PROFESSOR: The engines, the aircraft engines, have a lot of sensors on them because the engines really need to work reliably. So it tends to be more sort of thermal structural components. And my sense is in cars, you monitor more electronics, how many--

AUDIENCE: Emissions.

PROFESSOR: --certainly admissions. It's slightly different what's being monitored, and the sensors are different. Even the companies that provide these sensors and health-monitoring equipment tend to be different as well. I think, there are similar trends, but they're somewhat parallel. I don't think one came before the other.

AUDIENCE: OK. Yeah.

PROFESSOR: Hey, Volcker, do you want to mention something about health monitoring in general for operations?

GUEST SPEAKER: I just sent you a link on your email because we've been for six years monitoring the health of [INAUDIBLE] that's up there. And it's live link, so I don't know if you are able from your computer to open it. I just sent you the link on your email. Right? So actually, into the first satellite that we both [INAUDIBLE] few years ago, we figured we want to know everything.

So the primary [? dom ?] system were all sent on every telemetry data the same [? dom ?] at every path and kept actual. So maybe after break or whenever there's a chance, go to the link, and you can see the actual housekeeping data. And you'll see that the battery, the voltage, is the only one that's [INAUDIBLE]. Likely, [INAUDIBLE] of the six years, which is not bad for a VC system.

PROFESSOR: Yup, OK, I'll pull it up during the break. Thanks for that. That'll be interesting. OK, let's move on. So unfortunately, I would say the F-18, and there's a lot of systems that were designed with operational excellence in mind-- maintainability, high reliability. That was a big thing. I did mention this before, I think, but I just want to say that it's not always the case.

So this is one of the counter-examples, the space shuttle. And I have a lot of respect. Don't misunderstand me. I think people that worked on the shuttle did an amazing job. It was an amazing vehicle. But things turned out quite differently than what was promised. I think that

everybody will agree with that. So this is a paper that was actually a very short paper published believe it or not in nature in 2011 right after the retirement of the shuttle and by Pilcke et al.

And what they did is, they looked at the costs of the shuttle program. And the cost is well known because this is all public money. This is all money that was appropriated by Congress. And then the light blue bars are the number of launches that happen in a particular year. So you can see the maximum was nine-- nine launches in 1984-- not a launch a week that Congress had been told.

And so we have about 10 years of design, build, test until initial operating capability. And then we have about 30 years of actually usage and operations. And this is true for any system. The operational phase is much longer than the design phase. So in this case, the operational phase was 30 years right, three times longer than the actual design phase, which was about a decade. The Vision was a partially reusable space vehicle, quick turnaround, high flight rate.

What we actually got is a complex and fragile vehicle with an average cost of about $1.5 billion for flight and a workforce of about 20,000 people to keep the shuttle flying. And I think I've shown you this before, right? Did I show you this before? So this is an original illustration from the proposal to Congress. It kind of looks like the F-18 that I just showed you. It's a hangar, pristine, a few people, a couple of ground support equipment carts-- this is kind of like an airplane, like an airliner. And then this is what we actually got.

This is a picture taken in the Orbiter Processing Facility at the Kennedy Space Center. And you can't even see the shuttle, right? It's hidden behind the scaffolding, and the main systems that required a lot of work between flights were the shuttle main engine and of course the TPS, the thermal protection system. Now, you can say, well why such a big discrepancy between what was promised, the Vision, and what's actually delivered?

And people will have different opinions. My opinion is, certainly over-optimism was a part of it. But also Congress kept the research development costs for the Orbiter in particular to about 5.1, 5 billion. There was actually an act of Congress that said those shall not spend more 5.1, 5 billion on development of the Orbiter. So then, when it was clear, 24 metric tons to low-earth orbit. If you can't achieve that, the system will not satisfy.

So performance is king, and of course, this was also a politically challenging because there

were military requirements and civilian requirements that had to be met. And then maintainability, like I said, just doesn't happen automatically. You have to actually write requirements for maintainability. How long should it take? How many hours of work? How many actions or procedures to do certain maintenance actions? It has to be designed into the system, therefore the need for requirements.

And then no realistic lifecycle cost or value optimization. So that's, I think, the counter-example. But again, I am not blaming individuals for this. I'm blaming the system for this. Yes?

AUDIENCE: To what extent do you think that kind of problems within shuttle can be traced to effectively a failure to stop defining the requirements? I feel like when you look at commercial launch systems kind of as a comparison point. And I understand they're not reusable. And they're not being designed to necessarily the same specifications as shuttle. But I feel like because the commercial launch industry has had standards set by NASA and the Air Force that they needed to meet, that they had a very clear set of requirements from the beginning.

Whereas the development of shuttle, like the failure to design for maintainability, when I look at the development cycle, it looks like they continue to refine requirements as they went and kind of discovered new things. And then said, OK, so we need to do it this way instead of saying from the beginning, these departments we know we have to meet. Let's design to that.

PROFESSOR: Right, though I--

AUDIENCE: It look like they kind of crept through the development phase to me, that there was no hard stop. So I was just wondering if you could comment on that kind of--

PROFESSOR: It's definitely true that there was sort of reacting to-- and after the first few-- so an interesting history there is the shuttle main engines. They were completely disassembled and inspected after the first couple of flights. But that wasn't supposed to be done every flight. It was supposed to be, you're going to launch them, I think, like five times before you actually do big inspections. But they had already done inspections after every test flight. And then they just kept doing it.

So something that was supposed to be only a maintenance action or inspection during test flights became or crept into becoming an operational requirement. And of course, you have a big workforce and there's jobs and so forth. So there's that too. But it was never intended that the shuttle main engines would be disassembled and rebuilt after every flight.

AUDIENCE: Why was that permitted?

