705 --> 00:11:51.865
down if you're near the ground, right?

260
00:11:51.885 --> 00:11:53.645
So it depends on the context.

261
00:11:55.465 --> 00:11:56.605
We take each of those

262
00:11:57.225 --> 00:11:58.565
and we can now create

263
00:11:58.955 --> 00:12:01.205
what people call ucas unsafe control actions

264
00:12:01.205 --> 00:12:03.005
or yuca as Boeing likes to call them.

265
00:12:03.545 --> 00:12:06.725
Um, and you can structure them in terms of these five pieces

266
00:12:07.425 --> 00:12:09.085
you have, who's the controller?

267
00:12:09.085 --> 00:12:10.125
The source, right?

268
00:12:10.145 --> 00:12:13.165
In this case, in the, this is an example, the flight crew.

269
00:12:14.645 --> 00:12:17.785
The type provides not provide early, late, et cetera.

270
00:12:18.805 --> 00:12:21.345

The control action in this example, autopilot,

271
00:12:21.345 --> 00:12:23.145
disengage under a context.

272
00:12:23.295 --> 00:12:25.745
When you're relying on the autopilot, it would be unsafe

273
00:12:25.965 --> 00:12:28.025
to disengage the autopilot when you're relying on the

274
00:12:28.025 --> 00:12:30.985
autopilot and the last bit traces it back to a hazard.

275
00:12:31.125 --> 00:12:32.545
So you know what, what you're

276
00:12:32.735 --> 00:12:34.225
worried about in the first place.

277
00:12:35.285 --> 00:12:38.225
Um, then you can take each of those

278
00:12:38.845 --> 00:12:41.025
and you can say, okay, how could this happen?

279
00:12:42.745 --> 00:12:43.745
Multiple ways for each one.

280
00:12:44.125 --> 00:12:46.025
For example, while the airplanes near the ground,

281
00:12:46.025 --> 00:12:48.825
the flight crew accidentally bumps the yoke forward

282
00:12:48.975 --> 00:12:51.065
with sufficient force to disengage the autopilot,

283
00:12:51.565 --> 00:12:54.025
but doesn't notice that the autopilot has disengaged.

284
00:12:54.445 --> 00:12:55.985
The forward bump causes a descent,

285
00:12:55.995 --> 00:12:57.745
which the flight crew does not notice.

286
00:12:57.885 --> 00:12:59.625
And the airplane impacts the ground, right?

287
00:12:59.695 --> 00:13:03.905
Eastern Airlines, uh, Everglades crash. That's one way.

288
00:13:04.855 --> 00:13:06.425
There's probably many others,

289
00:13:06.445 --> 00:13:08.545
but now you have a way to think about them.

290
00:13:09.575 --> 00:13:12.145
When under what context does this UCA happen?

291
00:13:12.325 --> 00:13:13.905
How does it happen? How could it happen?

292
00:13:14.565 --> 00:13:17.785
And you end up with a very context rich, uh, you know,

293
00:13:17.785 --> 00:13:19.585
hazard description cause causality

294
00:13:20.685 --> 00:13:22.105
and it's not necessarily linear.

295
00:13:24.015 --> 00:13:27.185
Okay? Now we wanna put this into practice.

296
00:13:28.725 --> 00:13:30.265
That's where A CPA comes in.

297
00:13:31.765 --> 00:13:34.305

And I'm gonna walk you through, I'll,

298
00:13:34.305 --> 00:13:35.225
I'll give you an overview of

299
00:13:35.225 --> 00:13:36.305
the process, A four step process.

300
00:13:36.355 --> 00:13:38.785
We're gonna look at each step for flight tests,

301
00:13:38.785 --> 00:13:40.425
and we're gonna try to understand then

302
00:13:40.445 --> 00:13:42.905
how it fits into flight test risk management.

303
00:13:43.615 --> 00:13:46.835
Okay? Step one, the easy part,

304
00:13:46.835 --> 00:13:48.555
we're gonna define our hazards and our loss,

305
00:13:48.575 --> 00:13:49.675
or sorry, our losers first,

306
00:13:49.695 --> 00:13:53.835
and then our hazards top level, uh, you know, impact

307
00:13:53.835 --> 00:13:54.955
with the ground, impact with

308
00:13:54.955 --> 00:13:56.235
another aircraft, those kinds of things.

309
00:13:56.775 --> 00:13:59.155
And we're gonna a little harder to do. Define the system.

310
00:13:59.305 --> 00:14:01.475
What is inside our system? What are we considering?

311
00:14:01.475 --> 00:14:04.875
Is it the, the crew and the aircraft only maybe?

312
00:14:05.495 --> 00:14:06.635
And everything outside of

313
00:14:06.635 --> 00:14:08.275
that we're gonna say is the environment.

314
00:14:08.575 --> 00:14:10.035
And that goes into the context.

