

Good morning.

I am filling in for Professor Hoffman who is off addressing the French Parliament at this moment, or maybe it was yesterday afternoon.

Tough choices of whether to stay here or go there.

Well, that's right, Noah.

These days the issue of knowing where you are, navigation is really taken for granted.

We have GPS in our cell phones.

GPS in handheld devices.

GPS tells the taxi driver whether or not he should be turning up that one way street.

When we began with human space travel, particularly as we entered the Apollo era, the question of navigation, along with guidance and control, was still a major issue.

In fact, it was rather uncertain whether or not, in the Apollo mission, we were going to be able to, with assurance, do all of the navigation required for going to lunar trajectory and then doing the precise navigation to land on the moon.

The history of leading guidance navigation and control has now, for a period of over half a century, been located just adjacent to, at one time part of MIT, the Instrumentation Laboratory, now Draper Laboratory.

And the tradition carried on through Apollo to the Space Shuttle Program.

And then, as I think as you are aware, beyond that into NASA's current plans.

We're privileged today to have discuss with us the guidance, navigation and control issues on the Shuttle, Dr. Phil Hattis.

Dr. Hattis, a graduate of Northwestern and Caltech with his PhD from the Aero-Astro Department at MIT, has been at Draper since 1974.

He is a member of the Laboratory Technical Staff, which is the highest technical position available there.

He serves as the Technical Lead for the Crew Exploration Vehicle Development Program in GN&C at Draper Laboratory.

Phil has been very active in AIAA.

He is a fellow.

He has been head of the New England region.

Has received the Draper Lab Distinguished Performance Awards and various NASA recognition awards for his contributions to STS-1 and STS-8 missions.

Then we will hear about Draper's contributions and the overall issue of GN&C.

Thanks a lot, Larry.

I should just point out, when I came up here as a graduate student to pursue my doctorate, I was a Draper fellow.

I started working on the Shuttle as a Draper fellow, so much of the work I will be talking about here, I was probably only a year or two older than any of you when I was doing this.

And that's turned out to be fairly useful to NASA because with the Shuttle still flying from time to time issues come up and they stick pick my brain about what we did in 1974, '75 and '76, which wouldn't had been so easy if I had been at my current age then.

But it is also a little bit alarming because it means the people that are working on the system now don't really understand why it was designed the way it is.

Now, the other thing they could have asked me for was the report on which this material was based, which I wrote in 1983 to educate the rest of the people at Draper who were going to work on the program subsequently about this system.

Now, the other thing I just want to say is feel free to interrupt me at any point to ask questions.

I am going to be covering a lot of ground, and I may not get back to the area that you're interested in asking me about if you wait.

So just raise your hand or speak up or whatever you feel like.

And the other things I want to point out are two things.

One, what you're going to be looking is largely what was done for the first Shuttle flight except where I mention specific upgrades.

Now, I am not going to be comprehensively covering all the upgrades that have been done to the Shuttle since.

What you will also note is this presentation will be largely monochrome.

And why?

Because it is drawn from a presentation of 1983 when there was no such thing as a laptop or PowerPoint and color was a real pain to get.

You had to go to the artist and then get it lithographically reproduced which was an incredibly cost.

What color you see, I've added now and it's limited, except for a couple of pictures at the end.

I do have some before and after cockpit pictures at the end.

You will periodically see a chart like this, topics of discussion, we'll go from section to section and we're going to delineate the areas I'm going to cover.

There are going to be a whole bunch of sub-bullets for each of these areas as I go through.

This will be not real deep, unless you ask me the questions and I will go as deep as you want with the questions but covering a lot of ground.

Some of these pictures you may have seen in one form or another, but I should just highlight certain points.

The systems related to the flight control were placed all over the Shuttle.

In the forward area, which was the only pressurized portion of the Shuttle, below the livable areas was the avionics bay.

And, in there where the computers, the inertial measurement unit, and I want to say something about that in a moment, what they refer to as multiplexers-demultiplexers.

You've got a lot of analog systems or you had to convert back and forth between digital and analog.

And the electronic boxes that drove the commands for the reaction control system thrusters.

And then you have hand controllers and displays and indicators in the cockpit.

In the back you have pods which have many of the reaction control system jets, the orbital maneuvering system thrusters.

And I will be talking quite a bit more about them later.

And there was also in the aft avionics bay that had specific subsystems for which it was deemed unacceptable to have them forward.