PROFESSOR: Well, I guess, the sense was that it would be safer to do that, and that you really want to know what's the state of these engines. And I will say this, I mean at the contractual, there's jobs there. There's money there. And so the more maintenance actions you can do, the more of a business this is. But of course, that's not what the Vision was. The Vision was a very lean, operations, few people. So there's a socioeconomic things tied up with it as well.

AUDIENCE: Do you think that because that's inherently a government project that's part of the reason? Like whereas a commercial company is looking to cut as many employees as possible to increase profit margin?

PROFESSOR: I think that that's a part of it.

AUDIENCE: OK.

PROFESSOR: Yeah, I do think that's a part of it. Yeah, absolutely, it's a really interesting history. There's a lot to be learned from this. OK, so let me move on. So this is kind of a list, not a checklist really, but a list of operational considerations that you should think about when you design a system. So how will it be operated? And of course, we've done the CONOPS a while ago, but this is sort of more detailed than the CONOPS.

How will you inspect the system? How will you maintain it? What insights do the operators need into the system status? So when you are operating the system, how much about the internal workings do you really need to know? This is the internal telemetry temperatures, pressures, in the avionics, the electrical. I think the example of the electrical bus was good, the cryogenics system example, how much insight do you need?

Before turning over to the operators, what checks do you need to perform? How might the system fail? Think about failure, and you of course need to think about that as early as possible. What are the options available to you in case you have failures? And you will have failures. What spares are needed to repair the system? Will this system still perform even under partial failure? So maybe something failed but not catastrophically. It's a partial failure. Can you keep going with the system? How far can you push the system?

I think if you think about this is like five questions here, but I think, they are five of the most important questions for operations. Now in terms of the NASA lifecycle, we're talking Phase E

here, just to be clear. So Phase E is called Operations and Sustainment. And depending on what mission you're talking about, this could be short-- like the Apollo missions, like two weeks and they're back home-- ISS, six months rotations. Or it could be something like Voyager.

Voyager was launched when in '76? Voyager's been flying for 40 years, and we're still getting data and telemetry at very low data rates, like 100 bits per second or something like this. But still, that's remarkable, right? So Phase E, in that case, is very long. So it's worth really thinking about this.

All right, let me talk about commissioning. So commissioning is essentially the transition from Phase D to Phase E. So Phase D is System Assembly, Integration, Test, and Launch, and Transition to Use. And Phase E is then Operations and Sustainment. So to conduct the mission, meet the initially-identified need, maintain support, and then implement your mission operations plan.

So commissioning, essentially, is transitioning from Phase D to Phase E. And usually, the people that will operate the system day in, day out, tend to be different people than the people who design the system, who build the system, who launch the system. So usually, you have some kind of a handoff or handover of the system from the designers, builders to the operators. And that handover is very important that it be done well. And that's what we call commissioning.

Or in this case, this is the-- do you remember this? We haven't shown this for a while. Remember what do we call this, this thing here? The engine, right? The system's engineering engine at every level. So this is Step 9, Product Transitioning Process. And then there has to be a flow chart, right? Can't do without a flow chart. It's not particularly fancy or anything, but the idea is that you have inputs, which are the end product, ready to be used, documentation.

So when I ask you about the cryogenic system-- you mentioned the cryogenic system-- I ask you, do you have a user manual for it? So that would be here, in this box here, on the left side-- the documentation that goes with the end product. And then any product transition-enabling products, so those would be things that you only use during the transition, like equipment or facilities that you just use for this transitioning process. And then you don't use them during operations. You can think of examples of that.

And then you go through this multiple steps. There may be multiple sites that you have to prepare, multiple locations. And at the end of it, you've delivered the end product. It's

operational, transition work products, and you're essentially operational. So what it means in practice is deploying the system in the field, transitioning to the operators, physically and legally also-- I should point this out. This is really important.

So usually, in this commissioning phase, the legal ownership of the product or the asset is transferred from one organization to the other. So if it breaks now, it's your problem. It's not my problem. You've already taken ownership. You've signed off on it. And for insurance purposes, this is a very big deal. So at what point does legal ownership of the asset transition? You really have to know that. And then, of course, the training.

Checkout-- checkout means turning on all your systems and subsystems, making sure everything works, making sure there's no emergent behaviors, weird behaviors, unexpected behaviors. Comparing the predicted parameters against the actual behaviors. Does the system behave as we had predicted, based on calculations? These days, we usually build simulations. We build a pretty realistic simulation of the system, and there's the concept of digital twin.

Who's heard this before? Digital twin. Who's heard this before? Oh, nobody, OK. So the idea of a digital twin is that here's your physical system, airplane, satellite, cube sat, whatever it is, medical device. And there's a digital twin of it. There's a in silico version, a simulated twin, of that system that exists somewhere. And before you turn the system on and do operations on it, you do it on the digital twin to see what will happen and predict everything-- all the parameters, the position, velocity, accelerations, temperatures, pressures.

So if things look good in the digital twin, then you actually do it in the real system. So for example, JPL with their Mars rovers, they will do that. They have a digital twin, they have a digital version. They actually have a physical twin too. But they typically only use that if there's problems, like stuck in a sand dune or something like that. So you actually simulate commands that you're going to send to the spacecraft on your digital twin, make sure that the command sequence is correct, that things will-- and then you do it on the real system.

That's what we mean here. And during checkout, you do it initially. But actually, if it's a very complex system, you might do this as a matter of routine. And then sustainment is the third thing here. So sustainment means maintenance, both preventative and corrective. So preventative maintenance means you're taking actions before the system breaks. Corrective action means you're taking maintenance actions after you have failures of different kind--

spare parts management, reconfiguring system during use for different purposes, upgrading system, and then retrofits.

