WEBVTT

1
00:00:02.680 --> 00:00:05.490
Okay, so a little bit of motherhood.

2
00:00:06.830 --> 00:00:10.010
The reason these organizations do so well is that we're willing to share our

3
00:00:10.010 --> 00:00:14.290
ideas, but that also means that we treat that information with respect and

4
00:00:14.290 --> 00:00:15.690
confidentiality because we take,

5
00:00:15.700 --> 00:00:19.970
we're trying to gather the lessons learned so we can all be safer and do better

6
00:00:20.130 --> 00:00:22.930
at our jobs, not to use it in an inappropriate manner.

7
00:00:22.950 --> 00:00:25.610
So I'll just leave that up there for remind you. That's the, uh,

8
00:00:25.670 --> 00:00:27.410
that's the key to this organization working.

9
00:00:32.720 --> 00:00:34.940
Please turn off your cell phones or silence them.

10
00:00:34.960 --> 00:00:37.220
And if you do have to take a call, I please ask that you, uh,

11
00:00:37.220 --> 00:00:40.940
wanted to out into the back of the room or into the outside area to take that.

12
00:00:42.780 --> 00:00:44.400
And I want thank our sponsors.

13
00:00:44.460 --> 00:00:47.320
We have quite a few sponsors that makes this organization, uh,

14
00:00:47.320 --> 00:00:51.040
this event a success. Uh, you can see there's a pretty good number up there,

15
00:00:51.180 --> 00:00:53.680
and we just wanna say thank you to them for the work they did, uh,

16
00:00:53.680 --> 00:00:58.600
providing the support. Okay. Finally, let's get the, uh, tutorial going.

17
00:00:58.640 --> 00:01:01.040
I, what you're waiting for. So I'm gonna introduce Darren and he'll take,

18
00:01:01.040 --> 00:01:03.760
he'll introduce his team. For those who don't know, Darren McDonald,

19
00:01:03.870 --> 00:01:07.600
he's a technical fellow at, uh, Boeing, primarily in the, uh,

20
00:01:07.920 --> 00:01:10.600
stability and control and, uh, in flight test engineering group.

21
00:01:11.070 --> 00:01:13.520
I've known Darren for quite a few years through the manufacturer's flight test

22
00:01:13.520 --> 00:01:18.400
council, uh, where he's really the, for us as the part 25 OEMs to get together.

23
00:01:18.750 --> 00:01:20.240
He's the glue that binds that, uh,

24
00:01:20.240 --> 00:01:23.200
organization together and does fantastic work. Uh,

25
00:01:23.480 --> 00:01:25.960
bachelor of Science from Embry Riddle. And, um,

26
00:01:26.590 --> 00:01:29.400
he's also board on the board of Directors for Flight Test Safety Camp committee.

27
00:01:29.660 --> 00:01:31.520
So, couple notable things.

28
00:01:31.620 --> 00:01:34.440
He is the Tony Le Beer Flight Test Safety Award winner in 2024,

29
00:01:34.440 --> 00:01:37.560
his work on the M FTC and what he's done there. So, without further ado,

30
00:01:37.660 --> 00:01:39.880
I'm gonna introduce Darren and we'll get the tutorial started.

31
00:01:46.100 --> 00:01:47.680
Thanks, Stu. Uh,

32
00:01:48.640 --> 00:01:52.800
I feel honored to be able to be a part of this tutorial here today and, uh,

33
00:01:53.090 --> 00:01:57.120
especially because of the people that I get to be, uh, associated with. So, uh,

34
00:01:57.860 --> 00:02:02.200
we have, uh, Lieutenant Colonel Sarah Summers with us. Uh,

35
00:02:02.700 --> 00:02:06.400
she went to, uh, TPS as a,

36
00:02:06.420 --> 00:02:09.360
as an fte and then, uh,

37
00:02:09.360 --> 00:02:12.480
has continued her education in a number of different places. Uh,

38
00:02:12.630 --> 00:02:16.440

most notably today. Uh, she did a,

39
00:02:16.600 --> 00:02:20.960
a master's program at mit, and her advisor was Dr. Nancy Levison,

40
00:02:21.540 --> 00:02:25.280
who is one of the, uh, two founders of,

41
00:02:25.420 --> 00:02:28.680
of Stamp and s tpa. So, um,

42
00:02:28.850 --> 00:02:31.920
she's well educated there and,

43
00:02:31.980 --> 00:02:36.800
and has been able to practice s stpa since then and continues to, uh,

44
00:02:36.860 --> 00:02:41.840
uh, teach classes on s TPA at the, uh, test pilot school. Um,

45
00:02:42.030 --> 00:02:46.400
currently she's serving with the 709th Technical Maintenance Squadron.

46
00:02:46.940 --> 00:02:50.480
And, uh, it's fascinating to talk to her about what all goes on there.

47
00:02:50.550 --> 00:02:52.840
They're responsible for all of the, uh,

48
00:02:53.470 --> 00:02:55.800
nuclear monitoring sensors worldwide.

49
00:02:55.980 --> 00:02:59.580
So it's an interesting thing that I'd never really thought about. What,

50
00:02:59.730 --> 00:03:02.580
what we need to, to stay safe. Um,

51
00:03:03.480 --> 00:03:06.540
she has done a lot of testing there. You can,

52
00:03:06.720 --> 00:03:11.100
you can read through some of her previous, uh, uh,

53
00:03:11.100 --> 00:03:13.940
assignments are, are varied, uh,

54
00:03:14.210 --> 00:03:18.820
from hypersonics to aerial refueling and airdrops to electronic warfare. So,

55
00:03:19.320 --> 00:03:23.660
um, that's, we're in, we're in good hands with, with Sarah today.

56
00:03:24.360 --> 00:03:27.180
So, uh, then we've got, uh,

57
00:03:27.180 --> 00:03:31.940
Lieutenant Colonel Dan Montes on line with us today. He can't be here in person,

58
00:03:32.080 --> 00:03:36.340
but he's gonna be starting us off with our tutorial. Uh,

59
00:03:36.920 --> 00:03:41.500
and he also has multiple degrees, the last of which is a,

60
00:03:41.660 --> 00:03:45.860
a PhD in aeronautics and Astronautics. And he too had, uh, Dr.

61
00:03:45.970 --> 00:03:50.180
Levison as, as an advisor, and, um, got,

62
00:03:50.560 --> 00:03:54.940
got well versed in s Stpa, uh, through that. Um,

63
00:03:56.500 --> 00:04:00.360
Dan is part of the US Space Force and, uh,

64
00:04:00.940 --> 00:04:03.880
be interesting to hear more of what they're putting together there.

65
00:04:04.460 --> 00:04:08.240
He also teaches at, at the tps, uh, related to tpa.

66
00:04:08.820 --> 00:04:13.720
And he's been a flight test engineer on F 22, B one, b2,

67
00:04:13.880 --> 00:04:18.680
B 52 X 47, X 51, and then a bunch of weapons programs.

68
00:04:18.740 --> 00:04:23.680
So, um, we're privileged to have DA Dan with us today to,

69
00:04:23.780 --> 00:04:28.760
to walk us through sdpa. And then finally we've got, uh, dunes, uh,

70
00:04:29.510 --> 00:04:32.520
from, from Boeing Dunes, has a,

71
00:04:32.640 --> 00:04:35.320
a master's with George Washington University.

72
00:04:35.590 --> 00:04:38.680
He's been with us at Boeing for 18 years, uh,

73
00:04:38.680 --> 00:04:43.040
specializing in structural flight test. And, uh,

74
00:04:43.430 --> 00:04:48.080
then he's also been kind of leading the, the charge for us on S stpa.

75
00:04:48.420 --> 00:04:49.440
So, um,

76
00:04:49.940 --> 00:04:54.680
he has worked on 8 7 3 7 max and Triple seven

77
00:04:54.710 --> 00:04:58.800
nine, as well as a number of military derivative programs like the PA I.

78
00:04:59.580 --> 00:05:03.430

And, uh, he also is, uh,

79
00:05:03.770 --> 00:05:05.350
an avid sailor. And, uh,

80
00:05:06.110 --> 00:05:09.300
I wanna make sure I never try and play ultimate Frisbee against him,

81
00:05:09.300 --> 00:05:11.460
cause I know I'd lose. So with that,

82
00:05:11.530 --> 00:05:14.180
I'll turn it over to Sarah and she'll get us started with our tutorial.

83
00:05:18.240 --> 00:05:22.140
All right. Thank you. Everyone can hear me? All right.

84
00:05:23.120 --> 00:05:27.540
Um, so this is what we're gonna, we're gonna do today.

85
00:05:27.590 --> 00:05:31.700
We've got about 30 minutes of systems thinking background. Murph, uh,

86
00:05:31.760 --> 00:05:34.940
online is gonna give that piece. He's the smart p d type.

87
00:05:35.410 --> 00:05:38.260
I'll talk about s TPA basics for about 45 minutes.

88
00:05:38.270 --> 00:05:40.740
We'll have the 30 minute coffee break. Um,

89
00:05:40.740 --> 00:05:44.620
and then we're gonna have a test use case from, from, uh, dunes and
Darren.

90
00:05:45.490 --> 00:05:50.020
Then we'll get into, uh, the first portion of the UAV exercise.

91
00:05:50.050 --> 00:05:54.460

This is meant to be, um, interactive. So we'll see how that goes with, uh, this,

92
00:05:54.490 --> 00:05:56.860
this big of a group. This is the largest group I've done this with,

93
00:05:57.000 --> 00:06:00.020
so we'll see how that goes. Uh, then we'll do the lunch and tour,

94
00:06:00.700 --> 00:06:02.220
followed by the second part of the exercise.

95
00:06:02.290 --> 00:06:05.620
Wrap it up with some takeaways and talk about how you apply risk with this

96
00:06:05.620 --> 00:06:10.040
particular, uh, set. All right.

97
00:06:10.040 --> 00:06:12.520
So a little bit about me before I talk about how I got into S T P.

98
00:06:12.600 --> 00:06:17.000
I wanna talk about how I got into safety. Uh, so I'm third generation Air Force.

99
00:06:17.460 --> 00:06:19.640
My, my dad was a helicopter pilot in the Air Force.

100
00:06:19.660 --> 00:06:22.520
My mom was an engineer in the Air Force when I was 16.

101
00:06:22.620 --> 00:06:25.680
My dad was a squadron commander out at Ellis Air Force Base,

102
00:06:26.100 --> 00:06:29.960
and there was a mid-air collision that killed 12 members of his squadron. Um,

103
00:06:29.980 --> 00:06:33.960
so I, I thought about joining the Air Force prior to that, but, but after that,

104
00:06:34.300 --> 00:06:38.880
um, mishap, I decided that I wanted to serve in honor of them, uh, the,

105
00:06:38.980 --> 00:06:42.560
the 12 men that died that day. I didn't know what that meant at the time. At 16,

106
00:06:42.980 --> 00:06:46.320
uh, what do you really know? I thought I was gonna fly helicopters. Like my dad.

107
00:06:46.610 --> 00:06:49.520
Turns out I'm too short. I round up to five two. So,

108
00:06:49.620 --> 00:06:54.320
so that wasn't gonna happen. So I became an engineer instead. And,

109
00:06:54.440 --> 00:06:57.840
uh, throughout my career, there's been a, a thread of safety and,

110
00:06:57.840 --> 00:07:00.200
and it really boils down to that bumper sticker there,

111
00:07:00.200 --> 00:07:01.760
which is what gets me up every day.

112
00:07:01.760 --> 00:07:05.800
What what gets me in my uniform is making sure that the weapon systems that we

113
00:07:05.800 --> 00:07:09.640
deliver to the war fighters are gonna allow them to do their mission and then

114
00:07:09.640 --> 00:07:13.440
come back home to their families. Um, so,

115
00:07:13.620 --> 00:07:15.400
so when I was an aircraft maintenance officer,

116

00:07:15.680 --> 00:07:19.400
I attended the Jet Engine Mishap Investigation course at Shepherd Air Force

117
00:07:19.430 --> 00:07:21.120
Base. And then during that time,

118
00:07:21.120 --> 00:07:24.840
I did a few small incidents that that happened in maintenance engine, fod,

119
00:07:24.840 --> 00:07:29.040
that type of thing. Then I went to the Air Force Research Laboratory and, uh,

120
00:07:29.480 --> 00:07:34.480
investigated a few small UAS mishaps there. Uh, after test pilot school,

121
00:07:34.640 --> 00:07:37.680
I was the unit flight safety officer. Usually that's a, a rated guy,

122
00:07:37.700 --> 00:07:41.280
but I was the only one who had been to a formal mishap investigation course.

123
00:07:41.620 --> 00:07:44.400
So I gotta do that as well. And then, of course, doing, uh,

124
00:07:44.400 --> 00:07:49.200
safety planning for test, uh, uh, test operations as well.

125
00:07:49.640 --> 00:07:54.080
I was a squadron operations officer for a, an electronic warfare unit, or, um,

126
00:07:54.240 --> 00:07:58.960
a test unit there at Edwards as well. And some of the things that I saw is,

127
00:07:59.060 --> 00:08:01.800
one, we're very chain of events based. Uh, if,

128

00:08:01.800 --> 00:08:04.920
if you've ever looked at the Air Force, uh, safety, uh,

129
00:08:04.980 --> 00:08:08.720
system where we put all of our, uh, investigation information into, it's,

130
00:08:08.790 --> 00:08:10.600
it's very much about chain of events.

131
00:08:10.950 --> 00:08:13.640
What that means is if there are systemic issues with your program,

132
00:08:14.150 --> 00:08:16.080
it's not easy to document in there.

133
00:08:16.100 --> 00:08:20.320
And I actually got some pushback of trying to put some programmatic type issues

134
00:08:20.350 --> 00:08:23.000
that we had where we had these rapid reaction programs. We're trying to get,

135
00:08:23.220 --> 00:08:27.520
get out into the field quickly, um, and that, that led to some of these mishaps.

136
00:08:27.520 --> 00:08:32.240
But there's no way to capture that, uh, in the system that we are using. Um,

137
00:08:32.240 --> 00:08:36.640
we also tend to blame the operator versus fix the design and even more

138
00:08:36.640 --> 00:08:39.200
importantly, create, um, uh,

139
00:08:39.500 --> 00:08:43.480
create a system where we don't have dangerous designs in the first place.

140
00:08:44.300 --> 00:08:48.640
And then when I was doing flight tests, um, uh, I saw that,

141
00:08:49.140 --> 00:08:51.960
um, a lot of what we did was based off of previous knowledge,

142
00:08:52.040 --> 00:08:53.800
I was doing a lot of air refueling testing.

143
00:08:54.260 --> 00:08:57.900
So you dust off the last KC 1 35 test plan. You look at it,

144
00:08:57.900 --> 00:09:00.780
you see what's different, and then, and then you go from there.

145
00:09:01.520 --> 00:09:05.100
But what happens if you're doing something that's never been done before? Um,

146
00:09:05.160 --> 00:09:09.100
or, you know, I went from KC 1 35 to KC 46, you're,

147
00:09:09.100 --> 00:09:11.740
you mishaps that you're concerned about are the exact same, right?

148
00:09:11.740 --> 00:09:14.740
You're concerned about boom strike, you're concerned about mid-air collision,

149
00:09:14.740 --> 00:09:17.620
you're concerned about, uh, fuel system compatibility.

150
00:09:17.620 --> 00:09:20.500
Those are the main three things you're looking for. Um, but,

151
00:09:20.500 --> 00:09:23.060
but how you get into those situations is gonna be different.

152
00:09:23.080 --> 00:09:26.900
Cuz now you have a remote vision system, you don't have a hydro mechanical boom,

153
00:09:27.160 --> 00:09:30.580

you have, uh, you know, different, different system. So,

154
00:09:31.040 --> 00:09:34.700
so the knowledge that you had before doesn't always apply, uh,

155
00:09:34.700 --> 00:09:38.780
to what you're doing with the new program. Um, so I showed up to,

156
00:09:38.840 --> 00:09:43.700
to m mit, I saw, I saw this s TPA class. I didn't really know what that meant,

157
00:09:44.160 --> 00:09:48.220
um, but it sounded, sounded interesting. So I took the course and,

158
00:09:48.220 --> 00:09:51.380
and I saw this is what I was missing. This is, this is what I,

159
00:09:51.660 --> 00:09:53.900
I wanted to learn about and, and, uh,

160
00:09:53.900 --> 00:09:56.860
hopefully bring back to the Air force and to the test community.

161
00:09:59.700 --> 00:10:03.080
All right. And with that, Murph, you can come off mute.

162
00:10:03.080 --> 00:10:04.000
We'll see if we hear you

163
00:10:05.230 --> 00:10:06.063
With

164
00:10:06.940 --> 00:10:07.773
Any luck.

165
00:10:09.980 --> 00:10:10.813
No.

166
00:10:15.110 --> 00:10:15.943
Oh,

167
00:10:17.050 --> 00:10:17.930
I hear a tiny voice.

168
00:10:22.890 --> 00:10:23.860
Just a second mark.

169
00:10:34.400 --> 00:10:35.233
Uh, try again.

170
00:10:39.120 --> 00:10:39.953
No,

171
00:10:43.590 --> 00:10:44.423
Try again.

172
00:11:00.500 --> 00:11:02.640
We threw a lot of curve balls at these guys this morning,

173
00:11:02.820 --> 00:11:05.280
so they're working hard to get this all set up

174
00:11:15.480 --> 00:11:18.650
now. Try again.

175
00:11:41.650 --> 00:11:43.710
Got you. Good copy. Uh, how

176
00:11:43.710 --> 00:11:46.230
About me? Okay. Okay. Okay. Okay.

177
00:11:50.640 --> 00:11:51.480
I got a little bit of reading

178
00:11:59.730 --> 00:12:00.563
Best.

179
00:12:02.560 --> 00:12:03.393
Uh, good copy.

180

00:12:07.550 --> 00:12:08.820
Right? I see if that makes sense.

181
00:12:38.960 --> 00:12:39.793
Test.

182
00:12:40.960 --> 00:12:43.010
Good. Copy. Test, test.

183
00:12:54.580 --> 00:12:56.670
I'll try, uh, I'll try headphone mike again.

184
00:12:59.800 --> 00:13:03.170
It's nothing on your end. Um, I don't think it's stuff on our end.

185
00:13:08.560 --> 00:13:09.393
Audio check.

186
00:13:30.500 --> 00:13:33.480
All right. Let's, can you try again, Dan?

187
00:13:34.460 --> 00:13:35.680
Hey. Yep. Can you, can you hear me

188
00:13:38.300 --> 00:13:39.200
All right? Yeah, keep talking.

189
00:13:41.240 --> 00:13:42.073
Test, test.