315
00:14:10.175 --> 00:14:11.915
But we have to be very structured about

316
00:14:11.985 --> 00:14:14.155
what we're gonna care about and what we're gonna leave out.

317
00:14:15.005 --> 00:14:16.915
We're gonna model it as a control structure,

318
00:14:16.935 --> 00:14:17.995
and I'll talk about that more.

319
00:14:18.765 --> 00:14:21.115
We're gonna identify all of the ucas

320
00:14:22.055 --> 00:14:24.755
and all of their scenarios, okay?

321
00:14:24.815 --> 00:14:27.235
So, oh yeah, I'll point out.

322
00:14:27.295 --> 00:14:30.115
So this is for STPA is for prospective, right?

323
00:14:30.115 --> 00:14:34.075
Future things cast helps you apply a similar methodology

324
00:14:34.135 --> 00:14:35.395

to look at accidents

325
00:14:35.395 --> 00:14:36.955
and learn more than, than you might have before.

326
00:14:37.785 --> 00:14:41.115
Okay? Define the system boundary.

327
00:14:41.345 --> 00:14:43.715
Keep the scope within reason STPA can grow.

328
00:14:43.715 --> 00:14:45.595
You can boil the ocean very quickly or,

329
00:14:45.695 --> 00:14:48.075
or, uh, shave the yak as people like to say, right?

330
00:14:48.245 --> 00:14:51.925
Start small, start abstract, um, list the components

331
00:14:51.925 --> 00:14:53.365
that you need and then figure out how

332
00:14:53.365 --> 00:14:54.405
to include them in the system.

333
00:14:55.185 --> 00:14:58.285
Um, test techniques will play more into the context.

334
00:14:59.155 --> 00:15:03.405
Here is a, a control structure of, you know,

335
00:15:03.645 --> 00:15:06.165
everyone present on a kind of maybe typical day of test,

336
00:15:06.695 --> 00:15:08.925
we're gonna cut out a little piece of that maybe

337
00:15:08.945 --> 00:15:12.005
and just say it's the crew in the aircraft, okay?

338
00:15:12.025 --> 00:15:13.325
And then we're gonna define our losses.

339
00:15:13.585 --> 00:15:15.845
Things like, you know, standard things, injury, loss

340
00:15:15.845 --> 00:15:18.565
of life damage, um, et cetera.

341
00:15:20.185 --> 00:15:22.965
If you want, you can also include while you're doing this

342
00:15:23.205 --> 00:15:25.125
analysis, some further losses.

343
00:15:25.185 --> 00:15:28.325
Things like incorrect, uh, incorrect, corrupted,

344
00:15:28.325 --> 00:15:31.565
missing data, loss of trust, those kinds of things.

345
00:15:31.565 --> 00:15:32.965
They can be losses just the same.

346
00:15:32.985 --> 00:15:35.725
And you can work them all into the same analysis.

347
00:15:35.725 --> 00:15:39.085
Once you're already at it from those, you end up

348
00:15:39.085 --> 00:15:40.685
with some top level hazards.

349
00:15:41.185 --> 00:15:43.205
Things like aircraft gets too close to terrain

350
00:15:43.205 --> 00:15:44.925
or obstacles, aircraft gets close too close

351
00:15:44.925 --> 00:15:48.405

to other aircraft, and afterwards in parentheses are linked

352
00:15:48.405 --> 00:15:50.725
to the losses that these hazards could cause.

353
00:15:50.985 --> 00:15:53.845
And so you can trace everything backwards once you're done.

354
00:15:55.635 --> 00:15:57.925
Okay? Then you're gonna model it as a control structure.

355
00:15:58.545 --> 00:16:03.005
The idea here control the, the arrows are not wires

356
00:16:03.105 --> 00:16:06.245
and control is not what bits of data are going through.

357
00:16:07.665 --> 00:16:11.325
The, the arrows are exercise, like show

358
00:16:11.475 --> 00:16:14.085
what can exercise control or give feedback to what.

359
00:16:14.745 --> 00:16:17.085
And the information that goes in them is control

360
00:16:17.085 --> 00:16:18.285
actions or feedback.

361
00:16:18.285 --> 00:16:20.405
What am I commanding? Not how am I doing it?

362
00:16:20.425 --> 00:16:22.965
Not why, what why is it going through? What am I commanding?

363
00:16:23.025 --> 00:16:24.845
Am I commanding a pitch down or a pitch up?

364
00:16:24.845 --> 00:16:27.845
Those kinds of things. And you're gonna structure it from

365
00:16:27.865 --> 00:16:31.405
top to bottom, um, in an uh, hierarchical way.

366
00:16:31.955 --> 00:16:34.005
Sometimes you'll end up with things next to each other

367
00:16:34.025 --> 00:16:35.965
or things that flow backwards, but you're gonna do your best

368
00:16:35.985 --> 00:16:38.325
to kind of go from high level authority down to the bottom

369
00:16:39.225 --> 00:16:40.685
and you can do things like that.