So what is a retrofit? Anybody know? At EPFL, are you familiar with the term retrofit? Have you heard this word before? Volcker, do you want to explain what it means?

GUEST SPEAKER: Absolutely. So for example, let's take your [INAUDIBLE] system, the system volt's M109. Ours says from USA. Back in the '60s, '70s, then these things are aluminum, launch self-propelled. And in the '80s, '90s, they decided to not throw them away. They don't rust. But to retrofit them, to put guidance navigation system, new cam. So waiting through a retrofit program, meaning you sort of break down everything, down to the lowest elements, you decide what you can keep. You throw away the obsolete stuff. You buy new things, and you try to make it.

PROFESSOR: Yup.

GUEST SPEAKER: And then you reconfigure.

PROFESSOR: So retrofit typically means you physically go out in the field, and you physically change the system. Like Volcker said, you remove things, you typically add new things. So now you have like old generation and new generation stuff mixed up in the system. Retrofitting is a huge deal, particularly in the military, but in other domains as well, like hospitals, infrastructure, train systems.

You go there, and you see a mix of old stuff from when the system was originally built and deployed, and then new stuff layered on top of it through retrofits. And the key question, of course, when you do a retrofit is, you want the retrofit not to interfere. You want it to actually be value added as opposed to causing more problems. Yeah, go ahead.

AUDIENCE: Is retrofit the same as medium-life up grade?

PROFESSOR: I would say it this way-- a medium-life or middle-of-the-life upgrade is a particular type of retrofit that you do roughly halfway through the nominal mission life. Yes, and do you have experience with such upgrade?

AUDIENCE: Yes, actually we have both F-5 and AMX in Brazil. We have the medium-life upgrade and both performed by Embraer.

PROFESSOR: OK.

AUDIENCE: So it's interesting because the F-5, for example, is Northrop. And the medium-life upgrade was performed by Embraer. And we had lots of issues about it.

PROFESSOR: So what was done to the airplane?

AUDIENCE: Completely change of the dashboard panels and new electronic warfare equipment. But they kept the old hydraulics engine and-- actually, hydraulics and engine. The electrical system was changed as well.

PROFESSOR: Was changed as well. So you keep the frame, the engine--

AUDIENCE: And you change the radar, the antennas, and lots of different stuff.

PROFESSOR: That makes sense. That makes sense.

AUDIENCE: A new head-up display, a new helmet, stuff like that.

PROFESSOR: The interesting discussion, which I think in the US for much equipment, and Switzerland same discussions, is by the time you start adding up the cost of a midlife upgrade or retrofit, you start adding all these things up, pretty quickly you come to the question, well, wow that's pretty expensive. Is it really worth it, investing x millions or billions to squeeze another 10, 15 years out of this platform? Or should we just buy a new one and retire this one? And you'll have very vigorous debates about that. Yeah?

AUDIENCE: Just how does the funding structure ever come into play when determining how sustainable, or how you're going to retrofit something? I know sometimes, where you worked funding ends this time and something else starts up this time. So sometimes, you kind of design a little bit around those things. Is that ever taken into consideration?

PROFESSOR: Well, I think enlightened companies, enlightened organizations will actually build in retrofit and upgrade costs into their original budgets. But does it happen often? I think it's a minority of organizations who really are honest to think about the full lifecycle cost, including upgrades and retrofits. And to be honest, sometimes, these retrofits, it's hard to know about them ahead of time. In some cases you can predict them, but in many cases, it's more reactive. In fact, I'll tell you a story about the F-18.

These retrofits often come in bundles or packages called ECPs, Engineering Change Proposals. They're sort of packages of changes. And it's almost blackmail, but it's like, here's a

bundle of changes that is x million dollars. And it's up to you whether you want to implement that or not. But if you choose not to implement, then the warranty is void. Or you're losing compatibility with any future upgrades. Do you see what I'm saying?

So the configurations then start to diverge. And then you have to make a tough decision. Do you spend money on an upgrade that maybe you don't absolutely need, but some other customers wanted? And if you say no, we don't want this. We're going to freeze the configuration where we are today. Then, you might lose the option for future upgrades. And if you then choose to upgrade later, it could be much more expensive. And that's systems engineering too.

And it gets into technical issue, financial issues, strategic issues. So I hope you're getting a sense here that this is all happening during operations. This is fascinating stuff. This is not boring. This is not just routine operations.

OK, so in operations, we have launch for spacecraft science operations, safehold, anomaly resolution, and so forth. And I just want to show you a quick video here about the James Webb-- this is a one-minute video about the anticipated deployment of the James Webb Space Telescope. I think, I mentioned to you. I've worked on this as a Master's student. This is supposed to happen in 2018, launch from Kourou on an Ariane rocket. This is a NASA-ISA collaboration.

You can see right now, the spacecraft has been launched. It's deploying its sunshield. These are very thin membranes. The purpose of the sunshield is to keep the optics cold. The optics are on the top here. And there's spreaders, and there shouldn't be any wrinkles. And there's multiple layers. You can see the layers. Now, first you spread it out horizontally. Now, the layers are being spread to be right at the right angles.

And I don't know what's happening right now. But the last step that should happen-- I guess it didn't quite play until the end. But the last thing that happens is the optics are then deployed. And the optical deployment is also very, very involved and has to be very precise. So let me just minimize this. So and then after that, you have a commissioning.

I should also mention that the James Webb State, when I worked on it, it was a $500-million mission. It's now become an $8-billion mission. But the purpose of this instrument is to look back in time to what's known as the dark ages. It's basically like 300,000 years to about 100 million years after the Big Bang. The formation of the very first Pluto galaxies. We can't

observe that right now with Hubble or from the ground, mainly because these are so far away because of the expansion of the universe that the radiation is redshifted. And this is all in the infrared.