190
00:13:48.100 --> 00:13:49.640
All right. See, this should be a little bit better.

191
00:13:52.310 --> 00:13:54.360
Okay. Uh, how now? Yeah, this

192
00:13:54.360 --> 00:13:55.360
Is good. Gotcha.

193
00:13:56.750 --> 00:13:59.870
Okay. Awesome. So, so we're up?

194
00:14:02.170 --> 00:14:06.620
Yes. Yeah. Okay. Awesome. Um,

195
00:14:07.330 --> 00:14:11.980
yeah. Good, good morning everyone. I'm running on an old laptop myself, so, uh,

196
00:14:12.630 --> 00:14:16.660
we'll, uh, we'll give Microsoft, uh, some credit for making any of this work.

197
00:14:17.360 --> 00:14:22.340
Um, so, uh, good morning everyone. I, uh, I can't see the slides, but,

198
00:14:22.440 --> 00:14:23.820
um, I'm, uh, you know, I'm,

199
00:14:23.880 --> 00:14:27.980
I'm assuming we're on the one that says about me with, uh, with a picture of,

200
00:14:28.240 --> 00:14:32.660
of me and my, my lovely wife standing in much of a, a, a front bunch of statues,

201
00:14:32.760 --> 00:14:35.620
um, to, and yeah, feel free to build it out to that. Oh, yeah,

202
00:14:35.620 --> 00:14:40.020
I see the slides now. Um, so I have, I have one correction. Uh,

203
00:14:40.020 --> 00:14:44.660
Pancho said, uh, I'm a, I'm a smart PhD type, and I can definitely, uh, uh,

204
00:14:44.660 --> 00:14:49.020
back up the PhD type part of that statement. Uh, but, uh,

205
00:14:49.040 --> 00:14:52.780
no appreciate, uh, the chance to be here virtually with everyone. Sorry,

206
00:14:52.820 --> 00:14:56.940
I couldn't be there in person. Um, I, uh, you know, as far as, uh,

207
00:14:56.940 --> 00:15:00.340
my background and, and really appreciate the, uh, the intro, uh, as well a,

208
00:15:00.460 --> 00:15:05.020
a little earlier, um, I, uh, I, I am a, uh, uh, survivor of, of the, uh,

209
00:15:05.020 --> 00:15:08.620
the Air Force. And, and I am, I am now in Space Force, uh, for,

210
00:15:08.620 --> 00:15:11.780
for the last few years of my career. Uh, I work at the,

211
00:15:11.780 --> 00:15:15.220
the National Space Range, which is, uh, a, a new thing that we're,

212
00:15:15.220 --> 00:15:20.140
we're trying to stand up and, uh, and I, I work in safety, uh, at the range.

213
00:15:20.200 --> 00:15:23.780
So that's, that's kind of a neat way to cap off, um, uh, you know, a really,

214
00:15:23.860 --> 00:15:28.820
a really long career in the, in the military. Um, so, uh,

215
00:15:28.820 --> 00:15:32.300
yeah, with, with through dps, we, we call ourselves integrated test engineers,

216
00:15:32.560 --> 00:15:36.380
uh, in, in Space Force. So we're, we're trying to be new and different. Uh, and,

217
00:15:36.380 --> 00:15:38.300
and, and all that means is we, we try to,

218

00:15:38.320 --> 00:15:41.860
we try to cover end-to-end testing all the way from, uh, stuff on the bench, uh,

219
00:15:41.860 --> 00:15:46.700
all the way out, uh, to, uh, operational test and tactics development. Uh,

220
00:15:46.700 --> 00:15:49.980
it's a little bit of a different paradigm. And, uh, happy to chat about that.

221
00:15:50.040 --> 00:15:53.740
Uh, anytime, if, if, if someone wants to reach out to me later. Um,

222
00:15:53.740 --> 00:15:57.500
spent about half my life in test and, and half in research, uh,

223
00:15:57.500 --> 00:16:01.300
been stationed in, uh, uh, you know, uh, the standard, uh, several places as a,

224
00:16:01.300 --> 00:16:05.940
as a military person. And, uh, I, I keep this picture in here. Uh,

225
00:16:05.940 --> 00:16:09.740
it's really cuz we, uh, uh, poncho and I teach, uh, the, the space test course,

226
00:16:10.400 --> 00:16:14.260
uh, that I, I always talk about Easter Island and, uh, I mean, super g whiz, uh,

227
00:16:14.260 --> 00:16:17.620
get got a chance to travel there, uh, during my last assignment. But, uh, there,

228
00:16:17.620 --> 00:16:20.620
there is talk of a lot of international partnering and space and even putting,

229
00:16:21.010 --> 00:16:23.540
putting some, uh, space, ground support equipment, uh,

230
00:16:23.700 --> 00:16:28.380
in various partner nations, uh, territory, uh, including Chile. So,

231
00:16:28.760 --> 00:16:32.140
um, although none of those things are, are, uh, coming to fruition quite yet,

232
00:16:32.440 --> 00:16:35.260
uh, it's always kind of neat to think that we're gonna have these very complex

233
00:16:35.290 --> 00:16:38.540
architectures, uh, as we advance our, our systems. And,

234
00:16:38.540 --> 00:16:40.940
and space is definitely an environment where, uh,

235
00:16:40.940 --> 00:16:45.060
we can get pretty complex with the way we, uh, we interface things together.

236
00:16:46.000 --> 00:16:49.700
Um, I, uh, I wasn't thinking too much about safety until, uh,

237
00:16:49.700 --> 00:16:52.180
maybe about a third of the way in into my career. There were,

238
00:16:52.180 --> 00:16:55.780
there were a couple big accidents out at Edwards Air Force Base where I was at

239
00:16:55.780 --> 00:17:00.300
the time, uh, cools cool and, and dash razo, uh, where, where, uh,

240
00:17:00.300 --> 00:17:04.700
class a, uh, mishaps a few months apart from each other. Uh, and that, that,

241
00:17:04.700 --> 00:17:09.140
that was what changed my, um, my whole outlook on, on a lot of things, um,

242
00:17:09.240 --> 00:17:13.660
and kind of put me on this path of, of thinking a lot more about safety. So, um,

243
00:17:13.780 --> 00:17:14.140
I, uh,

244
00:17:14.140 --> 00:17:18.700
I had the opportunity to go out to m i t and study under Professor Levison, um,

245
00:17:18.840 --> 00:17:23.260
uh, uh, not quite overlapped with, with poncho, but, but close at the same time.

246
00:17:23.400 --> 00:17:25.460
So after we were both done with our programs,

247
00:17:25.460 --> 00:17:28.580
we were able to connect and do a lot of this really cool thinking on,

248
00:17:28.800 --> 00:17:33.020
on system safety. Uh, and then, then I had the chance to land in TPS and,

249
00:17:33.020 --> 00:17:35.860
you know, start thinking about these complex problems which were in blue there,

250
00:17:35.960 --> 00:17:40.460
uh, on the left side of the slide. Um, uh, lot of thought about, you know,

251
00:17:40.460 --> 00:17:44.380
how autonomy, uh, like real autonomy, uh, affects how we, you know,

252
00:17:44.380 --> 00:17:49.020
how we test our systems. Uh, and, uh, yeah, left, left the, uh, kill word, uh,

253
00:17:49.100 --> 00:17:51.900

there in, in the font. Uh, you know, cause at the end of the day, you know,

254
00:17:51.900 --> 00:17:55.620
we're in the military and we, we break things for a living. So, um, but, uh,

255
00:17:55.620 --> 00:17:58.460
yeah, I should probably think about not having terms like that in,

256
00:17:58.700 --> 00:18:02.900
in industry slides. So, uh, uh, go ahead and, uh, and flip over to the next one,

257
00:18:02.900 --> 00:18:06.180
please. And I'll, um, I'll, I'll go a little,

258
00:18:06.420 --> 00:18:09.460
a little faster cuz I know the, the Microsoft issues were,

259
00:18:09.460 --> 00:18:14.100
were delaying things a bit. Um, you know, we, we, uh, I'll, I'll leave the,

260
00:18:14.320 --> 00:18:18.740
the, uh, um, and you can, you can go ahead and flip through to the next one. Uh,

261
00:18:19.000 --> 00:18:22.060
so I'll, I'll, you know, briefly just talk about this. Uh,

262
00:18:22.560 --> 00:18:26.300
I'm sure a lot of people in the audience have either looked at this at a case as

263
00:18:26.300 --> 00:18:29.660
a case study or, or just, you know, familiar, uh, just because of the,

264
00:18:29.660 --> 00:18:33.540
the gravity of this, this event, um, you know, with the tsunami that caused the,

265

00:18:33.540 --> 00:18:37.980
uh, uh, the, the power plant to, to have some issues over there in, in Japan.

266
00:18:38.840 --> 00:18:43.020
But, uh, um, you know, if you look at how, uh, you know,

267
00:18:43.080 --> 00:18:47.580
any system is, is put together, uh, you can quickly start seeing,

268
00:18:47.960 --> 00:18:51.580
uh, you know, where the interfaces that that matter, uh, are. If,

269
00:18:51.640 --> 00:18:54.820
if you just sketch things out and you take a step back and you think about

270
00:18:54.820 --> 00:18:58.940
things. But, uh, you know, what happened, uh, this example is, uh, uh,

271
00:18:58.940 --> 00:19:03.540
power went out effectively, the short version, uh, and, uh, um,

272
00:19:03.800 --> 00:19:08.020
the, you know, the, the, the, the system was not able to keep, uh, you know,

273
00:19:08.020 --> 00:19:12.300
keep the nuclear cycle, uh, in check. Uh, and, uh, and, and they had a,

274
00:19:12.300 --> 00:19:16.780
they had a nuclear incident. Um, now there's a lot of ways to keep,

275
00:19:17.200 --> 00:19:20.700
um, you know, this cooling water pump powered. And, and those are listed there,

276
00:19:21.120 --> 00:19:25.500
uh, uh, the, uh, there's diesel generators, uh,

277
00:19:25.500 --> 00:19:29.540
they're on site. There's also diesel generators up on the hillside, uh,

278
00:19:29.540 --> 00:19:34.100
which could be switched on to, uh, to provide power in. So, um, you know,

279
00:19:34.100 --> 00:19:37.180
there's, there's no reason a a flooding event should, uh,

280
00:19:37.180 --> 00:19:42.100
should take all of these, these things out. Um, um, however, I, you know,

281
00:19:42.100 --> 00:19:45.020
you cross out the, the station itself because of the,

282
00:19:45.080 --> 00:19:47.460
the flooding that happened from the tsunami that, um,

283
00:19:47.460 --> 00:19:49.260
that prevented that from being a, a source.

284
00:19:49.400 --> 00:19:51.940
So you've got those other two backups, uh,

285
00:19:51.940 --> 00:19:56.020
that that should have made everything work fine. Um, and, uh, if you,

286
00:19:56.560 --> 00:19:59.700
if you flip to the next slide, uh, this, you know,

287
00:19:59.700 --> 00:20:04.380
Pancho alluded to kind of like the, the, the chain thinking. Um, and, uh,

288
00:20:04.380 --> 00:20:06.780
you know, I don't need it belabor how, you know, uh,

289
00:20:06.780 --> 00:20:10.220
failure probabilities work too much. But, um, you know, you've,

290
00:20:10.220 --> 00:20:12.780
you've got various different redundancies and you, you know,

291

00:20:12.780 --> 00:20:16.500
you do the one minus, you know, p type type thing, and, and, you know,

292
00:20:16.500 --> 00:20:18.860
you end up with, with a nice probability that everything will,

293
00:20:19.090 --> 00:20:23.540
will work fine or, or that, or that things won't fail. Um, and then, you know,

294
00:20:23.540 --> 00:20:27.260
we're, we're all very used to the, the severity types, probability, uh,

295
00:20:27.260 --> 00:20:30.980
risk matrices that have been around since the old days. So, um, you know,

296
00:20:30.980 --> 00:20:34.900
it usually helps to have a quantitative number when you can get it for the,

297
00:20:34.900 --> 00:20:38.740
for the probability piece. And then, uh, severity is a whole other, you know,

298
00:20:38.740 --> 00:20:42.740
ball, ball wax in terms of how you define, uh, severity. So, uh,

299
00:20:42.760 --> 00:20:46.620
so this is just a, you know, the simple math example of that. And, and, um,

300
00:20:46.620 --> 00:20:48.180
you know, some of our students are, you know,

301
00:20:48.180 --> 00:20:50.580
have never seen stuff like this before. So I'd normally spend a,

302
00:20:50.580 --> 00:20:54.260
a little bit longer on a slide like this. Uh, but you can, you can go ahead and,

303
00:20:54.480 --> 00:20:59.260

and, uh, press on to the next slide. Uh,

304
00:20:59.400 --> 00:21:03.750
so, uh, the, uh, the flood waters, uh,

305
00:21:03.810 --> 00:21:08.470
the actually took out all of the in-house, uh, diesel generators, which is,

306
00:21:08.510 --> 00:21:11.750
I believe it was four of them. Uh, basically sitting side by side to each other.

307
00:21:11.930 --> 00:21:16.030
So parallel redundancy. Uh, however, uh,

308
00:21:16.030 --> 00:21:17.590
you get your common cause, right? Your,

309
00:21:17.590 --> 00:21:19.950
your floodwater just takes everything out because the, uh,

310
00:21:19.950 --> 00:21:24.950
the dang generators were in the basement, uh, basically. And then the, uh,

311
00:21:25.140 --> 00:21:27.550
well, why not just switch on the, uh,

312
00:21:27.570 --> 00:21:30.710
the diesel generators that are way up on the hill that can't get hit with the

313
00:21:30.710 --> 00:21:34.470
flood well, or, well, the switches are in the basement too, to, uh,

314
00:21:34.470 --> 00:21:39.070
switch circuits. Uh, so you basically have a common cause that takes out, um,

315
00:21:39.220 --> 00:21:43.350
your primary, your first backup and your second backup, um, all with,

316
00:21:43.410 --> 00:21:47.030
all with one event. And, uh, and all of this was because of the whole, you know,

317
00:21:47.170 --> 00:21:47.910
uh, black swan,

318
00:21:47.910 --> 00:21:51.390
that's where that whole term kind of made it into pop culture from, um, uh,

319
00:21:51.390 --> 00:21:55.790
from, uh, tale that, uh, you know, the civil engineers didn't think that, uh,

320
00:21:55.790 --> 00:21:59.910
you know, the, the water was gonna crest the, uh, the seawall. Uh,

321
00:21:59.910 --> 00:22:03.830
and then it did, you know, it hit however many sigmas out, and it did. And, uh,

322
00:22:03.850 --> 00:22:08.110
the, the station was just not ready for this worst case scenario. Um,

323
00:22:08.110 --> 00:22:12.670
and all the eggs were proverbially in the, in the same basket. Uh, next slide.

324
00:22:15.530 --> 00:22:20.070
So, uh, you know, a lot of, a lot of things come out of, uh, thinking about,

325
00:22:20.170 --> 00:22:23.870
hey, uh, you know, how do we design an actual system to,

326
00:22:24.130 --> 00:22:27.750
to account for kind of these worst case scenarios that,

327
00:22:27.750 --> 00:22:30.110
that probabilistically shouldn't even, uh,

328
00:22:30.350 --> 00:22:33.470
ignite the rest of your probability tree. Um, so, you know,

329
00:22:33.470 --> 00:22:37.470
it's probability alone sufficient for, for safety. Um, you know,

330
00:22:37.470 --> 00:22:40.350
we talked about the seawater breach in the wall, um, you know,

331
00:22:40.370 --> 00:22:43.710
is reliability the same as safety? And, uh,

332
00:22:43.730 --> 00:22:48.210
and do we always have trigger redundancy? So, uh,

333
00:22:48.310 --> 00:22:50.210
you can go ahead and, and flip through.

334
00:22:53.410 --> 00:22:56.750
So, you know, the, uh, the risk matrix has been around for the,

335
00:22:56.810 --> 00:23:00.830
the better part of almost three quarters of a century now.

336
00:23:01.610 --> 00:23:05.470
Um, and, and hazard analysis techniques have, have, uh, have come and,

337
00:23:05.470 --> 00:23:09.630
and mostly, um, stayed, uh, since, you know, since the middle part of,

338
00:23:09.650 --> 00:23:14.270
of the last century, um, you know, simple electromechanical systems, uh,

339
00:23:14.460 --> 00:23:17.390
when, when something failed, it was usually right there in front of you.

340
00:23:17.390 --> 00:23:19.710
You could see it, you could see exactly what it was connected to.

341

00:23:19.710 --> 00:23:24.430
There weren't a lot of cross dependencies or complex coupling,

342
00:23:25.290 --> 00:23:28.510
uh, things happening, uh, nor software, uh,

343
00:23:28.510 --> 00:23:31.670
really being too much at play when a lot of these, uh,

344
00:23:31.670 --> 00:23:36.470
fault trees and those types of, of, uh, you know, uh, analysis techniques, uh,

345
00:23:36.490 --> 00:23:41.230
you know, came into fruition. So what we see in, in modern times,

346
00:23:42.370 --> 00:23:43.350
uh, is that, you know,

347
00:23:43.350 --> 00:23:47.660
simple component failures aren't typically the smoking gun and,

348
00:23:47.660 --> 00:23:50.980
and a lot of accidents. It's usually the coupling of a lot of cyber,

349
00:23:51.300 --> 00:23:55.780
physical and, and human decision making, uh, that, uh, you know, that affect,

350
00:23:56.040 --> 00:23:59.660
uh, when, when incidents happen, uh, you know, all the way through, uh,

351
00:23:59.770 --> 00:24:03.820
even management layers, uh, of, of, you know, human activity systems.