Some of them were local analog digital conversion boxes, but also rate gyros which were used during ascent and entry where they wanted them closer to the center of mass by being in the back and in the front avoiding some of the flexure issues associated with the long distance to the front.

This particular configuration you're looking at is before the external tank separated after the solid rocket boosters had come off.

This configuration is where the story begins because what I am going to be talking about is the part that Draper did which is the exoatmospheric flight control system.

And that begins at main engine shutdown and ends when you hit 400,000 feet on the way back.

There are different phases that we will be talking about.

The first is what we refer to as insertion which is from the time the main engines cut off to the time you do initial orbit circularization.

And that includes a brief but design challenge phase while you're attached to the external tank.

It includes the separation maneuver from that.

And, in the original flight profile for the Shuttle two burns of the orbital maneuvering system, the original orbit insertion strategy for the Shuttle put it in an orbit that typically had an apogee of about 60 nautical miles, a perigee of just a few nautical miles.

What you would do is the first burn would raise that perigee up to the 100 plus nautical mile target altitude and then the second burn halfway around the earth would put you into a circular orbit and then you would begin your mission there.

Later in the program for overall efficiency, in order to improve the payload margins, that strategy changed.

And they tended to do more what they call direct insertion which had a substantial higher apogee.

The perigee wasn't much higher but you would end up somewhere between those two.

And then you would do one OMS burn and you would get a net gain of maybe one or two thousand pounds which became very important.

During this insertion phase all the applicable sensors were on.

Now, I said I was going to say something about the IMU.

And most of you don't even think probably these days about having rate gyro separate from an inertial measurement unit.

You get these combined packages called inertial navigation systems now.

They're actually navigators that have the software.

They do all the processing for you.

They even have built in GPS receivers.

Of course, we didn't have GPS then.

The inertial measurement unit was a pretty clunky gimbaled device at the time the Shuttle first flew.

It subsequently got upgraded to ring laser gyro systems.

But that inertial measurement unit was simply outputting angles that were significant throughput issues.

Because you had to do a lot of data crunching to get rates from that.

Computers are really slow.

I will talk a little bit more about that in a few minutes.

Having rate gyros separate was a way to get data that these days would be all built into one box.

General purpose computers, all of them were on during ascent.

I will talk about the partisan of them, but there were actually five of them.

And the Vernier reaction control system, which is a small group of jets, and I will point those out later, were not active.

The larger thrusters were.

And then, after the second OMS burn, you transition to another flight phase.

And why all these flight phases, I will get to in a couple minutes also.

Then orbit phase began after the second burn.

You quickly open the doors so that you could dump waste heat.

The radiators are on the inside of the doors.

And, when the doors are closed, the heat just radiates back into the vehicle.

All payload operations are during this phase.

And you did a lot of power down to save.

You're working off of fuel cells.

It limits your mission life both because of the limits on the weight of the reactants and on the places you can put any extra tanks.

So you turn off the rate gyros, you don't need those anymore, and I will explain why.

Two of the five general purpose computers were shut down.

This also being a late '70s computer design, you're talking maybe on the order of a couple hundred watts per computer which, by the way, I will explain more about, but was a 104,000 word memory capacity.

That was actually an improvement from the approach and landing test when it was 64,000 words.

And then you turned off two of the three redundant inertial measurement units, except for critical phases.

Also the safe power, the feeling was that if you lost your navigation reference you would have a relatively benign environment to bring one of the others up.

And the Vernier thrusters were made available because they were used for flying control.

Then you have the deorbit phase.

You close the doors again.

You do the deorbit burn.

You dump any residual propellant from the forward tanks by simultaneously burning opposing thrusters in order to get an acceptable center of mass for entry.

Getting the acceptable location of the center of mass for attitude and thermal control during entry is very critical.

You reactive all the sensors.

You go back to all the computers being up.

Then you turn the Vernier jets back off and you fly the vehicle using this mode until you're at 400,000 feet which is about where you pick up 0.05 Gs.

And that is where the entry phase takes over.

And this is just a summary of the profile.

Now, this is where I wanted to take the opportunity to talk a little bit about computers and profiles and everything else.

When we started this program with a 64,000 word computer, I talk in terms of words instead of bytes.

The architecture of this computer didn't have bytes.

You had words and half words.

Each word was equivalent to about four bytes in terms of number of characters you could insert into it.

But you only could break it down into pieces of two.

So we had 208,000 - well, a thousand times 24 pieces of memory that we could work with on this computer.