So you to have a very quiet, very cold instrument to see these first proto-galaxies being formed. So I know we can argue, is it worth spending 8 billion to see the very first galaxy being formed or not? People will debate it. But the fact is, it's happening. James Webb will launch. And then, it's going to go through a commissioning phase, like I just talked about.

So I want you to answer this question here. How long do you think the commissioning phase of the James Webb Space Telescope will take? Three days, a week-- in orbit that is. Three days, a week, three weeks, a month, three months, six months, or you're not sure. So answer that question, and then we'll take a short break, like five minutes, and look at the answer. Yup?

AUDIENCE: Are they still on schedule with the telescope? Or do you have any idea on whether that will slip some more?

PROFESSOR: When I worked on it, it was supposed to launch in 2008. But I do think-- I mean, the spacecraft is being integrated right now at Northrop Grumman. We saw it in January. So they're not lying to us, I think. They're actually putting things together. And I think, it's going to launch in 20-- maybe slip by another six months, or maybe a year but not more. I don't think so. Basically, how long does it take from what you just saw in the video until PIs, Principal Investigator scientists--

[INTERPOSING VOICES]

AUDIENCE: Can start using it.

PROFESSOR: --can start using it for real science. How long will that take? So who wants to respond? Who thinks it's like a month, three weeks, a week? A month or less? Who responded to that, a month or less. Go ahead. What were you thinking?

AUDIENCE: No specific idea.

PROFESSOR: What were you imagining would happen in a month?

AUDIENCE: I thought that it couldn't be very, very long because if the objective is to collect the data, you can't wait that much before you start using it. But I had no specific ideas.

PROFESSOR: No, I think that's a good answer. You deploy the solar panels, the sunshield, the optics, the spacecraft's at the right place. By the way, this is going to launch too in Earth-trailing orbit, like Earth-Sun L2, kind of trailing orbit. So it's kind of away from the Earth, from albedo, all that. So you deployed it, let's get on with it.

[LAUGHTER]

Yeah, I agree. And then I think, 37% of you, a third of you thought maybe three months, and then 40% about six months. All right, so let's look at the current plans. And I took some slides here-- I referenced it-- from a lady that works at the Space Telescope Science Institute that's located in Baltimore, the NASA's Goddard Space Center of Baltimore. This is from last year.

So here's the plan to launch in October of 2018, and then do the deployment. And the answer is right now six months. Six months commissioning phase-- and then, there's different cycles of-- so GO stands for guest observer. So you have primary PIs. They usually get first dibs. And then you have observing time for guest observers. Here's another little bit more detail. So full schedule of deployment and check-out activities, a limited set of science calibration ops possible, science observations highly unlikely during this six-months phase.

And then, you have this Guest Observer Program, and there's a budget, actually, Guaranteed Time Observation Program from April of 2019-- a total of 3,960 hours allocated in the first 30 months after commissioning, OK? And so those 3,960 hours are-- people will fight over this. And there's a very detailed process for how to allocate and compete for that observation time. But the answer here is six months.

And it really surprised me too that it's going to take this long but the reason it takes so long is mainly calibration. Calibration is a big thing. You want to make sure that all the observations you're going to take are correct. And in order to do a proper calibration, you have to essentially image things that have already been imaged before by other instruments that were also properly calibrated. So that for a known set of targets, you know you're getting the same answer. And that just takes time. I think, in a nutshell, that's the main reason it takes so long.

GUEST SPEAKER: Pardon me?

PROFESSOR: Yup, go ahead.

GUEST SPEAKER: There's also the one aspect with this observatory is that you have to be stabilized. And as you

get to bring it up from Earth, even though it was pulled together in a clean, very high [INAUDIBLE], it's going to have to deploy. And then, just to get to the chemical stabilization, it's going to spend weeks before they even can start to calibrate the instruments. So for you to get the outgassing, the whole volatile substances and get that they move far away, not from the spacecraft, that they dilute in space, get stabilization of temperature, and then you can only start checking instruments.

PROFESSOR: Great point. So thermal stability, outgassing-- so really everything is very stable. Yeah, very good point. OK, so let me talk briefly. I'm going to go through two examples of research in operations. And then, we'll talk about the post-flight review. All right, so the first thing is, each of these two examples are based on papers. So "Spare parts requirements for space missions with reconfigurability and commonality." This is based on a paper in *Journal of Spacecraft and Rockets,* 2007.

So and this work was done during the Constellation Program which was, we're going to go back to the moon. We will re-establish a human presence on the moon. And we're going to bring a whole bunch of stuff with us, more than we did during Apollo to do this. So the picture on the upper-right, you see a habitat on top of a Lander stage. You see an Ascent Vehicle with a Lander stage. You see a Rover that looks kind of similar to the Lunar Rover, but there's also a pressurized version of it. So we're going to bring a whole bunch of stuff.

And the challenge is during operations, things will break. So you need to bring spare parts to support all this. And some recent research we've done in my group shows that for Mars, it's the same problem. You're going to stay there a long time. You don't know exactly what will break. But if you want a high probability of being able to successfully operate, you do need to bring spares.

So the idea that was explored here is, what if those spares could be common or reconfigurable and you can do scavenging? So the idea is that, instead of bringing a dedicated spare-- if you give these three systems that are shown here, The Habitat, the Ascent Vehicle, and the Rover, to three different companies to build, and they don't talk to each other, and you don't impose any commonality requirements, you're going to get very different solutions.

What's the classic example of this in spaceflight, human spaceflight? Apollo 13. What happened in Apollo 13? The cartridges for the CO2 scrubbing, square cartridges versus round cartridges. The two different contractors, they didn't talk to each other. The government didn't

say you have to make these common, so they weren't common. So the idea here is, what is the effect of reconfigurable and common spares on system availability if you allow temporary scavenging and cannibalization of systems that aren't used?