352
00:24:04.640 --> 00:24:09.580
And, um, you know, we at, uh, I'll take a, a quick aside. Um,

353
00:24:09.600 --> 00:24:13.940
you know, uh, Pancho mentioned she went to, uh, to, uh, jet engine, uh,

354

00:24:14.200 --> 00:24:16.820
safety, uh, mishap, uh, school. I,

355
00:24:16.860 --> 00:24:21.580
I recently went to the first ever space mishap, uh, investigation course. Uh,

356
00:24:21.580 --> 00:24:25.340
pretty, pretty interesting experience. Uh, I got to spend some time at the,

357
00:24:25.340 --> 00:24:29.980
at the Air Force Safety Center and was, uh, was impressed that there is, uh,

358
00:24:30.180 --> 00:24:35.100
I would say some progress in the human involvement in, in accidents. Uh,

359
00:24:35.100 --> 00:24:39.660
you know, the, they're willing to say, Hey, we don't blame people. Uh, we, uh,

360
00:24:39.660 --> 00:24:43.380
we try to figure out, you know, kind of, you know, at what point, uh,

361
00:24:43.380 --> 00:24:47.740
could the way that humans are involved in the system be better? Um, uh,

362
00:24:47.740 --> 00:24:48.900
but then, you know, at the end of the day,

363
00:24:48.900 --> 00:24:53.020
there's still a root cause and it's usually, uh, you know, uh, John Doe or,

364
00:24:53.020 --> 00:24:56.460
you know, mishap engineer or, you know, such and such person, uh,

365
00:24:56.570 --> 00:25:00.660
effectively did a thing, uh, and they, and they put that in the, you know,

366

00:25:00.660 --> 00:25:05.100
in the bottom line of these, these AP investigation reports. So we've, you know,

367
00:25:05.100 --> 00:25:08.020
I think we've got a still a ways to go, uh,

368
00:25:08.020 --> 00:25:11.420
to kind of admit that it's really the coupling between components,

369
00:25:11.420 --> 00:25:16.380
whether those those components are human or, or not human, uh, to, um, to,

370
00:25:16.400 --> 00:25:18.260
you know, bring our mindset to, Hey, what,

371
00:25:18.260 --> 00:25:21.380
what is it that's really causing these, these hazardous conditions in our,

372
00:25:21.380 --> 00:25:24.540
in our modern day incidents? Right? Next slide.

373
00:25:27.400 --> 00:25:31.260
Um, so I'll, I'll pretty much just gloss over this. We, uh, when,

374
00:25:31.260 --> 00:25:33.340
when we were at test pilot school, uh, uh,

375
00:25:33.820 --> 00:25:37.300
starting to put some of this curriculum out, uh, at the school,

376
00:25:37.360 --> 00:25:42.020
and then e eventually, uh, get it out a little bit more into the wild, um,

377
00:25:42.020 --> 00:25:45.100
you know, we, we, we talked about this and we, you know, the, these,

378
00:25:45.110 --> 00:25:46.980
these kind of three tiers. Um,

379
00:25:46.980 --> 00:25:49.140
there's a lot of different books and a lot of different lit,

380
00:25:49.140 --> 00:25:50.860
and these things are called a lot of different things. Um,

381
00:25:50.860 --> 00:25:55.420
certainly in in military strategy. Um, you know, we get into this wicked domain,

382
00:25:55.680 --> 00:26:00.300
uh, quite a bit where you, you don't even know what the goal is. Um, but, um,

383
00:26:00.400 --> 00:26:04.220
you know, it's really to say that as, as, as systems do get more complex, and I,

384
00:26:04.260 --> 00:26:06.460
I think we took out the slide with the, the giant, you know,

385
00:26:06.660 --> 00:26:09.540
internet of things and, you know, a thousand things talking to each other. Um,

386
00:26:09.720 --> 00:26:10.100
it is,

387
00:26:10.100 --> 00:26:15.020
it does become pretty much impossible to decide exactly what specific components

388
00:26:15.080 --> 00:26:19.540
and specific things you, you have to test for, like your normal spec validation,

389
00:26:19.840 --> 00:26:22.300
uh, or spec compliance verification. And, and,

390
00:26:22.720 --> 00:26:25.540
and you have to start thinking more about just validating that, uh,

391
00:26:25.970 --> 00:26:29.100
that the mission is getting done, uh, and that you're accounting for as many,

392
00:26:29.320 --> 00:26:31.580
uh, weird cross variables as, as as possible.

393
00:26:31.760 --> 00:26:34.460
So even defining like what your system is,

394
00:26:34.790 --> 00:26:38.460
which boundary you wanna respect when you're doing your analysis, um,

395
00:26:38.530 --> 00:26:41.980
becomes absolutely necessary before you even start doing the analysis.

396
00:26:41.980 --> 00:26:44.940
So that's why we, we kind of of talk about, you know, these different tiers of,

397
00:26:45.000 --> 00:26:48.500
of problems. Um, but, you know, we won't, we won't go back to, uh,

398
00:26:48.500 --> 00:26:50.580
that too much today. All right, next slide.

399
00:26:53.320 --> 00:26:57.580
Pardon? My, my allergies are, are not doing great right now, Colorado. Uh,

400
00:26:58.360 --> 00:27:03.180
so, uh, so we, you know, we, we've all talked about complexity, um, and, uh,

401
00:27:03.180 --> 00:27:07.700
in, in some form, uh, you know, in our, in our engineering careers. And, um,

402
00:27:07.760 --> 00:27:09.940
you know, uh, the way we, we define it, uh,

403
00:27:09.940 --> 00:27:13.740
simply as possible is just interaction of a lot of parts in multiple ways that,

404
00:27:14.000 --> 00:27:17.820
uh, culminate in a higher order of, of meaning. And I emergence, uh, you know,

405
00:27:17.820 --> 00:27:21.620
greater than sum. And, uh, if you, if you keep going to the next slide,

406
00:27:22.860 --> 00:27:26.160
uh, there's, there's the way we've, we as a society have,

407
00:27:26.160 --> 00:27:30.560
have typically dealt with, uh, you know, uh, complicated or complex things,

408
00:27:30.560 --> 00:27:33.520
which is just, you know, put, build it, you know, build it down to the,

409
00:27:33.540 --> 00:27:37.440
to the elementary, uh, pieces as much as we can, and, uh, you know,

410
00:27:37.440 --> 00:27:40.520
kind of check each one, uh, make sure it works,

411
00:27:40.520 --> 00:27:44.440
and then you put it all together and everything should, should work great. Um,

412
00:27:44.580 --> 00:27:47.480
and, you know, I'll, I'll, uh, I'll do another aside. We've,

413
00:27:47.480 --> 00:27:50.920
we've been learning very, very quickly in the military, uh,

414
00:27:50.920 --> 00:27:55.800
that there are challenges when you have a bunch of different heterogeneous, uh,

415

00:27:55.800 --> 00:27:56.960
systems that, uh,

416
00:27:56.960 --> 00:28:00.400
we're each designed to exactly the thing that they were supposed to be designed

417
00:28:00.400 --> 00:28:03.400
to. And in theory, they should all work together and, and talk to each other,

418
00:28:03.940 --> 00:28:06.720
uh, and then we go do exercises and realize that, that, you know,

419
00:28:06.720 --> 00:28:08.880
the integration of all the various, um,

420
00:28:08.880 --> 00:28:12.200
different pieces of this system just aren't, you know, aren't working, right?

421
00:28:12.740 --> 00:28:15.520
So, uh, so th this idea that, um,

422
00:28:15.520 --> 00:28:18.560
things get a lot more complex as you start putting all the pieces back together

423
00:28:18.560 --> 00:28:19.720
in our, in our modern systems,

424
00:28:19.900 --> 00:28:24.240
is kind of showing why the reductionism approach is not, uh, wholly,

425
00:28:24.900 --> 00:28:27.600
um, you know, uh, uh, sufficient for, uh,

426
00:28:27.600 --> 00:28:29.080
for making sure that we're validating our,

427
00:28:29.080 --> 00:28:33.520

what we're actually trying to get done. Um, there's statistical approaches too,

428
00:28:33.540 --> 00:28:36.520
and, and, and Taylor goes into this stuff a lot, right? Like, yeah,

429
00:28:36.520 --> 00:28:37.720
you can just sit there and,

430
00:28:37.720 --> 00:28:41.640
and treat everything as a black box because it's all so complex. And, um,

431
00:28:41.640 --> 00:28:45.520
you know, you just, you just kind of make sure that the, uh, that you're,

432
00:28:45.520 --> 00:28:49.360
that the outputs of the system, uh, you know, meet a nice little normal curve,

433
00:28:49.500 --> 00:28:53.320
or you, you run a gazillion Monte Carlo's on, uh, what you think you're getting.

434
00:28:53.940 --> 00:28:55.240
And, um, and you, you know,

435
00:28:55.240 --> 00:28:58.960
you try to normalize what is happening with the system, and, uh,

436
00:28:58.960 --> 00:28:59.793
and you just kind of,

437
00:28:59.900 --> 00:29:03.120
you wait for more real world data to keep adjusting that model,

438
00:29:03.540 --> 00:29:06.080
but you're not looking too deeply into the, uh,

439
00:29:06.100 --> 00:29:09.360
the structured behavior within the system. All right, next slide.

440

00:29:12.340 --> 00:29:17.280
Uh, so where, where S D P A comes in is kind of, kind of in between,

441
00:29:17.660 --> 00:29:20.400
uh, those two approaches. Um,

442
00:29:20.400 --> 00:29:24.480
it doesn't completely ignore the mechanisms, uh, within,

443
00:29:25.220 --> 00:29:29.480
uh, a, a complex system or complex psychology. So we call it organized, uh,

444
00:29:29.690 --> 00:29:31.440
complexity. Um,

445
00:29:31.940 --> 00:29:35.640
but it doesn't also just assume that things work very linearly and

446
00:29:35.880 --> 00:29:39.680
independently. So it does try to account for those interactions, uh,

447
00:29:39.680 --> 00:29:44.660
between the components within a a system. And, and that's, you know,

448
00:29:44.660 --> 00:29:46.860
it comes from systems theory. It, it,

449
00:29:46.860 --> 00:29:50.700
it's actually pinned very nicely on systems engineering and, and, you know,

450
00:29:50.700 --> 00:29:54.060
with, with an emphasis on the engineering, uh, you know, part of,

451
00:29:54.060 --> 00:29:58.060
of systems engineering. Um, and, uh, uh, and it, you know, it,

452
00:29:58.130 --> 00:30:01.420
it's kind of come about in the last few decades as, as something that's been,

453
00:30:01.520 --> 00:30:05.300
uh, quite useful, uh, uh, in, in, in a lot of industries. And I know,

454
00:30:05.340 --> 00:30:07.980
I know there's, uh, several in, in this audience who have, uh,

455
00:30:07.980 --> 00:30:11.620
had some experience with, with those types of methods. All right, next,

456
00:30:14.000 --> 00:30:16.940
Uh, so, so we'll belabor this one, either. Got got a couple,

457
00:30:16.940 --> 00:30:20.340
couple nice quotes there from, uh, you know, some, some of the greats, right?

458
00:30:20.560 --> 00:30:25.060
But, uh, um, you know, I, I, uh, I guess I probably, uh, should, uh,

459
00:30:25.060 --> 00:30:28.540
should think about, you know, doing this slide before the, uh, the graph, uh,

460
00:30:28.540 --> 00:30:31.020
you know, on the slide before. But, uh, um, you know,

461
00:30:31.020 --> 00:30:33.540
kind of covered all this is, is, uh, you know, you,

462
00:30:33.640 --> 00:30:37.900
you can't do complete reductionist analysis on, uh, on complex ecologies.

463
00:30:38.560 --> 00:30:41.060
Uh, but you can't just ignore the mechanisms, uh,

464
00:30:41.060 --> 00:30:43.060
inside of those systems either. You, you gotta,

465
00:30:43.080 --> 00:30:46.500
you gotta find something that that's a nice balance, uh, in between those,

466
00:30:46.500 --> 00:30:50.140
those two approaches, okay? We can keep going.

467
00:30:53.250 --> 00:30:56.230
Uh, so systems theory, uh, is, uh,

468
00:30:56.250 --> 00:30:59.390
not something I would ever claim to be an expert in. It is, uh, an,

469
00:30:59.390 --> 00:31:04.270
an underpinning of a lot of stuff in the world right now. And, uh, um,

470
00:31:04.530 --> 00:31:08.070
we basically try to boil it down to our, or, you know,

471
00:31:08.070 --> 00:31:12.550
I would say even simplify, uh, systems theory as, as this idea of, uh, feedback,

472
00:31:13.690 --> 00:31:15.870
um, to think about the structures within your systems,

473
00:31:16.090 --> 00:31:20.230
and then the idea of emergence to think about, um, the, you know,

474
00:31:20.230 --> 00:31:23.230
the whole being more than the sum of the parts, uh, within the system itself,

475
00:31:23.250 --> 00:31:26.670
and kind of how you've, you've got a higher purpose and a higher meaning at, at,

476
00:31:26.670 --> 00:31:31.550
at the higher levels of, of stake, uh, in, in the system. So, um, so that,

477
00:31:31.550 --> 00:31:34.630
that's about as much as I, I go into it, and I, I'll, I'll, uh, we,

478

00:31:34.630 --> 00:31:35.670
we can keep going to the next slide,

479
00:31:35.670 --> 00:31:40.030
and I've just got a few slides on each one of those things. Um, so, uh,

480
00:31:40.030 --> 00:31:40.270
you know,

481
00:31:40.270 --> 00:31:43.950
anyone who's done anything systems engineering has seen some version of,

482
00:31:44.090 --> 00:31:47.590
of this, uh, and, and the whole idea is, is, you know, you can,

483
00:31:47.590 --> 00:31:51.110
you can decompose, uh, a system to, uh,

484
00:31:51.150 --> 00:31:54.390
various different levels of meaning, right? You know, all the way from, uh,

485
00:31:54.390 --> 00:31:57.190
and you know, there, there's also a million ways of slicing the pie, right?

486
00:31:57.190 --> 00:32:00.110
This is, this is just one of them. And, uh, and actually, uh, uh,

487
00:32:00.110 --> 00:32:03.550
forget the source for this, apologies. Um, but, uh, you know,

488
00:32:03.550 --> 00:32:07.350
this one's got goals at the very top and then actual physical, uh, processes,

489
00:32:07.630 --> 00:32:11.230
resources, and, and components at the bottom. But, um, but each one of those is,

490
00:32:11.230 --> 00:32:15.750
uh, satisfying, uh, a why, uh, coming from the, from the level above.

491
00:32:16.330 --> 00:32:20.390
And, um, and, you know, you can go all the way into doing traceability, uh,

492
00:32:20.750 --> 00:32:23.790
exercises on, on these things. And, and I know a lot of systems engineering, uh,

493
00:32:23.950 --> 00:32:28.110
students get to do things like that and get to go into functional decompositions

494
00:32:28.210 --> 00:32:32.710
and, and all those fun things. Uh, but, but the main gist is that, um, you know,

495
00:32:32.990 --> 00:32:37.230
a an agent sitting, uh, you know, at the very, very, uh,

496
00:32:37.330 --> 00:32:38.350
top end of,

497
00:32:38.370 --> 00:32:42.300
of a mission or a system isn't really sitting there thinking about what every

498
00:32:42.580 --> 00:32:47.340
molecule in the airplane or in the, you know, the vehicle, uh, is doing.

499
00:32:47.760 --> 00:32:50.020
Uh, they just kind of wanna know, hey, is is, you know,

500
00:32:50.080 --> 00:32:53.540
is the company doing well? Uh, you know, is the profit margin, uh,

501
00:32:53.540 --> 00:32:56.820
where it needs to be, uh, is the fleet being efficient? You know, those,

502
00:32:56.820 --> 00:33:00.260
those types of things, uh, which, which trace up from the, uh, you know,

503
00:33:00.260 --> 00:33:03.740
the bare physical processes at the bottom? All right, next slide.

504
00:33:05.200 --> 00:33:08.460
And then the other, the other pillar is structure, uh,

505
00:33:08.460 --> 00:33:11.700
which comes from this idea of, of feedback, which comes from, um,

506
00:33:12.090 --> 00:33:16.900
cybernetics way back in the World War II days, uh, that, uh, if you,

507
00:33:17.040 --> 00:33:20.900
you know, can just give yourself a chance to think about, uh,

508
00:33:21.000 --> 00:33:24.380
how these different levels and echelons of the systems are actually interacting

509
00:33:24.380 --> 00:33:29.060
and tracing between each other, um, that is what you put on top of this,

510
00:33:29.320 --> 00:33:31.460
uh, you know, hierarchy of meaning that I,

511
00:33:31.460 --> 00:33:34.460
that I talked about on the previous slide, when you start, um,

512
00:33:34.710 --> 00:33:38.420
using systems modeling and, and, uh, in a systems theoretic approach to,

513
00:33:38.420 --> 00:33:41.900
to look at your systems. Um, and, uh, the whole, uh,

514
00:33:41.900 --> 00:33:46.580
if you wanna go to the next slide, uh, uh, the whole idea of feedback, um,

515
00:33:46.580 --> 00:33:48.940
again, you know, anyone with, with an engineering background has,

516
00:33:48.940 --> 00:33:50.780
has probably had to take a controls class or,

517
00:33:50.840 --> 00:33:54.380
or is at least very familiar with this concept and has, uh,

518
00:33:54.440 --> 00:33:58.100
has seen it from everything from a qualitative to a quantitative, uh,

519
00:33:58.190 --> 00:34:01.980
point of view. Um, you know, we, uh, we always joke with our students, like,

520
00:34:01.980 --> 00:34:04.700
we're not gonna teach you any math, but we at least want you to know what, uh,

521
00:34:04.700 --> 00:34:06.820
you know, what control means, right? And, you know,

522
00:34:07.100 --> 00:34:10.700
feedback is transmission about what's actually going on, uh, in,

523
00:34:10.720 --> 00:34:15.700
in a process to a process regulator or a controller. Um, I'll use words like,

524
00:34:15.760 --> 00:34:18.460
uh, agents, uh, decision makers, um,

525
00:34:18.460 --> 00:34:22.620
pretty broadly to talk to both human and non-human controllers.

526
00:34:23.280 --> 00:34:26.220
Uh, because, uh, what, um, what you'll see when, uh, when, uh,

527
00:34:26.220 --> 00:34:29.780
Pancho starts getting into some of the, the aspects of s stpa, um,

528
00:34:29.800 --> 00:34:33.820

the more you can just think about, uh, nodes and aspects of your system as,

529
00:34:33.840 --> 00:34:37.860
as agents, um, uh, without worrying about whether it's cyber,

530
00:34:37.860 --> 00:34:40.700
whether it's physical, whether it's human, whether it's non-human, uh,

531
00:34:40.700 --> 00:34:43.420
the more you can kind of, uh, normalize the, the way that,

532
00:34:43.420 --> 00:34:45.740
that you do the analysis. So, um, yeah,

533
00:34:45.900 --> 00:34:49.220
I mentioned that this all came from cybernetics. Uh, it, you know,

534
00:34:49.220 --> 00:34:51.380
underlying notion for organized activities is one of the,

535
00:34:51.380 --> 00:34:55.260
one of the foot stomper test questions. You know, we, we give our students, and,

536
00:34:55.320 --> 00:34:56.040
uh, and it,

537
00:34:56.040 --> 00:34:59.620
it lets you think about how your system is really structured or whether we

538
00:34:59.740 --> 00:35:02.980
structured it enough when, when, when we designed it. Okay? Next slide.