370
00:16:40.875 --> 00:16:42.405
That dashed box, right?

371
00:16:42.505 --> 00:16:44.205
For now we're gonna say aircraft automation.

372
00:16:44.495 --> 00:16:45.885
Maybe we'll dig into it later,

373
00:16:46.065 --> 00:16:47.645
but you can stay abstract for now.

374
00:16:48.105 --> 00:16:50.125
And you're gonna list the control actions

375
00:16:50.125 --> 00:16:53.245
and the feedbacks in, in broad generalities.

376
00:16:54.515 --> 00:16:56.845
Okay? Start abstract and then drill in.

377
00:16:57.545 --> 00:17:02.285
And for each controller, now we can say, what are all

378
00:17:02.285 --> 00:17:04.165

of its control actions that it can issue?

379
00:17:05.105 --> 00:17:07.165
And then we can go find ucas, right?

380
00:17:07.835 --> 00:17:11.285
When could each possibly be wrong? Okay?

381
00:17:11.285 --> 00:17:13.525
You're gonna end up with a table for each control action.

382
00:17:13.745 --> 00:17:15.565
On the left, you have four archetypes.

383
00:17:16.475 --> 00:17:19.325
Provide, not provide too early, too late, et cetera.

384
00:17:19.985 --> 00:17:23.565
For each one of those, you can come up with a list of ucas.

385
00:17:23.905 --> 00:17:25.965
It is unsafe to not provide

386
00:17:26.105 --> 00:17:27.645
for the crew not to provide action.

387
00:17:27.745 --> 00:17:31.805
One under this condition, under that condition, right?

388
00:17:31.805 --> 00:17:34.805
Those are all the different contexts from each UCA.

389
00:17:34.865 --> 00:17:38.965
Now you can create a list of scenarios, all the ways

390
00:17:38.965 --> 00:17:40.485
that you can think of that happening.

391
00:17:42.575 --> 00:17:45.235
Now, this is like some weird high dimensional table,

392
00:17:45.375 --> 00:17:48.555
and it's nicer maybe to think of it as a tree,

393
00:17:49.055 --> 00:17:51.965
which you can, and I've only filled out just

394
00:17:52.065 --> 00:17:53.085
so the system at the top.

395
00:17:53.085 --> 00:17:54.245
You have all the parts of the system.

396
00:17:54.355 --> 00:17:56.685
I've only filled out the leftmost branch,

397
00:17:56.745 --> 00:17:57.925
but you can have, you know,

398
00:17:57.925 --> 00:17:59.765
you'll have equivalent branches for everything, right?

399
00:17:59.795 --> 00:18:02.845
I've filled out only part A control action,

400
00:18:02.965 --> 00:18:05.445
A one provide, et cetera.

401
00:18:05.465 --> 00:18:07.965
But you'll have a full tree and you can trace it.

402
00:18:08.205 --> 00:18:09.845
Everything's also tagged

403
00:18:09.955 --> 00:18:12.325
with its respective hazards and losses.

404
00:18:13.385 --> 00:18:16.605
So you can kind of slice the tree a different direction and,

405
00:18:16.625 --> 00:18:18.125

and look at it that way if you want to.

406
00:18:20.435 --> 00:18:22.405
Okay? How does this relate?

407
00:18:23.185 --> 00:18:27.005
If you want to, you can think of this UCA table

408
00:18:27.225 --> 00:18:29.885
as guiding you into all of the branches

409
00:18:29.885 --> 00:18:31.325
of possibility of the system.

410
00:18:31.465 --> 00:18:33.725
And within each one you can do your brainstorming

411
00:18:33.985 --> 00:18:37.445
and that works and that helps you cover your bases.

412
00:18:37.895 --> 00:18:40.045
There are more structured ways to do this,

413
00:18:40.625 --> 00:18:43.085
and I can, I can point people to them if they're interested.

414
00:18:43.585 --> 00:18:47.085
Um, but it helps you achieve the coverage

415
00:18:47.085 --> 00:18:48.085
that you're looking to achieve.

416
00:18:50.285 --> 00:18:54.775
Okay? So in the context of flight test risk management,

417
00:18:57.015 --> 00:18:59.295
STPA essentially helps you understand the system,

418
00:19:00.255 --> 00:19:01.935
identify your hazards, and analyze them, right?

419
00:19:01.935 --> 00:19:03.975
It gives you back this rich context.

420
00:19:04.195 --> 00:19:06.095
And those are the four steps of STPA.

421
00:19:06.425 --> 00:19:10.055
Let's look at it a different way. THA spits out six pieces.

422
00:19:10.885 --> 00:19:12.655
Hazards their causes effects.

423
00:19:12.655 --> 00:19:14.735
Mitigations, recoveries risk assessment.