And so one thing you need for that is an operational profile for each element. And that's shown in the lower left. So this is essentially a binary. Zero means that particular element is dormant or not being used. It's kind of in slumber mode. And 1 means it's actively being used.

And so then we have at each of these time periods, T1, T2, T3-- our time periods where there is a change in the operational status of a particular element. Either it goes from sleeping mode to active mode, or from active mode to inactive mode. And so knowing these cycles' operational profiles is very important to do the analysis.

So this is a little bit of math here. I'm not going to go through this in detail. But basically, when you do classical sparing, and maintainability, and failure analysis, you assume that failures arrive according to a Poisson process. So this is the equation for a Poisson distribution. And then you can see the various variables that are used here. So your lambda is your failure rate. P of n is the probability they have exactly n failures. And then, down here, we have the spares that are available to you.

And really spares can come from two different sources. One is, you bring spares with you from Earth. So this is a spares from repository, s sub i. These are spares you brought with you as a pool of spares. And then s sub e are spares that you take out of elements that are not being used. So these are spares that are scavenged temporarily from inactive elements. That's s sub e minus n sub f, which is the number of failures that have occurred up to that point.

So the total number of spares available at any given point in time is your initial spares pool plus spares you can scavenge from other inactive elements in the system, minus elements that have already failed. And this is assuming no repair, so you can't repair. And it assumes that you know ahead of time what the operational profile is. So there's spares available from elements from scavenging is this equation here. It's essentially the sum over all the elements, E. E is the number of elements in your architecture.

Q sub E is something known as quantity per application, QPA also. So basically, if you have like a mission computer or in like UAVs, we have servos. Like, this particular element has six servos, identical servos. They're used on the vehicle. So QPA, this QE would be 6. So if that element isn't used, we could go in, take out a servo, put it in somewhere else. And so we can

treat that as a spare, at least during the period where that UAV isn't used. Does that make sense?

OK, so the difference then is that in the kind of classic way of doing it, we have dedicated spares. Each element, one element 1, element i, element E, has dedicated spares that only work on that vehicle. There's no swapping, there's no scavenging, there's no communality. And therefore, your spares repository, s sub i, is going to be pretty big because there's no commonality, no sparing. In this new situation, you have reconfigurable or common parts. So we still have a spares repository.

But now those spares can be deployed across all or a subset of the elements, plus we can treat-- and this is this dashed line here-- we can treat elements that are part of idle elements. We can treat them temporarily as being part of the spares repository. Does that make sense? So that's a much more, in a sense, smarter way to do. And the question is, what's the benefit of this? So in order to calculate the benefits for this, we essentially-- we have some constraints.

So for example, the number of failures that you can have is between-- if you have zero failures, that's great. That's your lower floor. And then N is the total number of units you have in your architecture, including the ones in the inventory, in the initial inventory, and plus the ones that are built into all the vehicles. And then, the key here is what's known as back-order level.

So back-order essentially is the number of spares that you would need but may not-- so when the back-order level becomes larger than zero, it essentially means that your number of failures have exceeded the number of spares that you have. You don't have enough spares to satisfy all your operational needs. So this is this conditional back-order at spares level s. And you sum that essentially then over all the possible failure states that you could see.

And why is that useful? Because you can then calculate essentially your element availability. So a is your availability of at time ti. And then your probability of the whole system is the minimum of your system availability at any time and point during your mission horizon, your mission time, T. Do you see how that works? So you have your spares. You have failures of the spares, which are random. And then you can calculate, are you going to have enough spares to operate every element that you need to operate when it's supposed to be operational?

And the back-order level, this number b here, is what you use. You look at your back-order level across the whole mission timeline to see what your system availability will be. And there's a closed form approximation of this. And then for a larger number of elements and different QPAs and so forth, you typically then have to switch to simulation, like Monte Carlo simulations.

So what are the results here? So this was applied to-- the example here is a co-located mission elements. This is for, I think, it was a lunar mission. And you define essentially the operational time profile, quantity per application, and so forth. And the example that was used was an electronic control unit, and ECU, with a meantime to failure of 100,000 hours. So failure rate is 1 over meantime to failure. Lambda is the expected failure rate is 1 over meantime to failure. So pretty reliable, 100,000 hours of operation meantime to failure is pretty reliable.

But of course, you're far from Earth. This is a 600-day timeline, and you can see here the operational profiles for your various mission elements. So this is actually kind of reminds you of *The Martian,* right? Anybody seen the movie *The Martian* recently? Who's seen *The Martian?* Who's not seen *The Martian?* You've got to go. You're the only one in the room. It's a great movie. So he does scavenging and even things that weren't supposed to be scavenged.

And so we have four elements here. We have the PR, which is the Pressurized Rover, the Habitat, the All-Terrain Vehicle, and then the ATV, which is the Ascent-Descent Vehicle. In this case, it's the same vehicle for ascent and descent. And so the Ascent-Descent Vehicle, you only need it when you land and when you depart. The rest of the time it's dormant. The Habitat is used while you're on the surface. The ATV is used while you're on the surface.

And then, the Pressurized Rover is used-- the assumption here is you're going to operate for like 100 days very close to the base. And only after 100 days are you going to start going further away with the Pressurized Rover. So those are the operational profiles. Yeah?

AUDIENCE: Is there an argument that you wouldn't want to be scavenging parts from your Ascent-Descent Vehicle at all?

PROFESSOR: That's a good point. So if basically, your back-order level is too high, and you run out of your last spare the day before you're supposed to launch on the ADV, you're in trouble. But if that's

the case, then what you have to do is you have to exclude the minimum-- and there may be redundancy in that Ascent Vehicle.