539
00:35:05.840 --> 00:35:08.980
Uh, so, um, in a nutshell, uh,

540
00:35:09.240 --> 00:35:12.820
if you have at least some attempt at structure within your system,

541

00:35:13.200 --> 00:35:17.860
it is not impervious, but it is at least resilient to,

542
00:35:18.160 --> 00:35:22.020
uh, those disturbances and those interactions with the environment. Now,

543
00:35:22.050 --> 00:35:24.500
what is the system and what is the environment that's,

544
00:35:24.500 --> 00:35:27.020
that's up to you to decide. Um, you know,

545
00:35:27.020 --> 00:35:30.140
we have the very simple circle with the pyramid looking hierarchy, which,

546
00:35:30.240 --> 00:35:34.420
you know, the real world is not like that at all, right? But, um, you know,

547
00:35:34.860 --> 00:35:38.620
whatever your, uh, structure is that you feel you have control over,

548
00:35:38.760 --> 00:35:41.740
or you feel that you have an influence over making sure that it's put together

549
00:35:41.740 --> 00:35:45.620
the right way, and that the individual nodes are, uh, uh,

550
00:35:46.020 --> 00:35:49.660
interacting and thinking the way that they should be, that's,

551
00:35:49.660 --> 00:35:50.700
that's what you call your system.

552
00:35:50.700 --> 00:35:53.580
And then everything outside that boundary you drew is, is the environment,

553
00:35:53.590 --> 00:35:54.220
which you're,

554
00:35:54.220 --> 00:35:57.860
you're just gonna let the environment do what the environment does. Um, and,

555
00:35:58.000 --> 00:36:01.820
you know, boundaries are porous. Uh, you know, these are open systems. So, um,

556
00:36:01.820 --> 00:36:05.580
there will be challenges to your system from the environment.

557
00:36:06.650 --> 00:36:10.750
All right, next slide. Uh, s EPA is,

558
00:36:10.970 --> 00:36:15.630
is mbse. Um, so I, uh, I, you know, MBS e is,

559
00:36:15.630 --> 00:36:19.590
at least in the military, starting to, I, I think, find its footing and, uh,

560
00:36:19.590 --> 00:36:22.110
space Force has come right out from top level doctrine and said,

561
00:36:22.110 --> 00:36:24.990
we are gonna be a digital force, and we're gonna be, you know,

562
00:36:24.990 --> 00:36:28.350
we're going to go into, you know, an engineering based way of life, like,

563
00:36:28.350 --> 00:36:29.190
just from the get go.

564
00:36:29.650 --> 00:36:32.670
So a lot of people are picking up books and trying to figure out what the heck

565
00:36:32.890 --> 00:36:35.990
MBS e means to them. There's a million books out there,

566
00:36:35.990 --> 00:36:40.270

there's a lot of software suites. Um, sdpa is, uh,

567
00:36:40.660 --> 00:36:45.350
MBSE without needing to learn fancy software. Uh, you can do it on a napkin,

568
00:36:45.350 --> 00:36:48.630
you can do it on a whiteboard, you could do it on PowerPoint, on Visio,

569
00:36:48.690 --> 00:36:52.350
or anything in between, or anything more complex if you wanna, um, you know,

570
00:36:52.370 --> 00:36:56.790
get really fancy with it. But, uh, you know, at the end of the day, it's, um,

571
00:36:56.850 --> 00:37:00.190
you know, as case in point today, something that you can really, uh, you know,

572
00:37:00.200 --> 00:37:04.750
teach to a wide audience, uh, of various backgrounds, uh, engineering,

573
00:37:04.750 --> 00:37:09.550
operations, uh, management, uh, you know, every, and, and, and everybody else.

574
00:37:10.210 --> 00:37:12.230
Um, and, and the whole point is that, you know, if,

575
00:37:12.250 --> 00:37:15.710
if someone is a stakeholder in a system, uh,

576
00:37:15.710 --> 00:37:18.550
they should be invited to the planning for that system,

577
00:37:18.610 --> 00:37:22.150
and they should be able to point at a common, uh, uh,

578
00:37:22.390 --> 00:37:26.630

a common model and a common, uh, set of assumptions and understanding and,

579
00:37:26.630 --> 00:37:31.310
and group and, uh, group, uh, um, uh, understanding of,

580
00:37:31.370 --> 00:37:35.030
of what the system is so that everyone can, can fine tune, uh,

581
00:37:35.030 --> 00:37:37.750
exactly what that, how that system is structured and what it's supposed to do.

582
00:37:39.050 --> 00:37:42.960
All right, next, uh, so, uh,

583
00:37:43.030 --> 00:37:46.800
just a couple slides to, to wrap up and then, and then back to Poncho. Um, and,

584
00:37:46.800 --> 00:37:51.120
and hopefully I didn't take us too, too far off, off time. Um, you know, when,

585
00:37:51.120 --> 00:37:54.160
when it comes to model-based techniques, the, the whole idea is,

586
00:37:54.180 --> 00:37:58.760
is just admitting that models are wrong. Um, and, uh, you know, the whole, all,

587
00:37:58.780 --> 00:38:03.280
all of them are wrong. Some of 'em are useful. Um, a an mdsc approach,

588
00:38:03.290 --> 00:38:07.960
especially a, a static approach, which is, which is what, what s TPA is,

589
00:38:09.140 --> 00:38:13.200
uh, really just lets a group of people, you know, structure, uh,

590
00:38:13.210 --> 00:38:16.760
their beliefs about the world. Uh, and, you know, from, from,

591
00:38:16.910 --> 00:38:19.600
from a sense of what abstraction is, that's what it is, right? I mean, it,

592
00:38:19.600 --> 00:38:23.560
it can be math, it can be cave paintings, it can be, it can be art, it can be,

593
00:38:24.060 --> 00:38:26.720
uh, you know, the way we generalize our theories and the way we,

594
00:38:26.720 --> 00:38:30.400
we try to document and, and communicate, uh, what, what reality is.

595
00:38:30.400 --> 00:38:34.840
Because at the end of the day, it's all just, uh, the best fine tune, uh, um,

596
00:38:34.900 --> 00:38:38.860
understanding that we'll always keep getting updated later by, you know, uh, uh,

597
00:38:38.860 --> 00:38:43.300
smarter, more informed people down the line from you. So, so the idea that, uh,

598
00:38:43.300 --> 00:38:45.700
you bring that group together, like I mentioned the previous slide, is,

599
00:38:45.760 --> 00:38:48.380
is super important. And, um, uh,

600
00:38:48.460 --> 00:38:50.820
I would definitely stand behind.

601
00:38:50.880 --> 00:38:55.420
We don't do it enough on the engineering and development side of the military.

602
00:38:55.480 --> 00:38:57.260
We, we certainly do it on the, you know,

603
00:38:57.260 --> 00:39:00.980
all the battle planning and all the ops and all those things. But, um, you know,

604
00:39:00.980 --> 00:39:04.460
what, what we've been trying to do on, on our side of, of this, this, uh,

605
00:39:04.460 --> 00:39:06.980
you know, engineering and product development industry on, on the,

606
00:39:06.980 --> 00:39:10.500
on the government military side, is just really encourage people to, uh,

607
00:39:10.550 --> 00:39:12.460
bring all the right minds, uh,

608
00:39:12.530 --> 00:39:16.420
into a room to just make sure we're kind of on the same page before we commit to

609
00:39:16.420 --> 00:39:19.740
too many big design decisions or, um, or tactics,

610
00:39:19.740 --> 00:39:23.620
development decisions based on new technologies. And then the last slide, and I,

611
00:39:23.840 --> 00:39:27.740
and I'll hand it back after that, is, is modeling, uh, you know,

612
00:39:27.760 --> 00:39:32.420
all models are wrong, right? So we, we say use model is a verb, not as a noun.

613
00:39:33.000 --> 00:39:36.820
Uh, it's, it's the act active modeling, it's the use of abstraction. Um,

614
00:39:36.850 --> 00:39:40.500
it's the, the group interpretation of the system and the,

615

00:39:40.500 --> 00:39:43.020
and the creation of something we all can get behind on,

616
00:39:43.040 --> 00:39:45.700
on what we think the important parts of our structure are, um,

617
00:39:46.200 --> 00:39:49.460
to do all those things in the bullets, right? That, that are really,

618
00:39:49.460 --> 00:39:51.740
really important. And that's what, that's what makes modeling useful,

619
00:39:52.000 --> 00:39:55.100
and not just the artifacts of modeling, right? That the models themselves,

620
00:39:55.100 --> 00:39:58.660
which, which we all know are not 100% correct, um,

621
00:39:58.720 --> 00:40:03.380
or ever the level of fidelity that we would ever want, um, uh, actually,

622
00:40:03.520 --> 00:40:06.620
you know, able to be part of the discussion and able to be, uh,

623
00:40:06.620 --> 00:40:11.340
to lend themselves to, to usefulness to the team. So, uh, with that,

624
00:40:12.280 --> 00:40:16.500
um, I will, uh, hand it back to, to you, Sarah, and, uh, I'll,

625
00:40:16.500 --> 00:40:19.820
I'll stay online this morning. Uh, you know, appreciate everybody's time. I, I,

626
00:40:19.820 --> 00:40:22.420
I think there might be a couple, couple slides she, she pitches back to me, but,

627
00:40:22.640 --> 00:40:26.820
um, always open for questions, uh, uh, whenever, uh, those are possible. And,

628
00:40:26.820 --> 00:40:30.020
uh, appreciate, uh, appreciate the opportunity to chat with everyone. Thanks.

629
00:40:30.090 --> 00:40:30.923
Over.

630
00:40:34.950 --> 00:40:39.770
All right, thanks Mur. Um, so, so appreciate you getting us, uh,

631
00:40:39.770 --> 00:40:42.090
pretty close to back on schedule. As you can tell,

632
00:40:42.090 --> 00:40:44.370
there's a lot of meat in there, um,

633
00:40:44.390 --> 00:40:48.330
to really go into the underlying theory that, that we're gonna,

634
00:40:48.420 --> 00:40:50.810
we're gonna talk about more of a practical approach to

635
00:40:56.430 --> 00:41:00.050
All. Thank you. Um, so, so what is tpa?

636
00:41:00.360 --> 00:41:03.650
ASMR said it's a type of model based systems engineering. Um,

637
00:41:03.670 --> 00:41:06.410
but there's no software required. Uh, I've done,

638
00:41:06.530 --> 00:41:10.450
I've done many sketches on whiteboards on a piece of paper, uh,

639
00:41:10.450 --> 00:41:11.530
that type of thing, which,

640
00:41:11.530 --> 00:41:15.210
which makes it very accessible and makes it easy to do with, uh,

641
00:41:15.210 --> 00:41:17.890
with a small group of folks. Um, it's,

642
00:41:17.990 --> 00:41:20.290
it was created by Professor Nancy Levison.

643
00:41:20.390 --> 00:41:24.410
So her background is in software safety, uh, and that's where,

644
00:41:24.630 --> 00:41:29.570
that's where she, she started in computer science and then got into safety. Uh,

645
00:41:29.670 --> 00:41:33.980
she, she created, um, a few software requirements, um,

646
00:41:34.560 --> 00:41:38.460
um, books and, and then she got into the aviation side, and that's where she,

647
00:41:38.460 --> 00:41:40.300
that's where she is in at mit.

648
00:41:41.180 --> 00:41:45.280
And the big thing is focusing on emergent problems that you're not necessarily

649
00:41:45.280 --> 00:41:47.320
gonna see in a, in a failure based analysis.

650
00:41:47.320 --> 00:41:51.800
So these are system behaviors that we've inherently designed into the system,

651
00:41:51.800 --> 00:41:55.600
whether or not we've realized it. Um, and it all,

652
00:41:55.600 --> 00:41:56.960
it all goes back to the visual model.

653
00:41:56.980 --> 00:42:00.480

You're gonna see that you're gonna get a build your own today. Um,

654
00:42:00.480 --> 00:42:02.120
so it's not just documentation.

655
00:42:02.220 --> 00:42:06.200
You're gonna get documentation out of it to fulfill whatever safety, um,

656
00:42:06.270 --> 00:42:10.240
process you have in your particular organization. Um, but it,

657
00:42:10.320 --> 00:42:13.400
but it goes much deeper than that. Um, and,

658
00:42:13.540 --> 00:42:16.240
and what's really interesting is you can use it for any emergent property.

659
00:42:16.270 --> 00:42:19.560
When I was at mit, I went over to hanscomb and I was talking to,

660
00:42:19.660 --> 00:42:22.640
to some of the engineers, um, and I was,

661
00:42:22.720 --> 00:42:26.200
I was telling 'em about tpa and how it's great for safety. And,

662
00:42:26.220 --> 00:42:29.480
and this guy said, well, it sounds like it's a mission assurance technique,

663
00:42:29.900 --> 00:42:34.000
and he's 100% correct. Uh, you can use it for any,

664
00:42:34.100 --> 00:42:38.240
any emergent property that you have. So security, there's, uh, there's a,

665
00:42:38.260 --> 00:42:43.160
now retired Colonel Dollar Young. Uh, he, he actually, um, uh,

666
00:42:43.550 --> 00:42:47.800

started up a, a new wing within the Air Force, the spectrum warfare wing.

667
00:42:48.500 --> 00:42:51.200
Uh, so he actually got his PhD under Nancy as well,

668
00:42:51.300 --> 00:42:53.640
and he applied STPA to cybersecurity.

669
00:42:53.940 --> 00:42:56.520
The whole idea was you're never gonna be able to keep,

670
00:42:56.520 --> 00:42:59.720
build a moat deep enough and wide enough to keep people outta your system,

671
00:43:00.100 --> 00:43:03.720
but how can you control the behaviors that they have, uh, the ability, uh,

672
00:43:03.720 --> 00:43:06.720
to control once they're in your system? And then, of course, uh,

673
00:43:06.720 --> 00:43:10.320
performance as well is gonna come out in the analysis.

674
00:43:12.860 --> 00:43:16.480
So, uh, the safety management is, and how,

675
00:43:16.480 --> 00:43:19.200
how we do tests is gonna look a little bit different for every different

676
00:43:19.200 --> 00:43:23.000
organization, but, but roughly, uh, from the big picture, it's about the same.

677
00:43:23.260 --> 00:43:25.160
You've got a technical review phase.

678
00:43:25.260 --> 00:43:28.120
You're looking at your technical objectives, your measures of performance,

679
00:43:28.430 --> 00:43:32.960
what techniques you need to, to use to get the data that you need. Um,

680
00:43:32.960 --> 00:43:35.360
you go through that planning process, you get approval,

681
00:43:35.740 --> 00:43:38.360
and then you start the safety planning phase. You're,

682
00:43:38.360 --> 00:43:42.280
you identify various hazards and then figure out how to control those hazards

683
00:43:42.280 --> 00:43:44.440
and then document it, uh, in some method,

684
00:43:44.650 --> 00:43:49.080
often with a risk matrix to get approval, uh, from whoever is the,

685
00:43:49.080 --> 00:43:52.320
the approval authority within your organization. Uh,

686
00:43:52.320 --> 00:43:56.600
and then you go out and test with s tpa.

687
00:43:57.180 --> 00:44:00.560
Uh, you can actually do, do all the,

688
00:44:00.620 --> 00:44:05.400
the technical planning and the safety planning all together and make it

689
00:44:05.400 --> 00:44:09.760
more of a cohesive effort. And then, as I said, the output of this is,

690
00:44:09.860 --> 00:44:14.440
is something that you can utilize, uh, through the approval phase. And,

691
00:44:14.440 --> 00:44:17.520
and we found actually with the, the safety control structure, with the model,

692
00:44:17.540 --> 00:44:21.760
the visual model, that actually is really useful when you're talking, uh,

693
00:44:21.760 --> 00:44:25.440
to whoever's the approval authority in your organization to explain what the

694
00:44:25.440 --> 00:44:28.640
system does, how it functions, and how you're, you're, um,

695
00:44:28.650 --> 00:44:30.120
gonna execute the test safely.

696
00:44:33.900 --> 00:44:36.480
So s tpa can be broken down into a few steps.

697
00:44:36.580 --> 00:44:39.640
The first one is identifying your losses.

698
00:44:40.300 --> 00:44:43.680
So those are typically defined by whoever the stakeholder is in your

699
00:44:43.680 --> 00:44:48.000
organization. Could be a program office, um, could be, could be, uh,

700
00:44:48.280 --> 00:44:51.120
somebody in management of some sort. And it's what we want to prevent.

701
00:44:51.120 --> 00:44:55.360
So these are very, very high level losses. So we're talking loss of life,

702
00:44:55.360 --> 00:45:00.280
we're talking loss of the system under test, um, you know, damage to, uh,

703
00:45:00.420 --> 00:45:04.320
to infrastructure, those types of things, very high level. And next,

704
00:45:04.340 --> 00:45:05.680
you identify the hazards,

705

00:45:05.940 --> 00:45:08.400
and those are a system state that will lead to an accident.

706
00:45:08.410 --> 00:45:11.920
We'll go a little bit deeper into that, and it's traceable to your losses.

707
00:45:12.020 --> 00:45:16.080
So when you identify your hazards, you're gonna say what loss, uh,

708
00:45:16.100 --> 00:45:19.080
it would lead to. Uh, so what's nice about that?

709
00:45:19.300 --> 00:45:20.800
What's nice about that traceability?

710
00:45:20.800 --> 00:45:23.720
And Murph talked a little bit about traceability as part of systems theory,

711
00:45:23.860 --> 00:45:27.560
is it makes you continuously go back to the previous steps.

712
00:45:28.100 --> 00:45:30.040
So what happens if you identify a hazard,

713
00:45:30.460 --> 00:45:32.520
but you don't have an associated loss for it?

714
00:45:33.580 --> 00:45:38.160
So either you missed a loss or maybe it's outside the scope of,

715
00:45:38.160 --> 00:45:41.280
of your test planning. So those, those are your two things. So,

716
00:45:41.340 --> 00:45:44.240
so it allows you to go back through and look at that as you go through,

717
00:45:44.240 --> 00:45:48.080
which helps you with making sure that you get as complete of an analysis as you

718
00:45:48.100 --> 00:45:52.080
can. Um, next, you build your safety control structure.

719
00:45:52.700 --> 00:45:57.080
And we talked a little bit about that, and we'll go deep into that today. Uh,

720
00:45:57.080 --> 00:45:58.960
and then you have unsafe control actions.

721
00:45:58.960 --> 00:46:03.800
Those are commands that would leave to lead to an unsafe condition. So, uh,

722
00:46:03.810 --> 00:46:08.200
we'll go, we have an example that we'll we'll go through, but, um, you know,

723
00:46:08.200 --> 00:46:11.720
every day controllers are, are initiating some kind of command.