424
00:19:15.975 --> 00:19:18.055
STPA gives you the first three.

425
00:19:18.325 --> 00:19:20.175
Your loss scenarios give you a hazard

426
00:19:20.175 --> 00:19:21.855
with its causes and its effects.

427
00:19:23.775 --> 00:19:26.355
The next two, it gives you much more

428
00:19:26.355 --> 00:19:27.515
insight than you would have.

429
00:19:27.695 --> 00:19:32.315
You have a scenario now that says, you know, this piece

430
00:19:32.315 --> 00:19:33.795
of the system acts in this way,

431
00:19:33.795 --> 00:19:35.515
under this context, et cetera, et cetera.

432
00:19:35.515 --> 00:19:38.515

You have so many places to intervene for your mitigations.

433
00:19:39.155 --> 00:19:41.875
Likewise for recovery, you know a lot of things about

434
00:19:41.875 --> 00:19:43.515
what needs to be undone.

435
00:19:44.215 --> 00:19:47.355
The risk assessment has whatever issues you can use.

436
00:19:47.355 --> 00:19:48.435
Your your 2D matrix,

437
00:19:48.465 --> 00:19:50.555
your 3D matrix, whatever, whatever you want.

438
00:19:50.585 --> 00:19:53.555
It's gonna have the same shortcomings of, of

439
00:19:53.555 --> 00:19:54.555
however we currently do it,

440
00:19:54.555 --> 00:19:55.835
but we at least know how to do it

441
00:19:55.835 --> 00:19:57.035
and we're comfortable with something.

442
00:19:57.035 --> 00:20:01.955
And so we can just drop STPA into this, uh, framework

443
00:20:01.955 --> 00:20:03.115
that, that we're used to.

444
00:20:05.495 --> 00:20:09.185
Okay, there is, I, I wrote a thesis about all of this.

445
00:20:09.185 --> 00:20:11.545
There's more there. Um, there's a link at the bottom.

446
00:20:11.695 --> 00:20:13.025
It's on, on my website.

447
00:20:13.365 --> 00:20:15.825
If you read it, even if it's only in part,

448
00:20:16.025 --> 00:20:17.025
I would love your feedback.

449
00:20:17.095 --> 00:20:20.985
What parts are informative, insightful, helpful to know

450
00:20:20.985 --> 00:20:22.185
what parts are confusing.

451
00:20:23.065 --> 00:20:26.385
I would like to turn this into a pretty short handbook,

452
00:20:26.385 --> 00:20:27.385
guidebook, intro.

453
00:20:27.625 --> 00:20:30.385
STPA for flight testers talks about

454
00:20:30.385 --> 00:20:31.505
it in the language of flight test.

455
00:20:31.625 --> 00:20:32.865
'cause I did a lot of work pulling it out

456
00:20:32.865 --> 00:20:34.865
of academia into our language.

457
00:20:35.565 --> 00:20:38.905
Um, and I would love your feedback so that I can help steer

458
00:20:39.135 --> 00:20:40.945
that in a, in a useful direction.

459
00:20:42.165 --> 00:20:46.025

Um, I believe STPA

460
00:20:46.565 --> 00:20:49.405
can help us achieve safer flight tests

461
00:20:49.545 --> 00:20:51.245
by better identifying hazards.

462
00:20:51.785 --> 00:20:54.245
It gives us a bunch of additional benefits on the side.

463
00:20:55.145 --> 00:20:57.885
Um, and I am happy to take whatever questions.

464
00:20:58.005 --> 00:21:01.465
I think I've left myself five minutes for that. Yeah,

465
00:21:05.275 --> 00:21:06.785
Thank you for the presentation.

466
00:21:06.975 --> 00:21:09.145
Very, uh, it's very thorough.

467
00:21:10.045 --> 00:21:12.465
The process itself is certainly very

468
00:21:12.625 --> 00:21:14.305
thorough, which is great.

469
00:21:14.925 --> 00:21:17.105
Um, but I feel it also

470
00:21:17.105 --> 00:21:21.145
because of how thorough it is, it can get very overwhelming,

471
00:21:21.775 --> 00:21:24.665
very fast and very exponentially.

472
00:21:24.925 --> 00:21:27.945
Uh, you only showed the left side of the, the tree,

473
00:21:28.445 --> 00:21:30.905
but each one of those can branch out into its own,

474
00:21:30.965 --> 00:21:32.825
so it can get overwhelming really quickly.

475
00:21:33.365 --> 00:21:35.785
So are you proposing any aids

476
00:21:35.805 --> 00:21:39.585
or any resources that can help maybe map this out

477
00:21:39.685 --> 00:21:41.465
and organize things better? Yeah, that's an

478
00:21:41.865 --> 00:21:42.865
Excellent question. So I don't

479
00:21:42.865 --> 00:21:45.545
know as much about what's happening on the

480
00:21:46.335 --> 00:21:50.105
defense side, on the, on the commercial or civilian side.