And you may or may not be willing to sacrifice the redundancy. I mean, this is all about risk, right? And exclude those or keep out spares that you cannot touch because if you can't, then you can't get back home. So you just don't count those in your spares pool if that's the case. But you can still do the whole analysis.

OK, so what's the bottom line here? What's the punch line here? So the punch line is that if you have a-- the D case here is the dedicated case, OK? So this is where there's no scavenging, there's no commonality of spares among these elements. You have to have dedicated spares. And let's assume you want a 90% availability, which is not that high.

That's a relatively modest requirement. You want 90% availability. What it means is you need to have in this case, you can see the line just crosses below here, this crossover. You need four spares in your initial spares pool for this electronic control unit. You have to have at least four spares, dedicated spares, for that electronic control unit for a 600-day mission for a unit that has 100,000 MTTF or MTBF to guarantee at least 90% availability.

And you say, oh, that's not a big deal. That's just four spares. Well, that's just one unit. That's just one box, right? You probably have dozens of boxes, or even hundreds across all these elements. And so that could be a lot of spares. You translate that to mass and volume, that's a big deal. So using closed-form analytics to calculate the minimum number of spares you need, this is the R case, the reconfigurable case.

You can see that you can achieve that same requirement with two spares. You see that? That's this line here. It's this line here, and this is a conservative model. This is a conservative model. So by doing reconfigurable and common spares and scavenging, you can cut your number of spares in half. You can cut your number of spares in half and still achieve a 90% system availability.

And then you multiply that across all the elements in your architecture. And that's a big deal. And then this result here-- so this is a rigorous bound because it makes some conservative assumptions, and it uses closed-form equations to calculate this. And the details are in the paper. And then this curve here is the simulated. So if you simulate this using essentially a discrete event simulation several times, and then you take averages, it's actually even a little better. This suggests you could even get away with one spare. But it's not as conservative as

the closed-form solution. OK, so the bottom line is reconfigurable parts allow for 33% to 50% reduction in the number of required spares for 90% availability level.

But if you think about what that means operationally, it means that you really have to know ahead of time what's going to be operational when, you have to have the crew trained to be able to actually go in and scavenge. And the equipment, the vehicles, have to be designed such that you can actually remove this stuff and put it back in relatively easily. So that would impose some accessibility, and replaceability, and maintainability requirements.

The other option is you say, we don't want spares. Well, then you need to do a lot of redundancy. And then, your vehicles are going to get heavy and more complex. I mean, those are the real world trade-offs. Yup, Sam?

AUDIENCE: Does this potentially increase the risk for the crew of the mission if there's some sort of inherent failure in the particular part that is being used everywhere?

PROFESSOR: So I don't know if you looked ahead or you just-- I know you're a smart guy, Sam. So this is the answer to your question right here. So this is great. OK, we like the fact that we can cut down on the number of spares and still meet the same availability. But you can ask the question in different ways. So on the left side is a kind of sensitivity analysis that says, well, maybe we're not so mass constrained.

We have plenty of transportation capacity. So we're not really mass constrained. But we know that designing ultra-reliable electronic boxes or whatever components is very expensive, right? So can we decrease the requirement on the manufacturer of these boxes? And can we go from, say, 100,000 to 75,000 MTTF? So we're decreasing the nominal reliability of the equipment by a fourth. We're making the job easier for the supplier of that box. Presumably, that should be cheaper. That should be a cheaper box to design and build.

So what will happen if we drop the reliability requirement by 25%? And then you can see the impact here. So the blue curve is essentially what you get for the less reliable equipment. And then the black was the original. So now, Sam's question. So this is basically-- so here's your failure rate. OK, this is your failure rate, 10 to the minus 3. And we're varying the failure rate over a large range. And then we're looking at system availability. This is for a fixed number of spares.

And what's really interesting-- so when your failure rate is low-- so we're on the left side-- then

the blue curve is lower, the dedicated case. So for a fixed number of spares, for relatively reliable equipment, you're better off going with the reconfigurable or common spares. This is logarithmic, so it's a little tricky. So system availability is higher when you have common and reconfigurable spares, relatively reliable equipment.

But there's a crossover point. If your boxes, your elements, your components, are very unreliable, which is on the right side, there's actually a crossover point. And the idea is that, well, now because it's common and reconfigurable across all the vehicles, you have this really bad box that breaks all the time. Now, the problem is everywhere. Every vehicle, everything is affected by it. Whereas before, it was kind of more contained, right? And so that's what that crossover is.

So if you're in a situation with very unreliable equipment, unreliable components, you're actually worse off making them common or reconfigurable. And you can now calculate where that crossover point is. That's pretty cool, don't you think? I get excited about this stuff. I don't know about you guys, but this is real.

This is what you care-- in operations, this is-- how many spares of each kind, can we guarantee that we can successfully do this campaign, whether it's a military campaign, or you go to Antarctica. And we heard about the Octanus Rover. And it's just one Rover, but what's all this stuff that you need to bring with you in terms of spares to make sure you can actually have a successful campaign and have a guarantee of that? Yeah?

AUDIENCE: I'm wondering if the reconfigurability argument also has some sort of impact on the kind of finances and manufacturability-- in terms of if you're making reconfigurable parts for different things, they may be more similarly manufactured, and therefore may represent a decrease in cost on the manufacturing side? If that's another motivation.

PROFESSOR: That's a great point. What I will say about that is that in order to capture that benefit, you need to lock that in contractually. So either you give all this work to the same manufacturer and say, OK, you're now making 50 boxes instead of just five. There has to be a discount on a per-unit basis for that. Or if it's different manufacturers, then it gets hard.