724
00:46:12.220 --> 00:46:13.440
So in what,

725
00:46:13.700 --> 00:46:17.480
in what situation would that command now be unsafe?

726
00:46:17.660 --> 00:46:21.440
How would that realize a hazard? And that's traceable to the hazards.

727
00:46:21.860 --> 00:46:26.800
And then lastly, you develop scenarios, uh, which is, is your deepest level.

728
00:46:26.800 --> 00:46:30.120
That's when you're getting in deep into the weeds of the interactions of your

729
00:46:30.120 --> 00:46:32.640
system, the interactions of humans with the system,

730

00:46:33.220 --> 00:46:36.960
and you're trying to def determine why a UCA might occur.

731
00:46:37.190 --> 00:46:41.120
It's kind of at that point, kind of becomes a structured brainstorming session.

732
00:46:42.300 --> 00:46:45.560
And out from the scenarios, you're gonna get your mitigations, your constraints,

733
00:46:46.380 --> 00:46:50.840
um, how whatever, uh, you need to put in place to prevent, um,

734
00:46:50.840 --> 00:46:52.280
the loss from occurring.

735
00:46:56.090 --> 00:47:00.150
All right? So another way to look at, um, traditional test safety planning,

736
00:47:00.210 --> 00:47:03.790
and then how, how s TPA feeds in. Uh, when you start off,

737
00:47:03.790 --> 00:47:06.710
you're gonna be looking for your test unique hazards.

738
00:47:07.210 --> 00:47:09.270
So some ways you may try to gather that data.

739
00:47:09.290 --> 00:47:11.590
You may look at previous tests or similar tests.

740
00:47:11.810 --> 00:47:15.990
You're gonna look at the system safety hazard analysis that was provided. Um,

741
00:47:16.090 --> 00:47:19.390
you may look at other safety reviews, modification documents,

742
00:47:19.790 --> 00:47:23.350
whatever whatever's given to you, um, based off of either, uh,

743
00:47:23.410 --> 00:47:28.030
his previous historical, um, similar programs, uh, or,

744
00:47:28.370 --> 00:47:31.980
or, uh, the actual documentation for the, for the aircraft.

745
00:47:32.600 --> 00:47:35.020
And then you're gonna look to eliminate or control those hazards.

746
00:47:35.020 --> 00:47:38.460
And there's a few ways there to do it. Uh, test design methodology.

747
00:47:38.600 --> 00:47:41.380
You can have safety devices. Uh, you can,

748
00:47:41.480 --> 00:47:45.340
you can have cautions and warnings of some sort. You can train your folks to,

749
00:47:45.400 --> 00:47:48.780
to avoid a particular situation. And we're gonna get deeper into,

750
00:47:48.930 --> 00:47:53.820
into hazards as well, how you eliminate or control those hazards. And then, um,

751
00:47:54.280 --> 00:47:58.020
lastly then you have to go through the documentation for approval.

752
00:47:58.040 --> 00:48:00.540
And that's gonna look of course a little bit different for everybody,

753
00:48:00.600 --> 00:48:02.860
but roughly you're looking, you're looking to,

754
00:48:03.480 --> 00:48:06.380
to determine what the test hazards are and how you correct those actions.

755
00:48:09.390 --> 00:48:12.450

And this works really well when you've got experienced teams and you've got

756
00:48:12.450 --> 00:48:13.930
really well known systems.

757
00:48:14.030 --> 00:48:17.170
But what happens when it's something that's completely different, uh, that,

758
00:48:17.170 --> 00:48:19.410
that no one has seen before, um,

759
00:48:19.410 --> 00:48:24.290
you don't know what the behavior's gonna look like. Uh, we are working, um,

760
00:48:24.290 --> 00:48:27.050
working with a team that's doing some AI work right now.

761
00:48:27.070 --> 00:48:32.010
So putting AI on an airplane, um, we haven't really done that before too much.

762
00:48:32.300 --> 00:48:35.130
We've done it a couple times, but not a lot. So, so what does that look like?

763
00:48:35.150 --> 00:48:39.810
How do we make sure that, that we do it in a safe manner? So for,

764
00:48:40.110 --> 00:48:43.770
uh, if you use s tpa, your losses and your hazards,

765
00:48:43.810 --> 00:48:48.330
that's how you identify your test, unique hazards. And then the other steps,

766
00:48:49.030 --> 00:48:51.050
uh, are how you eliminate the control hazards,

767
00:48:51.150 --> 00:48:54.330

and then you can input that into your normal documentation.

768
00:48:57.260 --> 00:49:01.680
So, um, we'll go through each step in a little bit more detail. Again,

769
00:49:01.680 --> 00:49:04.800
losses are what we wanna prevent. So for the Air Force Test Center,

770
00:49:04.990 --> 00:49:09.680
what we've identified as as losses with the, with the test center, uh,

771
00:49:09.870 --> 00:49:13.080
test safety office is loss of life or injury to people,

772
00:49:13.510 --> 00:49:16.440
loss of or damage to the system under test, and then loss of,

773
00:49:16.440 --> 00:49:20.720
or damage to any other infrastructure that you might have. And,

774
00:49:20.740 --> 00:49:24.280
and these are intentionally very, very high level. If you start deep,

775
00:49:24.280 --> 00:49:27.120
you don't know if you've missed something, uh, if you, so,

776
00:49:27.120 --> 00:49:29.560
but when you start high level and then work your way down,

777
00:49:29.620 --> 00:49:32.920
you can have a good idea that you're fairly complete in the analysis

778
00:49:34.520 --> 00:49:36.410
hazards, again, there are system level,

779
00:49:36.420 --> 00:49:40.530
state or condition that combined with environmental factors could lead to
a

780
00:49:40.530 --> 00:49:44.610

loss. So the two big things to take away, one is it's a system level state.

781
00:49:45.270 --> 00:49:48.250
So let's say, let's say your aircraft is having issues with propulsion.

782
00:49:48.250 --> 00:49:51.410
Propulsion is a subsystem that's not a system level state. Now,

783
00:49:51.410 --> 00:49:54.130
issues with your propulsion could create a system level,

784
00:49:54.310 --> 00:49:57.130
can condition that could lead to a hazard. Uh, and,

785
00:49:57.130 --> 00:50:00.490
and you're gonna find that later on as you go down into the analysis.

786
00:50:00.910 --> 00:50:03.450
The other piece is combined with environmental factors.

787
00:50:03.870 --> 00:50:08.530
So you can realize a hazard, but you don't necessarily realize the loss.

788
00:50:09.470 --> 00:50:09.710
Um,

789
00:50:09.710 --> 00:50:13.010
so some examples of that are controllable aircraft violates minimum separation

790
00:50:13.210 --> 00:50:16.730
distance to another air vehicle aircraft, parts controlled flight,

791
00:50:17.310 --> 00:50:18.330
or you have a,

792
00:50:18.730 --> 00:50:23.370
a weapon or store that hits outside of the intended target area. Um,

793
00:50:23.550 --> 00:50:27.620

so, um, and there we have several, several of these. We have a,

794
00:50:27.680 --> 00:50:30.220
an air force test center, uh, guide to s tpa,

795
00:50:30.240 --> 00:50:34.700
and we have several hazards that we attempted to accomp encompass all of the

796
00:50:34.700 --> 00:50:38.780
various test center units. Uh, so Eglin gets the, the last one,

797
00:50:38.800 --> 00:50:43.220
the weapon store. Um, but we also have some ground test, uh,

798
00:50:43.220 --> 00:50:48.190
safety hazards as well. So there's two different ways,

799
00:50:48.650 --> 00:50:52.070
uh, to refine a hazard, you don't necessarily have to refine hazards you,

800
00:50:52.330 --> 00:50:53.830
but you can, sometimes it's helpful.

801
00:50:54.650 --> 00:50:58.870
So controllable aircraft violates minimum separation distance to another air

802
00:50:58.870 --> 00:51:01.670
vehicle. That's one of the hazards that was defined.

803
00:51:01.670 --> 00:51:03.350
So there's two different ways you can do this.

804
00:51:04.010 --> 00:51:08.070
One is you can look at variables that need to be controlled. Um,

805
00:51:08.070 --> 00:51:11.950
so you can look at acceleration, deceleration, ascent, descent,

806
00:51:11.950 --> 00:51:16.550

that type of thing, uh, horizontal maneuvering. And then you can, you can,

807
00:51:17.010 --> 00:51:18.790
uh, refine that by saying, uh,

808
00:51:18.790 --> 00:51:23.070
you ascend or des descend into another aircraft flight path, for example.

809
00:51:25.300 --> 00:51:29.670
Another way to do it is talk about how a particular hazard becomes test

810
00:51:30.070 --> 00:51:30.690
specific.

811
00:51:30.690 --> 00:51:35.550
So maybe you have dedicated airspace that that is violated n pedostatic

812
00:51:35.650 --> 00:51:40.590
system or TCAs. Uh, so there's different things like that, um,

813
00:51:41.100 --> 00:51:44.750
that, uh, that can create, uh, a test specific hazard.

814
00:51:48.590 --> 00:51:50.280
Alright, safety control structure.

815
00:51:50.510 --> 00:51:53.640
This is really the backbone of the analysis.

816
00:51:54.460 --> 00:51:58.880
So MPH talked a lot about the structure associated with, with,

817
00:51:59.780 --> 00:52:02.360
uh, the, the model that you wanna do. So you start,

818
00:52:02.660 --> 00:52:06.280
you start with your highest controller first. Uh, so let's say,

819
00:52:06.370 --> 00:52:09.360
let's say you have a test director, maybe the test director,

820
00:52:09.740 --> 00:52:13.280
and then you've got, then you've got the test pilot, maybe, then you've got the,

821
00:52:13.620 --> 00:52:17.160
um, autopilot, and then you have the actual process, which would be, uh,

822
00:52:17.300 --> 00:52:21.520
the flight of the aircraft. It can, it contains commands and feedback.

823
00:52:21.740 --> 00:52:24.760
So the controller is providing commands to the process,

824
00:52:25.180 --> 00:52:28.880
and then that process is providing feedback back to the controller, uh,

825
00:52:28.880 --> 00:52:30.880
that informs the controller's mental model.

826
00:52:31.340 --> 00:52:33.960
And then based off of the control algorithm, uh,

827
00:52:33.960 --> 00:52:35.760
that's gonna determine what the commands are.

828
00:52:35.780 --> 00:52:39.400
So you see that feedback loop that you have there. And again,

829
00:52:39.400 --> 00:52:43.520
those can be human or automated controllers. So the control algorithm, it's,

830
00:52:43.520 --> 00:52:47.160
it's easy to think about, uh, when you, when you're talking about a, a machine,

831
00:52:47.240 --> 00:52:51.320
a computer. But we, we all also have control algorithms. Uh,

832
00:52:51.320 --> 00:52:56.000

so what we've been trained on, the procedures that we're trying to follow, uh,

833
00:52:56.020 --> 00:52:59.280
we, we got away with something once, so we think we can get away with it again,

834
00:52:59.300 --> 00:53:02.320
or we got smack down once. So we're never gonna do that again.

835
00:53:02.730 --> 00:53:06.880
Those all feed into the control algorithms that we have in our head that,

836
00:53:06.880 --> 00:53:11.320
that are gonna define, uh, what commands we, we choose to do, um,

837
00:53:11.320 --> 00:53:12.880
based off of the feedback that we have.

838
00:53:13.340 --> 00:53:17.680
And what's really important about s CPA is it includes the entire sociotechnical

839
00:53:17.680 --> 00:53:21.440
system. You don't just have the aircraft and then a human, uh,

840
00:53:21.440 --> 00:53:25.700
you have both combined, and that, that makes this, this technique very powerful.

841
00:53:26.680 --> 00:53:28.500
And when you build your safety control structure,

842
00:53:28.800 --> 00:53:32.380
you want it to be at the highest level of useful abstraction. Um,

843
00:53:32.380 --> 00:53:36.260
so you can go down super into the weeds, but it's gonna make your analysis very,

844
00:53:36.260 --> 00:53:40.100

very hard. So start high level, and then if you find that you need to go deeper,

845
00:53:40.520 --> 00:53:44.940
you need to, you break out a particular element into, into smaller elements,

846
00:53:44.940 --> 00:53:48.060
you can do that. It's way easier to break out than it is to,

847
00:53:48.320 --> 00:53:49.500
to start super detailed.

848
00:53:53.770 --> 00:53:57.070
All right, so Murph talked about box. We've got the quote there,

849
00:53:57.090 --> 00:54:00.710
that's the actual quote of all models are wrong, but some are useful.

850
00:54:03.980 --> 00:54:07.790
It's definitely been, uh, been shortened over time.

851
00:54:11.020 --> 00:54:11.540
Uh,

852
00:54:11.540 --> 00:54:15.720
so we talked about the system theoretic convention with the controller and the

853
00:54:15.720 --> 00:54:17.080
process. Um,

854
00:54:17.260 --> 00:54:21.440
so this just goes into how you can have a full structure with multiples of

855
00:54:21.720 --> 00:54:23.960
controllers and processes throughout your system.

856
00:54:28.630 --> 00:54:33.050
And I'm sure a lot of you have seen this, this interface, uh, diagram before.

857
00:54:33.120 --> 00:54:36.490
It's pretty common in systems architecture, systems engineering.

858
00:54:36.600 --> 00:54:39.970
What we're really focused on is that information flow at the bottom.

859
00:54:40.550 --> 00:54:45.410
So how are we transmitting data? How are we transmitting commands? Um, and,

860
00:54:45.410 --> 00:54:47.370
uh, and how are those commands being developed?

861
00:54:49.290 --> 00:54:52.270
And right now that's really not covered well under,

862
00:54:52.480 --> 00:54:57.340
under traditional hazard analysis. All right? So I'm gonna,

863
00:54:58.030 --> 00:55:02.100
Murph created these for his PhD, so I'm gonna attempt to hand it back to him,

864
00:55:03.080 --> 00:55:03.913
see how this goes.

865
00:55:12.610 --> 00:55:14.630
Hey, we don't hear you yet. Can you hear me?

866
00:55:16.050 --> 00:55:20.710
Uh, yes, I can, I can hear you. Uh, how me, any better?

867
00:55:21.050 --> 00:55:25.850
Yep. Okay. Awesome. Uh, okay,

868
00:55:25.990 --> 00:55:30.770
so, um, these are both flying examples. Uh, so,

869
00:55:30.790 --> 00:55:34.450
so great, great for this crowd, right? Um, the, uh, uh,

870
00:55:34.470 --> 00:55:38.210
so what you see is a bunch of boxes and, uh, that's on purpose. Uh,

871
00:55:38.210 --> 00:55:39.210
so if you've never seen a, um,

872
00:55:39.450 --> 00:55:43.010
a safety control structure or a functional control diagram, uh, the,

873
00:55:43.010 --> 00:55:46.370
these are examples of what they could look like. And, and, um, there's,

874
00:55:46.370 --> 00:55:47.850
there's one or two more slides with,

875
00:55:47.850 --> 00:55:51.810
with similar things on 'em here that we'll go through. Um, the whole point,

876
00:55:51.810 --> 00:55:55.290
and I I think I mentioned earlier, is, uh, treat, treat every,

877
00:55:55.290 --> 00:55:59.490
everything that you consider, uh, an agent or a node, uh, the same. So,

878
00:56:00.190 --> 00:56:04.370
uh, it's all, it's all a container and it's all receiving, uh, giving commands,

879
00:56:04.370 --> 00:56:06.290
receiving feedbacks, uh,

880
00:56:06.290 --> 00:56:10.690
looking for other information or even doing a lateral, uh, coordination. In,

881
00:56:10.710 --> 00:56:13.890
in some cases, the, um, the,

882
00:56:13.950 --> 00:56:16.330

the real thing you're going for is that from the top down,

883
00:56:16.470 --> 00:56:19.850
you're putting the things that have more, um, authority,

884
00:56:19.850 --> 00:56:24.540
responsibility or accountability, uh, at the top of the diagram. And then,

885
00:56:24.800 --> 00:56:28.060
um, all the way down to kind of like, uh, what you'd call the bare airframe,

886
00:56:28.060 --> 00:56:31.900
or what you would call just kind of the, the bare physical processes, um,

887
00:56:32.010 --> 00:56:34.860
more near the, the bottom. Um, I've,

888
00:56:34.860 --> 00:56:37.420
I've called these functional control diagrams before because sometimes you,

889
00:56:37.480 --> 00:56:40.700
you haven't designed the whole system yet, and you just know that, uh,

890
00:56:40.780 --> 00:56:45.420
a thing has to do a thing. Uh, so you might draw a very vague, you know, uh, uh,

891
00:56:45.480 --> 00:56:50.180
box around, uh, this function of, you know, flying or piloting or, or, um,

892
00:56:50.560 --> 00:56:52.180
uh, you know, uh, runtime,

893
00:56:52.180 --> 00:56:55.340
assurance wrappers are something that we're dealing with heavily right now with,

894
00:56:55.340 --> 00:56:59.580

with, with our, uh, our satellite programs. So, um, when it gets into autonomy,

895
00:56:59.760 --> 00:57:00.820
so, um, you know,

896
00:57:00.820 --> 00:57:03.620
the whole idea is that you're just abstracting and capturing the things that you

897
00:57:03.620 --> 00:57:07.700
think matter. Um, so what you have on the left is, uh,

898
00:57:07.780 --> 00:57:11.700
a two aircraft, uh, um, scenario with, uh,

899
00:57:11.700 --> 00:57:15.700
with some next gen tech, the trans oceanic, uh, in trail procedure, which, uh,

900
00:57:15.920 --> 00:57:16.980
allows, uh,

901
00:57:17.260 --> 00:57:20.340
airplanes that are flying over the ocean to be spaced a little closer to each

902
00:57:20.340 --> 00:57:24.460
other than they normally are. Uh, because now you have a D S B, um,

903
00:57:24.460 --> 00:57:29.140
talking amongst themselves and, uh, presenting more accurate, uh, relative, uh,

904
00:57:29.140 --> 00:57:31.380
you know, position of velocity data between the aircraft,

905
00:57:31.380 --> 00:57:33.900
which air traffic control can then, uh, you know,

906
00:57:34.030 --> 00:57:37.100
based on whatever those aircraft are, transmitting back,

907
00:57:37.370 --> 00:57:39.100
even though they're not on radar, uh,

908
00:57:39.100 --> 00:57:41.860
can have a better confidence that the airplanes can be closer to each other cuz

909
00:57:41.860 --> 00:57:45.180
you have higher fidelity, uh, between the, the A DS B beacons on the aircraft.