481
00:21:50.485 --> 00:21:52.465
Boeing, as far as I can tell,

482
00:21:52.645 --> 00:21:53.985
is kind of at the front of this.

483
00:21:54.005 --> 00:21:55.505
And they have developed a bunch of tools.

484
00:21:55.565 --> 00:21:57.025
So there are certain parts of it, right?

485
00:21:57.185 --> 00:22:00.025
Breaking it out into the four archetypes for each,

486
00:22:00.925 --> 00:22:02.425

uh, control action.

487
00:22:03.675 --> 00:22:06.215
That's an automated thing you could just do right there.

488
00:22:06.215 --> 00:22:08.895
There's things you can do to start creating the table,

489
00:22:09.255 --> 00:22:10.855
creating the structure, and then humans

490
00:22:10.855 --> 00:22:11.935
filled in within that.

491
00:22:12.235 --> 00:22:13.735
You may be able to use ai,

492
00:22:13.735 --> 00:22:15.335
but I am not ready to stand up here

493
00:22:15.335 --> 00:22:16.335
and endorse that just yet.

494
00:22:17.035 --> 00:22:22.015
Um, and I know there's some additional tools,

495
00:22:23.315 --> 00:22:23.535
um,

496
00:22:27.375 --> 00:22:28.545
various people have done.

497
00:22:29.015 --> 00:22:30.025
Your mileage may vary.

498
00:22:30.025 --> 00:22:31.585
You may have to develop some on your own.

499
00:22:32.885 --> 00:22:36.425
The flip side of it is, if we're gonna complain,

500
00:22:36.425 --> 00:22:40.195
it's too thorough, so we don't want to do that.

501
00:22:40.225 --> 00:22:42.115
What are we giving up? What are we missing? Right?

502
00:22:42.115 --> 00:22:43.875
These are the hazards that may kill us.

503
00:22:44.575 --> 00:22:49.155
And so I think the solution is to stay more abstract.

504
00:22:49.255 --> 00:22:50.995
So you're looking at system behavior.

505
00:22:51.015 --> 00:22:52.875
You don't, you're not diving into exactly

506
00:22:53.055 --> 00:22:55.155
how does you know x, y, Z happen.

507
00:22:55.155 --> 00:22:58.955
You're saying if this happens, um, you later you can go

508
00:22:58.955 --> 00:22:59.955
to your SME on the thing

509
00:22:59.955 --> 00:23:01.155
and say, okay, how could this happen?

510
00:23:01.295 --> 00:23:02.555
How can we mitigate it?

511
00:23:02.975 --> 00:23:06.755
Um, so you, you keep the workload down by abstraction

512
00:23:06.975 --> 00:23:08.435
and by scoping.

513
00:23:09.335 --> 00:23:12.465

Um, I had one more thing I was gonna say.

514
00:23:12.485 --> 00:23:13.425
Can I remember what it was?

515
00:23:17.935 --> 00:23:20.385
I'll add it to someone else's answer if I think of it.

516
00:23:21.285 --> 00:23:23.065
So, uh, the, the, uh, the second part

517
00:23:23.065 --> 00:23:24.145
of my question, if you don't mind.

518
00:23:24.255 --> 00:23:26.465
Yeah. And, and I'm glad you brought up hazards

519
00:23:26.465 --> 00:23:28.545
because I noticed on one of your, uh,

520
00:23:28.545 --> 00:23:33.265
earlier slides you had the unknown unknown hazards, um,

521
00:23:33.845 --> 00:23:36.705
and, and, and, and some hazards that, that you do accept.

522
00:23:37.325 --> 00:23:39.905
Um, now going to this, initially I thought, well,

523
00:23:39.905 --> 00:23:41.945
this is gonna help me identify those hazards.

524
00:23:41.945 --> 00:23:43.185
But as, as we went along,

525
00:23:43.335 --> 00:23:44.945
it's more about the actual process itself

526
00:23:45.425 --> 00:23:48.365
and identifying maybe mitigating some circumstances.

```
527
00:23:48.545 --> 00:23:50.565
So do you see this as, as a way to

528
00:23:51.365 --> 00:23:53.685
I identify those hazards as well?

529
00:23:53.705 --> 00:23:55.165
Or did, did, did I miss something?

530
00:23:56.765 --> 00:23:58.565
I think I'm not totally clear on the question.

531
00:23:58.585 --> 00:23:59.845
The question is, so, um,

532
00:23:59.875 --> 00:24:02.245
Will this Help you identify hazards and,

533
00:24:02.305 --> 00:24:04.805
and what's the alternative? What was your understanding?

534
00:24:04.915 --> 00:24:07.365
Okay. I I I absolutely butchered that question.

535
00:24:07.385 --> 00:24:09.925
So let me, let me say that again.

536
00:24:09.985 --> 00:24:12.725
And it's getting pretty late in the day. So my, I apologize.

537
00:24:13.505 --> 00:24:18.205
Um, my, when you started, you, you,

538
00:24:18.225 --> 00:24:20.445
you mentioned that there are a lot of hazards

539
00:24:20.445 --> 00:24:22.085
and that's the, that's the difficult part,

540
00:24:22.085 --> 00:24:23.845
```

is identifying all those hazards. That's right. We wanna

541
00:24:23.845 --> 00:24:24.845
Find them. Um,

542
00:24:24.845 --> 00:24:27.445
and what I got from this,

543
00:24:27.505 --> 00:24:30.925
and that's probably, I just misunderstood that maybe, um,