So yes, but you have to have the kind of business arrangements that will allow you to capture that value. EPFL-- were you able to follow this? I know this is pretty detailed discussion here on these curves. Is it-- Maxim, you're sort of shaking your head. Is it clear?

GUEST SPEAKER: [INAUDIBLE]-- I can give you a concrete practical about everyday life example that you probably know about in this particular view of [INAUDIBLE]. But imagine you go with your car on vacation for two weeks, and your children all need Pampers [INAUDIBLE]. And you can take them with you from your store. Well, you know how they are. They are more expensive but reliable. But you don't know how many you're going to consume. But you get a certain minimum amount per day, and you hope you don't go over the limit.

Now, it takes lots of volume. So you have to trade off your space because you have fixed space in your car. You cannot take more than the volume available. And so this is exactly the kind of reliability curve you have. You can take too little with you. You have to buy the wrong stuff when you get there, wherever you are. And then it might have leaks and failures and not worth it. So you'll need more than what you thought initially and cost more as well. So actually, this is extremely important in everyday life.

PROFESSOR: OK, so I like your-- I'm past that stage with my kids several years.

GUEST SPEAKER: Me too.

PROFESSOR: But I'm going to amend your example in the following way. Basically, if you had two kids, and they're very different, like one is really tall, and their same diapers will not fit, then you have a problem, right? But if they're twins, or if you buy stretchable diapers that have a huge range, then you can cut down, right? So you have to have like different kids in the car. Then it works. I think then the example works.

OK, let's see. We're kind of running short on time. So one more example. This is based on the doctoral thesis of Jeremy [? Oktay. ?] He's a flight test engineer. And the question that he looked at was robustness of degraded airplanes. So the idea here is that some systems are going to be used longer in long, ultra-endurance kind of systems where you do not have the option of repair. You don't have the option to land, repair, and fix the system, and bring it back to its pristine everything-is-working state.

And on the right side here, you see some examples of-- these are real systems that people have worked on, or are working on, or are thinking about that have this situation. The DARPA Vulture is a program where a UAV would stay aloft for five years with no landing and a repair allowed. So you can obviously see it's got solar panels, and I think it has fuel cells as well, if I'm not mistaken. So how do you achieve that?

This is an example from Antarctica flying several UAVs to map the ice sheets. This was a gap solution while the iSat satellite between iSat I and iSat II. And then here's a human colony maybe on the moon or looks like the moon. So we have this dome here. This crater has been covered with a dome, and we have a greenhouse inside. So life support systems that have to be super reliable for a very long amount of time.

And so the question that Jeremy looked at is, how do we design and optimize systems that have ultra-long endurance, where you know ahead of time that failures will occur? Failures will occur, and you can't repair the failures easily. So you have to design the system apriori, such that in those partially-failed states, it will give you the maximum residual performance that it possibly could.

And it turns out, when that's your objective function, you design the systems differently than if you just optimize nominal performance and then worry about what happens if there's failures. And this is the second paper that I uploaded for you. So both of these papers "The Reconfigurable Spares" and then this one are uploaded both on Moodle and Stellar if you want to take a deeper look.

So the case study here is the C-12-- this is the King Air airplane. This is the military version of it and typically flies out of Edwards Air Force base. And the idea is that there can be different failures on this airplane. So this diagram, this is a so-called Markov chain where n means nominal. And you can see the table that goes with this. Nominal means nothing has failed, and you just do turn control. This is climbing, left-turn climbing. You just turn control with your ailerons, which is just standard flying.

And then different failures could occur of different elements. So the left engine, the rudder, and the aileron could fail. Of course, a lot more can fail. But in this case study, those are the elements that are allowed to fail. And so 1 means the left engine has failed, 2 means the rudder has failed, and 3 means the ailerons have failed. And then as you move to the right, it gets worse and worse. So state 4 means you lost your left engine and the aileron, but you still have your rudder.

And then, the worst is state 7, where everything's failed. The left engine's failed, the rudder, and the aileron has failed. And what you worry about is what we call availability. Expected availability is what's the probability or fraction of probability that the system will perform above some minimum threshold, which in this case we call WM. And then expected performance is

the probability of each of these failure states multiplied by the performance that you're still getting in that failure state, OK?

And what was done here is to say, OK, we know what the C-12 airplane looks like the way it exists today. But what if that airplane had been designed slightly differently? Low value and high value around the baseline, a little bit bigger wing, bigger tail-- how would it impact the performance, not just the nominal, but the off-nominal performance in these failed states? So just to show you why this is interesting or relevant-- I picked out the most interesting failure states are the intermediate ones here, these partially-failed states.

And so on this picture, you can see in red what's failed on the aircraft, and then plotting bank angle versus specific excess power, which is essentially your ability to climb in feet per minute. And this is all calculated through a simulator, a pretty accurate six degree of freedom simulator, where you can actually modify the airplane. It's a very cool open-source simulator that Jeremy modified where you can actually fly the airplane simulated, and you can change the plane during flight. Like you could grow the wings as the plane is flying-- like morphing wings and things like this.

And of course here, you fail parts of the airplane during flight. And then, the flight dynamics are automatically the physics, automatically you have to adjust to that failure. So this is not like spreadsheet-type analysis, just so you know. So if you're inside the safe region here, then you can keep the bank angle between-- we defined it between 25 and 35 degrees-- and you have positive rate of climb. Then you're still in the safe region. And each of these points here is a slightly tweaked version of the baseline airplane.

So what's interesting here is in some of these states, you're outside of the safe region. So a small difference in the design of the nominal airplane will mean the difference between losing the plane or still being able to fly. So these points that are out here, these are the interesting points because they fall outside the safe region. And the points inside are inside the safe region. Everything is the same except the airplane geometry has been tweaked.