910
00:57:45.320 --> 00:57:46.260
So, uh, you know,

911
00:57:46.260 --> 00:57:51.260
what you see there is we've drawn a big gray container around each aircraft and

912
00:57:51.260 --> 00:57:55.540
then within the aircraft. Um, yeah, whoever modeled this, and it wasn't me, I,

913
00:57:55.620 --> 00:57:59.180
I just, uh, put it in physio, um, decided that, you know,

914
00:57:59.200 --> 00:58:03.140
the components that matter for the discussion are the flight crew of each

915
00:58:03.460 --> 00:58:06.420
aircraft, um, not even in the individual persons, right? You know,

916
00:58:06.420 --> 00:58:10.940
we're just gonna need the analysis on, on the crew. Um, the flight computer,

917
00:58:11.070 --> 00:58:15.620
which at itself is a, a complex hardware, you know, uh, software suite,

918
00:58:15.640 --> 00:58:18.260
but we're gonna call it the flight computer, the barrier air frame,

919
00:58:18.260 --> 00:58:22.980
and then those a dsb, uh, systems that can, uh, uh, talk to each other,

920
00:58:23.840 --> 00:58:28.140
uh, across those, those cor, those green coordination lines. Um, you know, uh,

921
00:58:28.200 --> 00:58:31.580
the, the color convention I, I like to use is, is, you know,

922
00:58:31.580 --> 00:58:35.780
black arrows and blue arrows, uh, where, where appropriate for controls and, uh,

923
00:58:35.780 --> 00:58:37.940
and feedbacks and then creates for coordination.

924
00:58:37.940 --> 00:58:40.460
It just makes it easier on my eyes and, and, uh, you know,

925
00:58:40.460 --> 00:58:43.020
cleans up the diagram a little bit, and you'll notice that I,

926
00:58:43.100 --> 00:58:45.620
I number all of the, the connections,

927
00:58:45.620 --> 00:58:48.660
because then I can just have a lookup table, uh, you know, elsewhere in the,

928
00:58:48.660 --> 00:58:50.860
in the plan that actually tells you what all those, uh,

929
00:58:50.860 --> 00:58:53.740
command and feedback channels are. Um, you know, they can be visual,

930
00:58:53.770 --> 00:58:58.380
they can be verbal, they can be, uh, through wire, through airwaves,

931
00:58:58.800 --> 00:59:00.380
uh, et cetera. Um, the,

932
00:59:00.380 --> 00:59:03.900
the cool thing about this is that it really doesn't matter how that,

933
00:59:03.900 --> 00:59:05.780
that the things are connected with each other. It's just that,

934
00:59:05.780 --> 00:59:08.420
that the idea that they are connected to each other and that the,

935
00:59:08.420 --> 00:59:12.420
they do have these, um, these, uh, hierarchical roles, uh,

936
00:59:12.420 --> 00:59:16.460
with respect to each other. Uh, on the right was a, was a fun analysis. I,

937
00:59:16.620 --> 00:59:20.500
I got to do a test pilot school, uh, gosh, close to 10 years ago, if,

938
00:59:20.500 --> 00:59:25.300
if anyone's tracking that the, uh, F 16 Vista was, uh, renamed, uh, an xplan.

939
00:59:25.330 --> 00:59:29.060
It's the X 62 now, and it's, it's been on the news a lot, uh, doing a lot of,

940
00:59:29.060 --> 00:59:32.300
uh, autonomous, uh, pilot research. Um, it's,

941
00:59:32.300 --> 00:59:35.420
it all started out with figuring out if we could just put a, a, a, you know,

942
00:59:35.540 --> 00:59:39.700
a dumb autopilot in inside, inside that airplane when it was still the vista.

943
00:59:40.360 --> 00:59:43.220
So, um, as far as color coding, um, and,

944
00:59:43.220 --> 00:59:47.580
and I'm a big fan of using coding, uh, when you're, when you're doing models,

945
00:59:47.580 --> 00:59:50.900
when you're doing visuals, right? So I, so I use color coding a lot. Uh,

946
00:59:50.900 --> 00:59:54.380
what we have there is in magenta is the, the,

947
00:59:54.440 --> 00:59:57.220
the new thing that you're trying to test or evaluate.

948
00:59:57.800 --> 01:00:02.780
And then an orange is the test infrastructure that is helping you

949
01:00:02.780 --> 01:00:07.020
with that evaluation, but that would not exist out in the field in real life.

950
01:00:07.640 --> 01:00:11.580
And then the things in the normal, you know, that just that the non, uh,

951
01:00:11.580 --> 01:00:15.660
colored containers there are, um, just the things that you would expect to,

952
01:00:15.680 --> 01:00:18.300
to see out there in the field. So, you know, uh, this,

953
01:00:18.400 --> 01:00:20.900
in this particular set of testing, you had, um,

954
01:00:21.140 --> 01:00:25.620
a lead aircraft and a test aircraft. Uh, so the lead aircraft was just a normal,

955
01:00:26.360 --> 01:00:30.860
uh, fighter jet. The test aircraft was, was that vista. Um, and, uh,

956
01:00:31.200 --> 01:00:35.940

we had this Ma Jetta automated pilot flying formation, uh,

957
01:00:35.940 --> 01:00:39.740
against the, uh, the gray jet. Um, that was the, the formation lead.

958
01:00:39.960 --> 01:00:41.780
And the way it knew, uh,

959
01:00:41.780 --> 01:00:45.700
where it was with respect to the other airplane is we put, we modified some,

960
01:00:46.250 --> 01:00:50.460
some old weapons pods and actually put some, some com software, uh, on them.

961
01:00:50.520 --> 01:00:54.780
And, and, uh, and had some, uh, some good, uh, uh, time space position,

962
01:00:55.400 --> 01:00:57.420
uh, solutions happening on both airplanes.

963
01:00:57.420 --> 01:00:59.900
And then these two pods were talking to each other, uh,

964
01:00:59.900 --> 01:01:02.820
while the airplanes were flying and passing that data back and forth. So,

965
01:01:02.840 --> 01:01:06.100
so kind of like a, you know, like a, like a MacGyver, uh,

966
01:01:06.380 --> 01:01:10.020
a DSB ish type type thing. But just for the, for the purposes of, uh,

967
01:01:10.020 --> 01:01:14.980
of this exact kind of test. Um, and, uh, and those pods talk to each other.

968
01:01:15.240 --> 01:01:20.180
Uh, you can see, uh, uh, another, uh, short, uh, uh,

969

01:01:20.280 --> 01:01:22.060
set of green, uh, uh,

970
01:01:22.060 --> 01:01:25.980
coordination lines between the two gray containers themselves. And, and that's,

971
01:01:25.980 --> 01:01:28.740
that's just the idea that the airplanes hopefully are, uh,

972
01:01:28.920 --> 01:01:31.660
are within visual sight of each other. Uh,

973
01:01:31.660 --> 01:01:35.540
and we don't abstract any anymore further in than that. And then you've got, uh,

974
01:01:35.540 --> 01:01:39.580
you've got, uh, a command and a feedback line as you look up a little higher in,

975
01:01:39.580 --> 01:01:42.020
in between the two grade, uh, diagrams of the,

976
01:01:42.050 --> 01:01:46.020
that lead pilot sending radio commands to the other airplane,

977
01:01:46.020 --> 01:01:48.220
because there are test pilots, uh,

978
01:01:48.220 --> 01:01:52.340
to test pilots and evaluator and a safety pilot inside of that surrogate, uh,

979
01:01:52.460 --> 01:01:56.180
x x 62, um, you know, uh, to coordinate the test itself,

980
01:01:56.180 --> 01:01:58.900
and then just make sure you can set up each test point, right? So there's that,

981
01:01:58.900 --> 01:02:02.940

that command and, and feedback relationship there. Um, and then, you know, uh,

982
01:02:03.030 --> 01:02:06.460
where able, uh, you know, draw your, your, uh,

983
01:02:06.460 --> 01:02:10.260
your green arrows with where they're at the bottom between the airplanes. Um,

984
01:02:10.440 --> 01:02:14.340
and now, um, you can choose to do this. You can choose not to do this, but, um,

985
01:02:14.340 --> 01:02:14.800
you know, the,

986
01:02:14.800 --> 01:02:18.060
the idea that we're flying these airplanes really close to each other means that

987
01:02:18.060 --> 01:02:21.500
there might be some horizontal interactions, uh, that are undesirable, uh,

988
01:02:21.500 --> 01:02:24.420
between the airplanes. So, uh, so, you know, in this particular case, I,

989
01:02:24.460 --> 01:02:25.460
I chose to show that yes,

990
01:02:25.460 --> 01:02:28.260
that physical relationship between the two bare airframes, um,

991
01:02:28.280 --> 01:02:31.860
is something that we have to be thinking about. Um, and as you,

992
01:02:31.860 --> 01:02:36.300
as you abstract up, uh, you can see the, the air traffic control structure,

993
01:02:36.840 --> 01:02:40.740

uh, other aircraft, um, whenever we're talking about, uh,

994
01:02:40.740 --> 01:02:45.460
congested airspace or, uh, or situations where there are gonna be more than,

995
01:02:45.530 --> 01:02:48.060
than one thing that you care about up in the airspace,

996
01:02:48.060 --> 01:02:51.940
we'll usually have the abstract, kind of like the other, uh, container there.

997
01:02:51.940 --> 01:02:55.420
We do that a lot with, um, some of the work I'm doing now with, uh, with,

998
01:02:55.420 --> 01:02:58.700
with satellites flying close to each other and, and those types of things, or,

999
01:02:58.700 --> 01:02:59.260
you know,

1000
01:02:59.260 --> 01:03:02.460
refueling in space and all these super g whiz things that we're thinking about

1001
01:03:02.460 --> 01:03:04.060
doing now. Um, you know,

1002
01:03:04.060 --> 01:03:06.940
you wanna consider the other when you're doing the analysis and,

1003
01:03:06.940 --> 01:03:09.820
and maybe a lot of your analysis focuses on that relationship with,

1004
01:03:09.820 --> 01:03:14.220
with that container and, and your own, uh, test aircraft. Uh,

1005
01:03:14.220 --> 01:03:17.060
or maybe it's, it's just something that you're acknowledging and that you're,

1006
01:03:17.060 --> 01:03:20.300
you're looking at a few scenarios, um, that, that involve the other,

1007
01:03:20.640 --> 01:03:25.490
the other player, if you will. And, uh, and the last thing I'll point out, uh,

1008
01:03:25.630 --> 01:03:29.930
is that, uh, and, and by the way, I, you know, I, I know this is, uh,

1009
01:03:30.700 --> 01:03:34.130
quite a lot to glaze over, right? And you're looking at, at diagrams like this,

1010
01:03:34.150 --> 01:03:37.250
and, and, uh, you know, as Pancho mentioned, we normally, um, you know,

1011
01:03:37.250 --> 01:03:42.050
we'll spend a, a whole, a whole half day plus just, just architecting and just,

1012
01:03:42.050 --> 01:03:46.210
just playing with models. So, uh, you know, forgive the brevity on this. Um,

1013
01:03:46.470 --> 01:03:50.370
but, uh, you know, the last container I'll point out is, uh,

1014
01:03:50.370 --> 01:03:53.490
that maintenance team on the top, right? Uh,

1015
01:03:53.490 --> 01:03:57.610
this was something that for the purpose of this analysis, we decided to include,

1016
01:03:58.120 --> 01:04:02.330
because there's so much that goes into instrumenting and getting,

1017
01:04:02.910 --> 01:04:05.610
uh, your test equipment ready for evaluation,

1018
01:04:05.960 --> 01:04:10.730
that even though the maintenance team is not there physically during the

1019
01:04:10.730 --> 01:04:14.490
actual mission, they do have a role, um, you know, uh,

1020
01:04:14.560 --> 01:04:18.530
controlling and having an impact on the things that you care about, um,

1021
01:04:18.530 --> 01:04:21.770
before the mission. So these models are, you know,

1022
01:04:21.800 --> 01:04:26.010
effectively temporarily agnostic. Um, uh, they're just static models of,

1023
01:04:26.070 --> 01:04:30.490
of everybody and, and every agent that's involved, uh, in, in your project.

1024
01:04:30.790 --> 01:04:34.410
So if, if you really wanted to flesh this out, you might have the, you know,

1025
01:04:34.410 --> 01:04:38.850
the management that talks to the maintenance team that coordinates with the ops,

1026
01:04:39.390 --> 01:04:41.210
uh, you know, mission planning team and,

1027
01:04:41.210 --> 01:04:43.170
and those types of things as part of your analysis, if,

1028
01:04:43.170 --> 01:04:44.730
if you think that it's important and enough to,

1029
01:04:44.910 --> 01:04:48.450
to make sure that all those communications and coordinations are, um, you know,

1030
01:04:48.450 --> 01:04:51.770

are buttoned up the way that, that you would want. Uh, and,

1031
01:04:51.770 --> 01:04:54.850
and then just the last thing before we, we get off of this slide is, uh,

1032
01:04:54.910 --> 01:04:58.690
you know, there's a lot of containers there, right? Um, it's, it's, uh,

1033
01:04:58.720 --> 01:05:01.050
this model did not start out that way. Um,

1034
01:05:01.110 --> 01:05:03.890
I'm pretty sure I started out with three boxes. Um,

1035
01:05:03.950 --> 01:05:08.610
it was just air traffic control, um, vanilla airplane and test airplane.

1036
01:05:09.550 --> 01:05:12.610
And I started drawing the relationships between those. And then I, you know,

1037
01:05:12.650 --> 01:05:15.890
I would go and interview the, the test team and the engineering team and the,

1038
01:05:15.890 --> 01:05:18.660
and the ops, and I would say, Hey, what are the, what are, what's,

1039
01:05:18.660 --> 01:05:21.380
what's your flow look like? What are you controlling? You know, how,

1040
01:05:21.400 --> 01:05:25.980
how the heck does this super complicated F 16 Vista work? Um,

1041
01:05:26.160 --> 01:05:30.820
and I, I spent, uh, several days trying to, uh, uh, understand that as,

1042
01:05:30.820 --> 01:05:34.140
as not a software guy. Um, and then you,

1043
01:05:34.240 --> 01:05:37.420

you slowly add more detail as your,

1044
01:05:37.970 --> 01:05:42.420
your scope and your process, uh, kind of, kind of dictates that, you know,

1045
01:05:42.420 --> 01:05:45.740
more stuff matters under the hood. So you, so you start adding more containers.

1046
01:05:46.000 --> 01:05:49.900
That's, that's the, the right way to do this. Um, I am an engineer.

1047
01:05:49.900 --> 01:05:53.380
There's a lot of engineers, uh, you know, in the room today, I'm sure. And, and,

1048
01:05:53.480 --> 01:05:55.020
and we all work with a lot of engineers.

1049
01:05:55.120 --> 01:05:59.940
It is very easy to draw like a million boxes. Uh, so we, we always encourage,

1050
01:06:00.320 --> 01:06:03.460
um, you know, start simple, ask all the questions at the beginning,

1051
01:06:03.750 --> 01:06:05.260
bring the experts as you need to,

1052
01:06:05.260 --> 01:06:07.700
to understand what matters in your system a little better,

1053
01:06:07.840 --> 01:06:11.340
and then start adding a little bit more detail. Um, because you,

1054
01:06:11.360 --> 01:06:15.420
you will be analyzing every relationship between, uh, each of these containers.

1055
01:06:16.280 --> 01:06:18.500
All right? Uh, you can go to the, the next slide, please.

1056
01:06:22.820 --> 01:06:26.750
This was, uh, uh, a more,

1057
01:06:26.950 --> 01:06:30.870
I would say integrated system with a lot of management layers. Uh, it's,

1058
01:06:30.870 --> 01:06:34.750
you know, it's military example, um, uh, which, uh, we, you know, we actually,

1059
01:06:34.890 --> 01:06:38.990
uh, in Space Force, we work with the Missile defense agency quite a bit. So, uh,

1060
01:06:38.990 --> 01:06:42.550
so a lot of my students kind of light up when they see, uh, a diagram like this.

1061
01:06:42.930 --> 01:06:45.710
Uh, and there's, you know, an absolute gazillion, uh,

1062
01:06:45.710 --> 01:06:49.110
examples of things going right and things going wrong, uh, you know, in, in,

1063
01:06:49.110 --> 01:06:52.750
in military scenarios that Dr. Levison, uh, likes to use as well. Uh,

1064
01:06:52.750 --> 01:06:56.830
what if her other Air Force students, Kip Johnson put this together as part of,

1065
01:06:56.830 --> 01:07:00.310
part of his thesis. He, he was very interested in coordination, uh,

1066
01:07:00.310 --> 01:07:03.310
that that horizontal relationship between controllers, uh,

1067
01:07:03.310 --> 01:07:05.670
and this is just one of the examples that he, uh, that he came up with.

1068
01:07:05.770 --> 01:07:08.310
So a lot of acronym soup there, a lot of military jargon,

1069
01:07:08.310 --> 01:07:11.910
but you can kind of see that, um, you know, down there at the bottom of,

1070
01:07:11.910 --> 01:07:13.630
of this hierarchy. And, and by the way,

1071
01:07:13.630 --> 01:07:16.750
you've probably noticed that these hierarchies are perfect, uh, pyramids, right?

1072
01:07:16.750 --> 01:07:20.470
Or, or like bowling pin setups, um, like some of the more, uh, you know,

1073
01:07:20.500 --> 01:07:23.670
cave a pictures we show you earlier in the slideshow, um, you know, the,

1074
01:07:23.670 --> 01:07:26.950
the hierarchies are whatever they are. Um, so, uh,

1075
01:07:26.950 --> 01:07:29.950
you can see that there's kind of the, the actual, you know,

1076
01:07:29.950 --> 01:07:32.590
the frontline bare physics happening there at the bottom to,

1077
01:07:32.590 --> 01:07:34.990
to the level that you want to analyze it. And then as you,

1078
01:07:34.990 --> 01:07:38.710
you go up higher in the, in the diagram, you see more authority, responsibility,

1079
01:07:38.710 --> 01:07:43.510
accountability, uh, more, uh, decision making as kind of the central focus,

1080
01:07:44.130 --> 01:07:46.430
uh, versus the actual, uh, activity happening.

1081
01:07:46.650 --> 01:07:51.390
But those communication links and those decisions are very

1082
01:07:51.390 --> 01:07:55.270
much, uh, you know, I I'd say at the center of the discussion on, you know,

1083
01:07:55.270 --> 01:07:58.870
how things can go wrong or how things can can, can be allowed to,

1084
01:07:58.870 --> 01:08:03.510
to maybe deviate from normalcy and, and get into a, a situation where, uh,

1085
01:08:03.510 --> 01:08:06.270
you know, your, your unpredictable environment can take advantage of,

1086
01:08:06.270 --> 01:08:10.070
of a system that's not resilient enough. All right, next slide.