544
00:24:31.185 --> 00:24:35.285
the process itself doesn't really show you

545
00:24:35.595 --> 00:24:37.925
what those hazards are or, or the unknown hazards,

546
00:24:37.945 --> 00:24:40.645
but we focus on the, on the details of it. I

547
00:24:40.805 --> 00:24:43.925
Think this is a confusion about maybe,

548
00:24:44.135 --> 00:24:47.085
maybe I overloaded the use of the term hazards.

549
00:24:48.085 --> 00:24:51.245
I showed listing out top level hazards, right?

550
00:24:51.245 --> 00:24:53.005
Collides with the ground, collides

551
00:24:53.005 --> 00:24:54.285
with another aircraft, et cetera.

552
00:24:55.295 --> 00:24:57.965
Those are top level hazards.

553
00:24:57.965 --> 00:25:00.285
You're gonna end up with all sorts of ways

554
00:25:00.315 --> 00:25:01.645
that could happen below that.

555
00:25:02.025 --> 00:25:05.965
So what SCPA does is it kind of, uh,

556
00:25:06.725 --> 00:25:07.925
somewhat flips it on its head.

557
00:25:07.925 --> 00:25:12.405
You're saying, here are all the bad things

558
00:25:12.915 --> 00:25:16.245
that, bad behaviors that could come out of the system.

559
00:25:18.035 --> 00:25:20.445
What are the ways in which those behaviors

560
00:25:21.015 --> 00:25:22.845
could emerge from the system,

561
00:25:24.925 --> 00:25:27.065
and how do we prevent that from happening?

562
00:25:27.085 --> 00:25:31.145
So it's a, it's more of a, it's a constructive view.

563
00:25:31.205 --> 00:25:33.745
So what it does is it breaks it down into all the pieces

564
00:25:33.885 --> 00:25:35.185
so you can find them.

565
00:25:36.525 --> 00:25:36.745
Um,

566
00:25:43.535 --> 00:25:43.885
right.

567
00:25:44.185 --> 00:25:44.925

So, so

568
00:25:48.995 --> 00:25:51.195
structural damage, right?

569
00:25:51.295 --> 00:25:55.075
Is, is a hazard loss of integrity. How does that happen?

570
00:25:55.455 --> 00:25:58.795
You can smash it, you can burn it, you can

571
00:25:59.495 --> 00:26:00.955
let it fall apart on its own.

572
00:26:01.255 --> 00:26:03.115
You could corrode it, you could whatever, right?

573
00:26:03.115 --> 00:26:04.115
These are all hazards.

574
00:26:04.115 --> 00:26:06.955
And you might find these as you go through,

575
00:26:07.105 --> 00:26:09.155
they all come back to that top level hazard

576
00:26:09.295 --> 00:26:10.635
of structural failure.

577
00:26:12.025 --> 00:26:13.075
Does that answer your question?

578
00:26:13.735 --> 00:26:14.995
Yes. So, so this is more kind

579
00:26:14.995 --> 00:26:16.595
of a maybe bottom up approach,

580
00:26:16.655 --> 00:26:18.875
and you end up maybe identifying that

```
581
00:26:18.975 --> 00:26:21.755
As you're looking at, at here are all the bad ways

582
00:26:21.775 --> 00:26:22.835
the system could behave.

583
00:26:23.025 --> 00:26:25.155
What are the ways in which it could be

584
00:26:25.225 --> 00:26:26.635
induced to happen badly?

585
00:26:27.585 --> 00:26:29.355
What are the ways that those could happen?

586
00:26:29.775 --> 00:26:31.115
How do we prevent it? Okay.

587
00:26:32.385 --> 00:26:33.915
Okay. Perfect. Thank you so much. Yeah.

588
00:26:36.135 --> 00:26:37.715
Hey, uh, no, I'm a great brief

589
00:26:38.015 --> 00:26:41.755
and I, I think this is a fascinating tool.

590
00:26:42.155 --> 00:26:44.685
I understand it. I think I've, I've read about it.

591
00:26:44.715 --> 00:26:46.165
I've never had the privilege of using it.

592
00:26:47.285 --> 00:26:51.285
I agree that it seems like it's a very

593
00:26:51.805 --> 00:26:55.205
detailed process that might get you bogged down.

594
00:26:55.505 --> 00:26:58.805
```

Yes, It seems like it. Um, so two questions.