And then of course, state 7 everything has failed. You lose the airplane. There's no way to recover the airplane. So in some cases, it's very clean. It's very clear what will happen. And these intermediate failure states are the interesting ones because small changes in the upfront design make a big difference in how the airplane will perform in a partially-degraded state or partially-failed state.

So the other thing you can do then is you can do a sensitivity analysis and say, well, how sensitive is, for example, expected performance to the various design variables in the airplane? Like rudder cord, and I'll talk about vertical tail here, and the engine failure rate, and so forth. And the difference between the yellow and the green is yellow is an eight-hour mission. So this is a typical eight-hour mission. You fly, you come back. And if something's failed, you just repair it. In the 20,000 mission, 20,000-hour mission, you can't come back and repair.

So what you see here is interesting. It means the sensitivity of performance to these design decisions depends on how long you will operate the system. And because the longer you operate it, the more likely is that it will see these partial failure modes, which will then influence the degraded or the residual performance of the airplane. And the most interesting parameter here, if you just look at this diagram beside the engine failure rate-- so the engine failure rate matters a lot when you fly a 20,000-hour mission.

But if you look at the cross these parameters, which one of these is the most interesting? Which one of these is the most interesting parameter? Let's see at EPFL. Can you see this diagram? Which one of these parameters is the most interesting? Go ahead.

AUDIENCE: The vertical tail?

PROFESSOR: Why?

AUDIENCE: Because it has different behavior for the lifecycle and just for the single mission.

PROFESSOR: Yes. So if you're only going to fly short missions with it and then land and repair, you see the sensitivity is off to the left, slightly negative sensitivity. So you could actually make it just a little bit smaller. But if you're going to fly very long, you should actually make it bigger. And this particular airplane has an undersized vertical tail. It has a Dutch roll mode, where it has a yaw damper that was added later. And so if you're going to fly for a long time period, you're going to see a failure mode that will then exasperate that particular failure mode.

So what it means is that if you're actually going to design this airplane for a 20,000-hour mission that you would design a much larger vertical tail which penalizes you in the nominal. It penalizes you in nominal operations, but it will benefit you in these partially-failed states. Does that make sense to you guys? You guys were laughing, or smiling, or thinking about this.

AUDIENCE: Yeah, it does.

PROFESSOR: So have you flown this airplane? Or do you have experience in it?

AUDIENCE: We did a flight test course, and we tested that troll.

PROFESSOR: OK, so this brought up some fuzzy memories or--

AUDIENCE: Yeah.

PROFESSOR: I mean, it's basically the wing tip does like a figure eight. That's sort of classic.

AUDIENCE: Right.

PROFESSOR: That's the classic manifestation of Dutch roll.

AUDIENCE: Yeah.

PROFESSOR: But if the Dutch roll is too big, you can actually lose the airplane. You can induce an instability. So this is a big deal. Yeah?

AUDIENCE: Would that mean that the vertical tail is sized properly then? Because you can make it smaller and get a little better in this area, or make it bigger and get a little better in this area. Because It seems like the vertical, like, other things--

PROFESSOR: It's fine with the yaw damper. It's fine with the yaw damper. But actually, there has been an airplane lost. There has been an airplane lost in flight. And the accident investigation showed that it was basically a Dutch roll mode that became unstable. And so the point here is, if you have a failure, then you're in trouble with the small vertical tail. But if you don't have a failure, then you're probably OK.

And that's the whole point of me showing you this-- is to make the point that if you are going to deal with a system or operate a system that is going to have a very long operational life, long endurance, without the possibility to land, repair, and send it back out-- so it's going to be perfect and pristine on day one. And then gradually, stuff will fail, and that's the case for infrastructure, bridges, spacecraft past Neptune, airplanes that are going to be aloft for five years. You just have to design them differently.

You just have to design-- and this is hard for engineers to think about-- that I'm actually designing for failure. I am designing a system expecting that it will partially fail, not completely,

but partially fail. And by taking that into account, the design looks different. This is kind of non-conventional. OK, final thing, post-flight review-- what happens at the post-flight or post-launch review? PLR, PFR.

So essentially, what you do is you review the telemetry from flight. You compare against your predictions. You find repair any failures. You secure the data for later use. And then you initiate the detailed commissioning and hand-over to Operations. And here's a detailed list of entrance and success criteria for post-flight review. And I put this up here because those of you that will actually go to the CanSat competition, this is part of the package. You are expected to launch your payload, do the flight, and if something goes wrong, you can maybe have a backup flight.

And then after the flight, you do a post-flight review. And good post-flight reviews are planned ahead. You already know what data you're going to analyze, if you already have your software ready to suck in the data after the flight and really get insights out of it. Summary here-- this is just kind of a checklist for thinking about operations.

System check-out and the lab, hangar, field-- is everything working OK? Bring sufficient consumables, spare parts, tools, support equipment, remote control, telemetry, cameras. Train the operators and support personnel. Checklists for nominal operations and routine emergency and contingencies. Think about your transportation logistics and plan enough time for a ramp-up for commissioning before operations.

OK, so that was all I wanted to cover today. Any questions about commissioning and operations? My main point in this lecture today was to kind of get you excited about operations and to highlight that there's a lot here. System engineers are not done. After CDR or PDR, you say, oh, I did my job as a system engineer. It's up to you guys, the operators. No, no, this is territory for system engineering as well.

And in the end, you just have to get operational experience. There's no substitute for actually being out in the field operating systems and getting that experience. Any questions or comments about this? OK, so a quick reminder, a quick reminder, we're going to have our PDR. You saw the schedule. Monday, Tuesday, Wednesday, please log in five minutes before. We're going to be using my WebEx Personal Room. The link is here. Upload your slide deck. 30 minutes presentation, and then we have up to 30 minutes of Q&A. All right? Questions?