1087
01:08:14.710 --> 01:08:19.670
And I, I think this is, uh, this might be my, my get back off the stage slide.

1088
01:08:20.050 --> 01:08:22.750
Um, but, uh, um, you know, you can,

1089
01:08:22.930 --> 01:08:27.550
you can go up as high as you think your analysis

1090
01:08:28.150 --> 01:08:31.430
requires. Uh, and you know, we, we always joke, well, you know,

1091
01:08:31.430 --> 01:08:34.910
at the end of the day, it's Congress's fault, right? Um, at least in the,

1092
01:08:34.930 --> 01:08:39.230
in the government, uh, uh, military complex. But, um, you know, this is,

1093
01:08:39.260 --> 01:08:42.910

this is a very tongue in cheek diagram way of just saying, um,

1094
01:08:42.940 --> 01:08:47.510
it's not just the actual things flying around the actual flight operations,

1095
01:08:47.580 --> 01:08:52.430
test operations, et cetera. Uh, it, it can be the entire, um, you know,

1096
01:08:52.530 --> 01:08:57.150
sociotechnical infrastructure, uh, that might have some areas that,

1097
01:08:57.150 --> 01:09:01.030
that you're interested in, in looking at. Um, and, uh, you know, we've,

1098
01:09:01.090 --> 01:09:03.070
you know, on the Air Force side, certainly with,

1099
01:09:03.070 --> 01:09:05.910
with me having more recent exposure to the way the,

1100
01:09:05.910 --> 01:09:09.590
the Air Force and Space Force are treating accident investigations now, um,

1101
01:09:09.590 --> 01:09:11.830
and certainly on the industry side, there's, you know, we,

1102
01:09:11.850 --> 01:09:14.550
we always do see a lot of examples where, um, you know,

1103
01:09:14.550 --> 01:09:18.710
you trace back up and you see a lot of, uh, a lot of those relationships, uh,

1104
01:09:18.730 --> 01:09:21.630
at, at those management layers that, uh, you know, that, you know,

1105
01:09:21.630 --> 01:09:24.790
can always be, um, you know, looked at a little bit more to kind of see how,

1106
01:09:24.810 --> 01:09:27.910
how things influence decisions and how things influence the way that we, uh,

1107
01:09:27.930 --> 01:09:31.110
you know, that we actually fly our, our airplanes and, and do our things. So,

1108
01:09:31.530 --> 01:09:35.990
um, my research was very lifecycle focused, so that's why I created this, uh,

1109
01:09:35.990 --> 01:09:40.070
this diagram. I mod modified it off something in one of Nancy's textbooks, um,

1110
01:09:40.070 --> 01:09:42.630
to just really think about, uh, testing as well as the,

1111
01:09:42.630 --> 01:09:47.150
the design and the feeling of a system. So, uh, back, back to you poncho, and,

1112
01:09:47.150 --> 01:09:49.390
uh, and I'll, uh, I'll, I'll keep staying online for, uh,

1113
01:09:49.390 --> 01:09:51.030
for any good discussions. Thanks. Over,

1114
01:09:53.680 --> 01:09:55.660
All right? Uh,

1115
01:09:55.660 --> 01:09:59.500
so we will not be building a safety control structure quite that complex today,

1116
01:10:00.120 --> 01:10:02.340
uh, with any luck if we do our jobs right?

1117
01:10:05.480 --> 01:10:09.260
All right. So, so a little bit deeper into, into the controller itself.

1118
01:10:09.320 --> 01:10:12.740
We talked about, talked about the mental model, we talked about feedback.

1119
01:10:12.800 --> 01:10:16.940
We talked about the, the, uh, control algorithm, um,

1120
01:10:17.600 --> 01:10:22.020
and how they, they feed into each other. Um, so the mental model,

1121
01:10:22.650 --> 01:10:23.700
it's the, it's,

1122
01:10:24.010 --> 01:10:27.700
it's what you believe or the autopilot leaves or whatever the controller might

1123
01:10:27.720 --> 01:10:32.060
be, uh, that that's the real time system or state of the system.

1124
01:10:32.840 --> 01:10:35.980
Um, and so, so examples of that for the,

1125
01:10:36.000 --> 01:10:39.340
for a car might be what speed are you going? Uh, what,

1126
01:10:39.340 --> 01:10:41.260
what's your fuel quantity? What's,

1127
01:10:41.400 --> 01:10:45.700
what's the position of your vehicle in relation to other vehicles or other

1128
01:10:45.980 --> 01:10:49.100
obstacles that you have, uh, in the, in the environment.

1129
01:10:49.520 --> 01:10:54.260
So those are all things that, that, um, ought to be understood, uh,

1130
01:10:54.260 --> 01:10:57.820
as you drive your car. And we'll go through a driving car example, uh,

1131
01:10:57.820 --> 01:11:01.260
cuz it's easy, I assume everyone has driven a car at some point in their life,

1132
01:11:01.640 --> 01:11:04.660
uh, in this room. Could be wrong, but I'm assuming that.

1133
01:11:08.200 --> 01:11:09.820
And then the control algorithm, again,

1134
01:11:09.820 --> 01:11:13.220
it's a set of rules and functions that enable you to make, uh,

1135
01:11:13.380 --> 01:11:17.260
decisions about what actions to perform. So, so that can be, you know,

1136
01:11:17.260 --> 01:11:21.700
literally a hard coded algorithm in some kind of, um, uh,

1137
01:11:22.210 --> 01:11:26.220
autopilot or, or controller hardware or something like that. Um, but it's also,

1138
01:11:26.520 --> 01:11:28.660
uh, what's been encoded in our human brains.

1139
01:11:30.880 --> 01:11:34.580
And so we'll think a lot about, about the input. So, um,

1140
01:11:35.490 --> 01:11:39.660
I'll tell a try to, uh, I'm gonna skip the story cuz we're running out of time.

1141
01:11:39.660 --> 01:11:42.340
If we have later, I'll, if we have time later, I'll, uh,

1142
01:11:42.530 --> 01:11:45.820
tell a story about that. But some additional things to think about, we can,

1143
01:11:45.840 --> 01:11:50.020

we can think about, um, uh, you know, the, the process,

1144
01:11:50.450 --> 01:11:51.700
what sensors we have,

1145
01:11:52.130 --> 01:11:56.380
what information those sensors are providing to the controller. Uh,

1146
01:11:56.380 --> 01:12:00.100
we can talk about the actuator based off of, uh, the, the, um,

1147
01:12:00.200 --> 01:12:02.060
the control or the command, excuse me.

1148
01:12:02.240 --> 01:12:06.420
And then the actuator actually sending something to the controlled process. Um,

1149
01:12:06.420 --> 01:12:10.820
and then of course, if, if this is a lower level, lower level controller,

1150
01:12:10.820 --> 01:12:14.460
you're gonna have feedback and commands coming from a higher level controller.

1151
01:12:15.080 --> 01:12:18.540
You may have other measurements that's coming into your system. Um,

1152
01:12:18.540 --> 01:12:20.100
you also may have other controllers.

1153
01:12:20.280 --> 01:12:23.220
So Murph talked about some of the cross collaboration with the,

1154
01:12:23.280 --> 01:12:26.180
the patriot missile battery example. Uh,

1155
01:12:26.180 --> 01:12:31.140
so maybe you have multiple controllers within your system from at a horizontal

1156

01:12:31.140 --> 01:12:35.660
level versus vertical. So what, what does that cross control look like? Um,

1157
01:12:35.660 --> 01:12:38.940
and you may have other controllers going directly to your controlled process,

1158
01:12:39.480 --> 01:12:42.260
um, maybe some sort of, uh, safety system that,

1159
01:12:42.260 --> 01:12:46.340
that might turn off the process or something along those lines. Um,

1160
01:12:46.340 --> 01:12:48.900
another thing to think about, you know, we talked about cybersecurity,

1161
01:12:49.250 --> 01:12:52.460
that other controller may not be friendly. Uh, so,

1162
01:12:52.460 --> 01:12:55.500
so how does that affect your system as you're designing it?

1163
01:12:58.140 --> 01:13:01.720
All right, so now we're gonna get into unsafe control actions. Again,

1164
01:13:02.030 --> 01:13:04.880
this is a control action that, that you have in your system,

1165
01:13:05.260 --> 01:13:07.160
but there's something that, uh, a state,

1166
01:13:07.160 --> 01:13:11.200
something about the state of the system that will lead to an unsafe condition

1167
01:13:11.700 --> 01:13:15.240
and, and potentially realize a hazard. Uh, so example,

1168
01:13:15.630 --> 01:13:19.040
when is applying brakes, um, while driving safe,

1169
01:13:19.710 --> 01:13:22.720
this is when I get to the interactive part.

1170
01:13:26.820 --> 01:13:27.580
Stop sign.

1171
01:13:27.580 --> 01:13:31.150
Yeah, stop sign. Yep. The car in front of you stops.

1172
01:13:31.220 --> 01:13:35.030
It's generally a good idea to stop when they stop. Yep.

1173
01:13:35.210 --> 01:13:36.510
And when would it be unsafe?

1174
01:13:40.980 --> 01:13:45.520
Icy road, your road conditions. Yep. I heard something else over here. Yep.

1175
01:13:45.520 --> 01:13:47.880
Middle of the highway, you've got somebody behind you,

1176
01:13:47.880 --> 01:13:52.600
doesn't know you're gonna stop. Yep. Those are all good ones. Um,

1177
01:13:53.230 --> 01:13:57.840
yeah. So location of vehicles relative to your vehicle. Road conditions. Uh,

1178
01:13:57.850 --> 01:13:59.440
there may be some others out there as well.

1179
01:14:02.610 --> 01:14:06.950
So ucas fall into one of four categories. If, uh,

1180
01:14:07.700 --> 01:14:09.790
Nancy's done some fancy math that,

1181
01:14:09.860 --> 01:14:14.340
that I do not understand that it's proven that if, that, if you fill out these,

1182
01:14:14.340 --> 01:14:18.300
these categories, your analysis should be complete. Uh,

1183
01:14:18.360 --> 01:14:22.780
so the first one is not provided, so, so I don't provide breaks. Um,

1184
01:14:22.800 --> 01:14:24.980
the second one is provided. So I do provide breaks.

1185
01:14:25.640 --> 01:14:30.060
The next one is provided too soon, too late or out of order.

1186
01:14:30.360 --> 01:14:32.860
So maybe you have a checklist and you have an order that you have to do things,

1187
01:14:33.760 --> 01:14:38.060
um, provided too short or too long. So that's for non-discreet commands.

1188
01:14:38.160 --> 01:14:41.620
So you know, it's aileron and when do you need to, uh, roll back out,

1189
01:14:41.620 --> 01:14:43.980
that type of thing or, or breaks release your brakes,

1190
01:14:43.980 --> 01:14:47.620
something along those lines. And it has a very specific structure.

1191
01:14:48.040 --> 01:14:51.580
So you start with your, the operator, the controller, whatever that might be.

1192
01:14:51.600 --> 01:14:55.580
So maybe it's the pilot, uh, driver, whoever it might be the category.

1193
01:14:55.880 --> 01:14:59.020
So that, that we just discussed, the command itself.

1194
01:14:59.680 --> 01:15:03.460

And then the circumstance that circumstances the state of your system, uh,

1195
01:15:03.460 --> 01:15:05.060
that leads it to be unsafe.

1196
01:15:05.120 --> 01:15:09.580
So the example I have here is operator provides GPS waypoints when the waypoints

1197
01:15:09.580 --> 01:15:11.620
present a conflict with other aircraft.

1198
01:15:15.000 --> 01:15:18.340
So this is just a visual representation. Um, so if you,

1199
01:15:18.360 --> 01:15:22.980
if you look at your inputs as some kind of step function, uh, so provided you,

1200
01:15:23.040 --> 01:15:24.860
you have that step function there not provided,

1201
01:15:25.000 --> 01:15:29.180
you just never have your set function. Um, and then the solid line is,

1202
01:15:29.400 --> 01:15:32.860
is the ideal for, for whatever your particular situation is,

1203
01:15:33.240 --> 01:15:36.620
the dash line on the left side applied too soon.

1204
01:15:36.680 --> 01:15:38.940
So you apply the brakes too soon, um,

1205
01:15:39.560 --> 01:15:42.460
or apply your brakes too late is that other dash line.

1206
01:15:42.840 --> 01:15:47.180
And then on the backside of your step function, um, you provided it too short.

1207
01:15:47.320 --> 01:15:51.380
So you ended that command too early or you provided it too long.

1208
01:15:55.560 --> 01:15:59.260
All right, so, so what you're gonna do is build out a UCA table. Uh,

1209
01:15:59.520 --> 01:16:03.100
so on the top there you have the, the categories.

1210
01:16:03.600 --> 01:16:07.060
And then I have applying brakes. So normally with a complex system,

1211
01:16:07.060 --> 01:16:08.780
you're gonna have multiple commands. For this purpose,

1212
01:16:08.880 --> 01:16:12.580
we just have one applying the brakes. So, uh,

1213
01:16:12.600 --> 01:16:15.620
so I threw in some examples for each. Um,

1214
01:16:15.620 --> 01:16:19.700
so the driver did not apply brakes when the car in front was stopped. Uh,

1215
01:16:19.700 --> 01:16:24.300
so that's not providing causes. The hazard providing is the, uh,

1216
01:16:24.300 --> 01:16:27.620
driver applied brakes abruptly when a car was tailgating. 'em,

1217
01:16:27.850 --> 01:16:30.260
they end up with a car in their trunk. Uh,

1218
01:16:30.260 --> 01:16:31.980
incorrect time of your order may be applied,

1219
01:16:31.980 --> 01:16:35.460
their brakes too late after a light turned red so they're not able to stop in

1220

01:16:35.460 --> 01:16:37.820
time. Um,

1221
01:16:38.000 --> 01:16:42.540
or the driver released the brakes too soon before the car in front began moving.

1222
01:16:43.240 --> 01:16:46.420
Uh, so maybe they give the car in front of him a little bit of a love tap.

1223
01:16:47.840 --> 01:16:50.140
All right, so any other examples you guys can think of?

1224
01:16:50.470 --> 01:16:51.780
Let's say for not providing,

1225
01:16:58.660 --> 01:16:59.960
we have hit a couple already.

1226
01:17:03.880 --> 01:17:07.310
Maybe there's something else in the road or something like that. You know,

1227
01:17:07.670 --> 01:17:11.820
a red light, something along those lines. Um, providing,

1228
01:17:11.840 --> 01:17:14.700
we talked about a couple, maybe, maybe you've road conditions,

1229
01:17:14.700 --> 01:17:19.380
that type of thing. Uh, incorrect timing and order. So I said applied too late.

1230
01:17:19.920 --> 01:17:23.540
Uh, could you have an applied too soon? Could that lead to something?

1231
01:17:25.100 --> 01:17:28.680
Yep, potentially for sure. And then, uh,

1232
01:17:28.980 --> 01:17:32.560
and then applied too long. So I give a give a release too soon.

1233
01:17:32.560 --> 01:17:33.880
What about applied too long?

1234
01:17:35.740 --> 01:17:38.920
So you're stopped and you just continue to stay stopped.

1235
01:17:41.070 --> 01:17:43.410
So it could, someone might rear-end you cuz they're,

1236
01:17:43.410 --> 01:17:46.370
they're not paying attention or something like that. Sometimes you'll,

1237
01:17:46.470 --> 01:17:50.130
you'll end up with, um, with something where maybe it's not ideal,

1238
01:17:50.470 --> 01:17:55.090
but it may not necessarily cause uh, a hazard. Um,

1239
01:17:55.460 --> 01:17:58.410
let's say, let's say you just never start your test point. You,

1240
01:17:58.470 --> 01:18:01.690
you don't get your data. If you've called that a loss, uh,

1241
01:18:01.690 --> 01:18:05.210
your lack of test data or not able to conduct the test, then,

1242
01:18:05.210 --> 01:18:06.130
then that would be a loss.

1243
01:18:06.310 --> 01:18:10.050
If you're solely focused on losing aircraft and and losing people,

1244
01:18:10.340 --> 01:18:13.330
maybe you're like, well, that's an inefficiency, but,

1245
01:18:13.330 --> 01:18:17.210
but it's outside the scope of my, my particular, um, analysis.

1246

01:18:20.140 --> 01:18:23.400
All right, so now we're gonna get into scenarios. Again. This is how,

1247
01:18:23.430 --> 01:18:28.320
this is how the UCA happened. Um, so what, what I've found,

1248
01:18:28.500 --> 01:18:33.480
as I said earlier, this is very much a kind of a structured, um, uh,

1249
01:18:33.480 --> 01:18:34.800
brainstorming type session.

1250
01:18:34.830 --> 01:18:39.120
What I've found is it's really useful to have multidisciplinary teams.

1251
01:18:39.200 --> 01:18:41.120
I think MF touched on that a little bit too.

1252
01:18:41.580 --> 01:18:44.000
So have ops engineers have folks that are,

1253
01:18:44.040 --> 01:18:46.360
that are deep into the particular system that you're testing.

1254
01:18:46.990 --> 01:18:49.480
Have your pilots have your range safety officers,

1255
01:18:49.480 --> 01:18:51.400
whoever it is that you need to have in the room,

1256
01:18:51.820 --> 01:18:54.400
cuz they're all gonna provide a unique, uh,

1257
01:18:54.460 --> 01:18:58.800
aspect based off of their experience and knowledge. Uh, so,

1258
01:18:59.660 --> 01:19:04.080
so why, why did I stop applying brakes before the car in front begin moving?

1259
01:19:04.100 --> 01:19:05.120

So I'm at a stoplight,

1260
01:19:05.940 --> 01:19:10.760
the light turns green and then I stop applying brakes. Um,

1261
01:19:10.760 --> 01:19:14.920
and then I again tap tap the car in front of me. Why might that I have,

1262
01:19:14.960 --> 01:19:17.680
I have some examples. So you could also just read to me. But, um,

1263
01:19:18.500 --> 01:19:19.920
if you guys have any thoughts on that,

1264
01:19:25.460 --> 01:19:26.293
say again?