595
00:26:59.185 --> 00:27:03.165
One, is there a ways that you've seen

596
00:27:03.385 --> 00:27:04.445
or you've thought about

597
00:27:04.775 --> 00:27:06.765
where we could use large language models

598
00:27:08.145 --> 00:27:12.205
to help us cut through some of the

599
00:27:13.395 --> 00:27:17.525
fine tooth comb parts of this process, uh,

600
00:27:17.665 --> 00:27:20.365
and move through the noise to find the signal?

601
00:27:20.745 --> 00:27:24.845
And then the other question, which I'm, I am a fan of STPA,

602
00:27:24.845 --> 00:27:29.125
don't take this as hostile, but identifying UCAS

603
00:27:30.625 --> 00:27:34.455
seems to be the domain of the creative experts

604
00:27:34.455 --> 00:27:35.735
that you bring into the room.

605
00:27:37.835 --> 00:27:41.895
How is identifying UCAS as a step within

606
00:27:42.415 --> 00:27:44.895
STPA any different at all?

607
00:27:45.565 --> 00:27:47.775
From what I already do? Yeah.

608
00:27:47.885 --> 00:27:50.375
When I create a test hazard analysis,

609
00:27:50.875 --> 00:27:51.935
Two excellent questions.

610
00:27:52.715 --> 00:27:56.095
Uh, generative ai, the only thing I've seen is the stuff

611
00:27:56.095 --> 00:27:57.375
that Jeff was talking about.

612
00:27:57.515 --> 00:28:00.655
So I, I can't point to a lot more there.

613
00:28:01.515 --> 00:28:04.535
Um, I rather suspect,

614
00:28:04.635 --> 00:28:07.455
and I can't make any real claim.

615
00:28:07.895 --> 00:28:09.935
I rather suspect that once you've been

616
00:28:09.935 --> 00:28:12.375
through a couple programs using STPA,

617
00:28:12.675 --> 00:28:14.575
it will be natural enough

618
00:28:14.925 --> 00:28:17.655
that it might actually be easier than going back

619
00:28:17.655 --> 00:28:19.455
and doing legacy methods.

620
00:28:20.395 --> 00:28:23.855
Um, uh,

621
00:28:25.115 --> 00:28:28.095

one way to make it extra efficient is

622
00:28:28.095 --> 00:28:29.455
to bring in a good facilitator.

623
00:28:29.455 --> 00:28:30.735
If anyone's had the privilege of working

624
00:28:30.735 --> 00:28:32.455
with Dr. John Thomas or

625
00:28:32.595 --> 00:28:36.175
or other people like that, it's amazing

626
00:28:36.275 --> 00:28:40.175
how quickly they can just get the, the team to the,

627
00:28:40.275 --> 00:28:43.015
to the bottom of it, and the team does not disappear.

628
00:28:43.115 --> 00:28:45.615
You need your experts, you need your engineering thinking.

629
00:28:45.735 --> 00:28:47.415
A lot of people have found, even just by

630
00:28:47.935 --> 00:28:49.615
creating a controlled structure, right?

631
00:28:50.135 --> 00:28:53.415
Modeling that out together on a whiteboard already the whole

632
00:28:53.415 --> 00:28:55.695
team gets, gets lifted to a new level.

633
00:28:56.275 --> 00:29:00.855
Um, having that facilitation to elicit those pieces is big.

634
00:29:01.285 --> 00:29:02.615
Finding the UCA.

635
00:29:02.635 --> 00:29:04.095
So, so, okay, so one thing

636
00:29:04.095 --> 00:29:07.095
that happens when you're brainstorming THA,

637
00:29:07.915 --> 00:29:12.695
is you identify a hazard and you add it to your list,

638
00:29:13.675 --> 00:29:16.935
but it doesn't reveal what might be a whole branch,

639
00:29:17.095 --> 00:29:18.375
a whole segment of hazards,

640
00:29:18.375 --> 00:29:20.295
unless it like triggers something in your brain

641
00:29:20.295 --> 00:29:21.335
or maybe someone else's

642
00:29:21.335 --> 00:29:22.695
and you're like, oh, I've seen things like this.

643
00:29:22.755 --> 00:29:24.055
So let's think about things like this.

644
00:29:24.765 --> 00:29:27.295
Finding the UCA gives you a whole branch,

645
00:29:28.115 --> 00:29:29.335
and then you can be like, oh,

646
00:29:29.685 --> 00:29:31.135
well actually there's another UCA

647
00:29:31.135 --> 00:29:32.335
and you got a whole nother whole branch.

648
00:29:32.335 --> 00:29:34.335

And then you can be like, wait, there's a hazard

649
00:29:34.365 --> 00:29:36.055
that we're not thinking about.

650
00:29:36.275 --> 00:29:38.615
Oh yeah, there's this other control action

651
00:29:38.615 --> 00:29:39.775
we forgot to list.

652
00:29:40.355 --> 00:29:44.365
So it, it gives you this domain in which,

653
00:29:45.705 --> 00:29:49.685
uh, everything that you find gives you a lot more,

654
00:29:50.505 --> 00:29:52.365
uh, breadth, depth and breadth.

655
00:29:52.945 --> 00:29:54.925
You don't have to dive in and,

656
00:29:54.945 --> 00:29:57.245
and drown in the ocean that you're boiling.

657
00:29:57.305 --> 00:29:59.405
You can keep it limited. It's an art.

658
00:30:00.225 --> 00:30:03.925
Um, and I think it's worth saying because it's common.

659
00:30:04.065 --> 00:30:05.965
You, you didn't say it, but it just reminded me.

660
00:30:05.965 --> 00:30:09.525
There's a common misconception. STPA is not a crank.

661
00:30:09.625 --> 00:30:13.285
You don't turn it and, you know, safety results spit out.

662
00:30:13.395 --> 00:30:15.405
It's a methodology that involves people

663
00:30:15.785 --> 00:30:19.165
and it's a process you walk through that gets more out

664
00:30:19.165 --> 00:30:21.365
of the people who you have in the room in a

665
00:30:21.365 --> 00:30:22.525
much more consistent way.

666
00:30:22.545 --> 00:30:25.925
And there's various papers from MIT about, um,

667
00:30:26.825 --> 00:30:30.325
the hazards identified using SCPA versus various legacy

668
00:30:30.325 --> 00:30:31.765
methods and the consistency

669
00:30:31.765 --> 00:30:34.245
with which you achieve those results.

670
00:30:34.265 --> 00:30:36.245
So it doesn't depend as much on who's in the

671
00:30:36.365 --> 00:30:37.645
room at, at what time?

672
00:30:40.615 --> 00:30:41.855
I have two. Who has a

673
00:30:41.855 --> 00:30:42.935
microphone? You have a microphone? Okay.

674
00:30:42.935 --> 00:30:44.735
Yeah, I've got a microphone over here. Go back.

675
00:30:44.835 --> 00:30:45.855

One question before.

676
00:30:46.675 --> 00:30:49.415
Um, I remember back when they were originally writing the

677
00:30:49.415 --> 00:30:50.695
40, 40, 26 and,

678
00:30:50.715 --> 00:30:52.935
and the River of Unknowns is, I think,

679
00:30:53.975 --> 00:30:56.695
I think maybe Rod Wete had a term for it.

680
00:30:57.075 --> 00:30:59.295
Um, there was always a misconception

681
00:30:59.445 --> 00:31:03.255
that the system we're going to analyze, uh,

682
00:31:03.355 --> 00:31:05.895
is gonna help us answer those unknown unknowns.

683
00:31:05.895 --> 00:31:08.895
Where from flight test, we always computed that.

684
00:31:08.895 --> 00:31:11.695
You must acknowledge that when you go to it,

685
00:31:11.695 --> 00:31:13.895
there will probably still be hazards out there

686
00:31:13.895 --> 00:31:15.215
that you never identified.

687
00:31:15.635 --> 00:31:17.895
And I don't care how good your analysis

688
00:31:17.955 --> 00:31:19.335
is, it's still there.

689
00:31:19.635 --> 00:31:22.695
And that's just to remind you, you can do all this

690
00:31:22.715 --> 00:31:25.055
to mitigate, but there's still something

691
00:31:25.675 --> 00:31:26.895
in the back of your mind still.

692
00:31:26.915 --> 00:31:27.975
We probably miss something

693
00:31:27.995 --> 00:31:29.335
and that that will always be there.

694
00:31:29.555 --> 00:31:31.855
So it's not, there's, there's no pure way

695
00:31:32.235 --> 00:31:34.375
to ever identify the unknown unknowns.

696
00:31:35.195 --> 00:31:36.935
Uh, you can minimize them though. You can

697
00:31:37.455 --> 00:31:38.455
Minimize, You can find more of them.

698
00:31:38.705 --> 00:31:40.655
We're never gonna it, it's called flight test.

699
00:31:40.685 --> 00:31:41.855
It's not called a flight demo.

700
00:31:42.085 --> 00:31:43.655
Once you find them all, it's a flight demo.

701
00:31:47.995 --> 00:31:48.995
We have one more,

702
00:31:56.215 --> 00:31:57.735

Probably one more than one question,

703
00:31:57.735 --> 00:31:59.415
but if we can hold that for the panel, um,

704
00:31:59.505 --> 00:32:01.175
we're gonna be running into that anyway.

705
00:32:01.565 --> 00:32:02.335
Come, coming up next.