1265
01:19:31.080 --> 01:19:35.240
I think I heard some of that. Uh, I, uh, the audiologist told me I need, uh,

1266
01:19:35.240 --> 01:19:37.880
hearing aids. I told him, no, I'm too young, so, uh,

1267
01:19:37.880 --> 01:19:41.240
you have to have to shout unfortunately. Um,

1268
01:19:42.590 --> 01:19:45.290
but I think, I think I heard a bit of that, yeah,

1269
01:19:47.750 --> 01:19:50.410
In a really big hurry. Yeah, yeah, you're late for work,

1270
01:19:50.410 --> 01:19:54.170
you're late for doctor's appointment to get to get hearing aids or something

1271
01:19:54.170 --> 01:19:58.600
like that. Um, yep. Maybe the,

1272
01:19:59.140 --> 01:20:03.400

so the car in front didn't have a working brake lights, so I,

1273
01:20:03.520 --> 01:20:06.440
I assumed they were going, but the brake lights weren't working.

1274
01:20:06.580 --> 01:20:11.180
So I didn't have a good feedback. The light turned green,

1275
01:20:11.580 --> 01:20:14.700
I assumed they were going, I was in a hurry. So I just started to go.

1276
01:20:14.700 --> 01:20:17.460
I didn't pay attention to the car in front of me. So maybe I have a,

1277
01:20:17.460 --> 01:20:20.180
there's a control algorithm. Green means go and I go, I don't,

1278
01:20:20.180 --> 01:20:24.490
don't look at what else is going on in my system. Um,

1279
01:20:24.950 --> 01:20:28.610
I'm 15, I'm learning to drive my driving driver's instructor told me to go.

1280
01:20:29.590 --> 01:20:34.170
So I did. Um, so I could, could feed into mental model, um,

1281
01:20:34.310 --> 01:20:37.330
cuz I believe it's safe. My instructor told me to, uh,

1282
01:20:37.330 --> 01:20:39.010
it could feed into the control algorithm.

1283
01:20:39.030 --> 01:20:41.810
My instructor tells me to do something, I don't think twice. I, i just do it.

1284
01:20:43.630 --> 01:20:45.490
Um, and then in interest of time,

1285
01:20:45.490 --> 01:20:47.570

we're not gonna talk too much about those next bullet points,

1286
01:20:47.630 --> 01:20:49.450
but just something to think about. Um,

1287
01:20:49.470 --> 01:20:53.130
how would it change if this was an automated vehicle as opposed to,

1288
01:20:53.470 --> 01:20:55.650
to me driving it, what does that change?

1289
01:20:55.750 --> 01:21:00.370
How does that change some of those scenarios as far as feedback

1290
01:21:00.590 --> 01:21:02.850
and commands and that type of thing. Um,

1291
01:21:03.210 --> 01:21:05.930
and then what about cybersecurity scenarios? Uh,

1292
01:21:05.930 --> 01:21:10.330
could someone hack into my car and tell my car to go? Or, or there other,

1293
01:21:10.330 --> 01:21:13.090
other things maybe, uh, affect the lights or something,

1294
01:21:13.200 --> 01:21:16.330
something along those lines. So those are some things to think about as
well,

1295
01:21:16.710 --> 01:21:17.570
uh, with this scenario.

1296
01:21:21.150 --> 01:21:24.970
So there's, um, a few different, uh, one way that you can, um,

1297
01:21:24.970 --> 01:21:28.610
break out scenarios as you're trying to think through what they are.
Again,

1298
01:21:28.750 --> 01:21:30.930

as a structured brainstorming method,

1299
01:21:31.310 --> 01:21:33.210
you don't wanna necessarily use this as a checklist.

1300
01:21:33.590 --> 01:21:34.610
If you use it as a checklist,

1301
01:21:34.610 --> 01:21:36.650
that means you're not thinking about anything else. Um,

1302
01:21:36.710 --> 01:21:40.850
but it can help get the creative juices flowing. Um, so,

1303
01:21:41.230 --> 01:21:44.850
so on the number one there command is not followed or it's followed

1304
01:21:44.850 --> 01:21:47.090
inadequately. So in that, in that situation,

1305
01:21:47.470 --> 01:21:51.690
the operator sent a command to the process and it was probably the,

1306
01:21:51.690 --> 01:21:54.370
the correct command, but it was either, uh,

1307
01:21:54.470 --> 01:21:59.170
not followed by the control process or it was followed inadequately in some way.

1308
01:21:59.710 --> 01:22:04.050
Um, and then, uh, number two is inappropriate decision.

1309
01:22:04.470 --> 01:22:08.970
So that gets into your control algorithm. Um, so, so something,

1310
01:22:08.970 --> 01:22:11.450
something about that control algorithm. Algorithm, again,

1311
01:22:11.450 --> 01:22:12.650
it could be the way it's hard coded.

1312
01:22:12.750 --> 01:22:15.730
It could be the way my brain is hardcoded led me,

1313
01:22:15.840 --> 01:22:18.450
even though I had adequate feedback. Uh,

1314
01:22:18.450 --> 01:22:21.810
so I understood the state of the system, it still led me to make a,

1315
01:22:21.850 --> 01:22:26.490
a poor decision. And then feedback in inadequate feedback,

1316
01:22:26.740 --> 01:22:29.250
maybe you have other inputs. Could be lack of feedback,

1317
01:22:29.340 --> 01:22:31.530
could be lack of timely feedback, uh,

1318
01:22:31.740 --> 01:22:35.290
could be the way that information is displayed. Uh,

1319
01:22:35.550 --> 01:22:39.490
all sorts of different things can affect, uh, the quality of that feedback.

1320
01:22:39.510 --> 01:22:42.490
And of course, that's gonna affect your mental model, uh, which,

1321
01:22:42.490 --> 01:22:45.690
which is then gonna drive through the rest of your control loop.

1322
01:22:46.110 --> 01:22:48.770
And then lastly, there's inadequate process behavior.

1323
01:22:48.870 --> 01:22:52.290
And this is really where you get, uh, your, uh,

1324
01:22:52.290 --> 01:22:55.570
your component failures that you get out of traditional hazard analysis.

1325
01:22:55.700 --> 01:22:58.130
Those are all gonna be captured in number four there.

1326
01:23:03.070 --> 01:23:07.660
All right, so minimizing procedures or mitigations, uh, there's a few,

1327
01:23:07.780 --> 01:23:08.780
I think, um,

1328
01:23:08.850 --> 01:23:13.220
professor Levison sometimes calls these requirements that gets confusing

1329
01:23:14.240 --> 01:23:19.100
in, uh, in, uh, acquisition land requirements or, or something different. So,

1330
01:23:19.200 --> 01:23:21.460
uh, so we typically call 'em, uh,

1331
01:23:21.460 --> 01:23:24.980
minimizing procedures mitigations or something to that effect. Um,

1332
01:23:25.720 --> 01:23:29.060
so each scenario is gonna have at least one minimizing procedure,

1333
01:23:29.880 --> 01:23:32.460
and it should be written in a way that it's actionable.

1334
01:23:32.460 --> 01:23:35.420
Someone can take that and then they can apply it. Uh,

1335
01:23:35.420 --> 01:23:38.580
so if it's written too vaguely, uh, just like a requirement, right?

1336
01:23:38.580 --> 01:23:41.220
Like a technical requirement, if it's written too vaguely, uh,

1337
01:23:41.220 --> 01:23:44.980
they may not be able to enact it sufficiently. Um,

1338

01:23:44.980 --> 01:23:48.820
so what are some minimizing procedures for that breaking example? Uh,

1339
01:23:48.840 --> 01:23:53.180
so one of the scenarios we mentioned was the car didn't have working brake

1340
01:23:53.180 --> 01:23:55.780
lights, so I couldn't tell, uh, that it was stopped.

1341
01:23:56.320 --> 01:24:00.140
So you can mandate working brake lights. Um, and then what does,

1342
01:24:00.140 --> 01:24:03.140
what does that do now? Now we gotta have inspectors looking at,

1343
01:24:03.140 --> 01:24:07.460
looking at brake lights. You gotta have annual inspections of your vehicle, uh,

1344
01:24:07.460 --> 01:24:09.660
cops pulling folks over, that type of thing.

1345
01:24:09.660 --> 01:24:13.300
So there's this overhead that comes with that type of a thing, right? Um,

1346
01:24:13.300 --> 01:24:17.860
you can design a backup system that notifies drivers that a car is stopped

1347
01:24:18.440 --> 01:24:22.940
or develop a sensor that detects an unsafe closure rate and beef sets a or

1348
01:24:22.940 --> 01:24:27.340
something like that to prevent you from, from hitting another car. Uh,

1349
01:24:27.440 --> 01:24:29.540
so the next scenario, the light turned green,

1350
01:24:29.660 --> 01:24:33.380
I assume the car in front would go, uh, so maybe,

1351
01:24:33.430 --> 01:24:36.380
maybe there's some training that you can do. Maybe train drivers to,

1352
01:24:36.440 --> 01:24:39.540
to look at the green light, but then also look at the car. Don't, just,

1353
01:24:39.540 --> 01:24:43.940
don't just make an assumption. My driving instructor told me it was safe to do.

1354
01:24:44.800 --> 01:24:48.900
Um, maybe we need to look at that training program, uh, and how, how we,

1355
01:24:49.120 --> 01:24:51.860
how we spin up those, those driving instructors. Uh,

1356
01:24:51.860 --> 01:24:56.740
we could fire the instructor. Um, and that's a joke. Don't actually, uh,

1357
01:24:56.740 --> 01:25:01.060
because hindsight bias leads us often to blame, uh, blame an individual,

1358
01:25:01.110 --> 01:25:04.980
blame an operator. And what that means is, is we have an issue with our system.

1359
01:25:04.980 --> 01:25:08.940
Maybe we have poor training, maybe we have poor hiring standards, uh,

1360
01:25:09.180 --> 01:25:13.340
whatever it might be. Um, now, now we're gonna pin it on an an individual.

1361
01:25:13.390 --> 01:25:15.540
We're not gonna fix the problem, the root problem.

1362
01:25:19.590 --> 01:25:24.090
Um, so, so that first one I talk about design mitigations. My assumption is,

1363

01:25:24.630 --> 01:25:28.610
uh, for, for this audience that we are too far down the design path, um,

1364
01:25:28.750 --> 01:25:32.090
and into flight test to go back and affect the design.

1365
01:25:32.190 --> 01:25:35.930
I'm gonna talk more about that. If you really want s TPA to,

1366
01:25:36.190 --> 01:25:38.850
to be effective for your particular organization,

1367
01:25:38.910 --> 01:25:43.050
you gotta start with design and we'll, we'll talk, uh, deeper about that after,

1368
01:25:43.340 --> 01:25:45.890
after the tour this afternoon. Um,

1369
01:25:46.230 --> 01:25:48.090
so if you don't have the ability to affect that,

1370
01:25:48.090 --> 01:25:52.130
you can choose whether or not you wanna include those mitigations or not.

1371
01:25:53.230 --> 01:25:58.170
Um, and again, there, there's, there's often more than one, uh, mitigation that,

1372
01:25:58.170 --> 01:25:59.610
that you might be able to use.

1373
01:25:59.610 --> 01:26:03.010
And we're gonna talk about the order of precedence here in a second. Um,

1374
01:26:03.240 --> 01:26:06.900
but you should go after the most effective one and also the most cost effective,

1375
01:26:06.990 --> 01:26:09.900
which tends to be the most cost effective. Um,

1376
01:26:10.130 --> 01:26:12.100
some mitigations may already be required,

1377
01:26:12.100 --> 01:26:15.140
maybe already have test processes that,

1378
01:26:15.140 --> 01:26:18.860
that were gonna prevent that particular scenario from occurring. What I,

1379
01:26:18.890 --> 01:26:23.140
what I would recommend is don't just blow that off and don't document it. Uh,

1380
01:26:23.540 --> 01:26:28.220
document it. Write down, Hey, we think we're covered by, by this regulation,

1381
01:26:28.320 --> 01:26:32.460
by this procedure, you know, whatever it might be. Um, and then make sure that,

1382
01:26:32.490 --> 01:26:35.140
that it truly does cover that mitigation.

1383
01:26:35.400 --> 01:26:38.580
Cuz what happens if that procedure change changes? Um,

1384
01:26:38.600 --> 01:26:41.620
but you never documented that in your, in your analysis.

1385
01:26:41.640 --> 01:26:44.700
And now you could introduce a safety concern into your,

1386
01:26:44.770 --> 01:26:47.580
into your test program and not even realize it because you don't have

1387
01:26:47.580 --> 01:26:52.100
traceability. So that traceability is, is very important. Um,

1388
01:26:52.760 --> 01:26:56.620
so in the, in the UAV example, we're gonna give, uh, I had,

1389
01:26:56.660 --> 01:26:59.180
I think it was seven elements. Um, in my,

1390
01:26:59.360 --> 01:27:03.740
in my safety control structure I came up with, it was right around 300,

1391
01:27:04.360 --> 01:27:08.380
um, mitigations. Um, so that's a lot. It's a lot to, to sort through.

1392
01:27:08.720 --> 01:27:11.540
So there's some different ways that you can, you can, um,

1393
01:27:11.900 --> 01:27:16.180
organize those I through a couple out there. You could, you could, um,

1394
01:27:16.180 --> 01:27:21.100
break it up by design test and then maintenance and operations. You can do, uh,

1395
01:27:21.100 --> 01:27:24.660
here's what we need for operational procedures, uh, developing influences.

1396
01:27:24.660 --> 01:27:26.660
So what, what's the environment? Uh,

1397
01:27:26.660 --> 01:27:29.580
what settings and configurations do we need to put into our test cards?

1398
01:27:30.120 --> 01:27:32.460
And there's, there's a million different ways you can set that up.

1399
01:27:32.520 --> 01:27:37.300
So whatever works for your particular program. All right?

1400
01:27:38.240 --> 01:27:40.460
Um, so, so what you end up with,

1401
01:27:40.650 --> 01:27:45.020
with s tpa is the hazard that you're trying to mitigate is,

1402
01:27:45.080 --> 01:27:47.460
is the cornerstone of your analysis.

1403
01:27:48.200 --> 01:27:51.420
And from that you understand the system behaviors, uh,

1404
01:27:51.420 --> 01:27:55.980
that can lead to those hazards. You've created minimizing procedures to try to,

1405
01:27:56.280 --> 01:28:00.780
uh, prevent them from occurring if some, if they do still occur. You've got, uh,

1406
01:28:00.800 --> 01:28:03.580
you have corrective actions that you can come up with, uh,

1407
01:28:03.580 --> 01:28:05.620
to control that exposure. Uh,

1408
01:28:05.620 --> 01:28:07.780
and then you have that system boundary that's important, right?

1409
01:28:07.780 --> 01:28:10.580
Because we said that a hazard is the state of the system combined with

1410
01:28:10.580 --> 01:28:14.780
environmental factors that lead to a mishap. So, uh,

1411
01:28:14.800 --> 01:28:18.380
so you can also come up with some recovery actions and we'll talk about that as

1412
01:28:18.380 --> 01:28:23.320
we go through the analysis, uh, later on the example later on. All right,

1413
01:28:23.320 --> 01:28:28.320
I think this is my last slide, second to last slide before the break. Uh,

1414
01:28:29.380 --> 01:28:30.280

so, uh,

1415
01:28:31.260 --> 01:28:35.280
who has everyone heard of the order of precedence before It's in mill standard

1416
01:28:35.290 --> 01:28:38.000
8 82. It's, it's out there quite a bit.

1417
01:28:38.380 --> 01:28:42.000
So the idea is if you can eliminate the hazard, uh,

1418
01:28:42.000 --> 01:28:43.720
particularly in the design phase,

1419
01:28:43.720 --> 01:28:47.440
whether that's the design of the system or design of, of your, uh, to your,

1420
01:28:47.590 --> 01:28:51.680
your test program, um, that's gonna be much more effective.

1421
01:28:52.580 --> 01:28:56.880
Um, and it's gonna be much more cost effective. Uh, so procedures, training,

1422
01:28:56.880 --> 01:29:00.960
warning devices, um, you use those because you couldn't design it out of,

1423
01:29:01.000 --> 01:29:04.180
of your system to begin with. And there's a number of, of, uh,

1424
01:29:04.180 --> 01:29:06.220
different definitions of order of precedence,

1425
01:29:06.240 --> 01:29:09.220
but I think that's really important to use as you're developing your

1426
01:29:09.220 --> 01:29:13.220
mitigations. Alright? Um,

1427

01:29:13.680 --> 01:29:17.700
so some advice as you're going into the analysis is, one,

1428
01:29:17.700 --> 01:29:21.380
don't dive into the details. Early Murph talked about how, you know,

1429
01:29:21.380 --> 01:29:24.380
we wanna create a thousand elements in our safety control structure.

1430
01:29:24.760 --> 01:29:28.460
The whole point of stpa is to start at that very high level, at your losses,

1431
01:29:29.000 --> 01:29:33.300
at these big picture, uh, situation, and then dive down into the details. So,

1432
01:29:33.400 --> 01:29:37.820
so go with the flow of the analysis. It's, it's there for a reason. Um, I think,

1433
01:29:38.100 --> 01:29:41.380
I think sometimes as technical folks have to fight that a little bit, fight our,

1434
01:29:41.380 --> 01:29:43.340
our inner nature. Um,

1435
01:29:43.340 --> 01:29:46.500
and then don't make an assumption that the design or the procedures that you

1436
01:29:46.500 --> 01:29:49.180
have are sufficient to prevent the hazard. Um,

1437
01:29:49.180 --> 01:29:53.780
the whole point is to find holes in the design. Uh, so if you assume it away,

1438
01:29:54.010 --> 01:29:56.460
it's not gonna happen. Early on, um,

1439

01:29:56.470 --> 01:30:00.140
after I graduated m i t I was working with, uh, with a team,

1440
01:30:00.220 --> 01:30:03.700
I was helping facilitate an analysis and it wasn't something I had no

1441
01:30:03.980 --> 01:30:06.500
familiarity with at all. And they kept saying, oh, you know,

1442
01:30:06.500 --> 01:30:08.340
we don't need to worry about that. We don't need to worry about that,

1443
01:30:08.340 --> 01:30:09.820
we don't need to worry about that. That could never happen.

1444
01:30:09.820 --> 01:30:10.653
That could never happen.

1445
01:30:10.880 --> 01:30:14.620
And then they were surprised that they got nothing useful out of their analysis.

1446
01:30:15.280 --> 01:30:18.580
Um, so, so don't make those, don't make those assumptions.

1447
01:30:19.080 --> 01:30:22.980
Assume assume that things could go wrong and then figure out how they can go

1448
01:30:22.980 --> 01:30:26.620
wrong, um, and document any assumptions.

1449
01:30:26.620 --> 01:30:30.980
We'll talk about that this afternoon as well. Again, St. Stpa is iterative.

1450
01:30:31.000 --> 01:30:34.500
You're constantly going back and tracing back to the previous step that you did.

1451
01:30:35.240 --> 01:30:38.900
Um, and then, uh, we, we talked about that last bullet already.