For the approach and landing test, which was very limited, you flew it off of a 747 for a couple of minutes, 64,000 words worked just fine.

And they were chugging along with the program saying we're going to get all this orbital mission stuff into that computer.

And, of course, we discovered probably a year after we really began the job, we began the job seriously in '75, and by '76 it was obvious 64,000 words wasn't going to work.

They upped it to 104,000 words.

It was probably obvious four months later that 104,000 words wasn't going to work.

So the solution, in addition to descoping as much as possible, what you had to have was to separate the computer loads that you had for up and down which you did when you were doing your orbital mission.

And then you had something called the mass memory device which is basically a tape drive which when you went from this phase to this phase would reload some of the computers.

And then you went from this phase to this phase we'd reload them again.

And I said there were five of these computers.

Four of them, of what I'll be talking about, were the primary computer set.

Quad redundant so that they would vote all data going in and out to decide whether or not there was an inconsistency between one computer and the other.

And it would automatically deselect the bad computer, the implications of which I will talk about probably about three-quarters of the way through the presentation.

When you went up and down, all four computers were operating the same software.

The fifth computer was called the backup flight control system.

And the reason it was there, these four primary computers, a chunk of that 104,000 words, probably 30,000 to 40,000 words was used to assure the computer set operated successfully redundantly.

There was always a concern that there would be a generic software error that would show up at some bizarre time and that you could pull down the whole computer set.

It was an independently coded similar architecture from the standpoint of algorithm content, but independently coded software called the backup flight control system that on the hand controller there was a button the crew could hit, a panic button, if they needed to.

And the system would revert from the primary system backup system.

It never happened in the history of the program, it has never been used, but it is still there.

And so those five computers are all operating on the way up and on the way down.

Now, when you go to the onboard phase, and only three computers are up, you freeze dry, as they say, to the computers.

One computer remains the backup flight computer turned off ready to turn on from emergency entry to backup.

The other one is a primary software load ready to start.

The remaining three computers, two of them were redundant set for the on-orbit functions.

And one of them, again, because of memory problems, everything payload related was in a system management and monitoring other non-flight control related functions with one of the other computers.

They did this spread of functions across computers, in addition to adding the tape drive in order to accommodate the memory constraints because the Shuttle Mission was so much more complex than what the computers were originally designed to accommodate.

So you say it never happened.

Have there been instances in which any of the backup computers have been brought online?

There have been instances in which primary computers have failed.

There has never been an instance in which they've reverted to the backup system.

Now, when the primary systems fail, and I will elaborate this in more detail, while each computer computes the functionality for everything, they only control more or less a quarter of the subsystems.

And there is a distribution.

And some of the charts towards the end will talk about how this was done.

And there are implications associated with what you lose when the computer goes down.

But, if you have time in your noncritical flight phase, you can restring those things to the remaining healthy computers and recover accessible systems even though that computer has gone down.

Now, on STS-9, that was incidentally our MIT department's first Shuttle flight.

And it had, Byron Lichtenberg, one of our people.

And what turned out happened to be floating solder balls and an early version of these computers that caused

intermittent shorts.

And one computer went down before entry.

They recovered the string.

Another computer went down during entry.

And, because they had reconfigured the string, they had three of the four strings left but only two computers.

And another one failed on touchdown.

And had that one failed before touchdown they probably would have reverted to the backup system.

That's the closest they ever came to a backup system.

Now, the question that comes to my mind there, since the generic failure was not software but floating solder balls, which all the computers were susceptible to, what would have happened if they had gone to the backup system?

Because it could have gone down, too, and then they would have had nothing.

Because, once they've gone to the backup, it is not easy to revert in critical flight phase to the primary system.

Lichtenberg, as I mentioned, was a crew member from our lab.

Later I asked him how did he feel when the first computer went down and then the second computer went down?

Byron has an aero-astro PhD and pretty savvy.

He said he was pretty worried until he looked at the commander, who was John Young, and John said well, we might as well go to sleep because we're not going to reenter today.

And when John went to sleep he said he might as well go to sleep, too, and it will be all right.

And it was.

Yes?

[AUDIENCE QUESTION] The computer was the same.

The software was not.

The computers themselves are all interchangeable AP101 computers.

Subsequently, they were changed to AP101S computers, which is modified version that was used on the B-1 Bomber.

And they went to 256,000 words of memory.

And that is the current state-of-the-art.

You have to understand several things.

One, it is very expensive to upgrade systems that are already flying.

But, independent of that, you never fly in space something that is close to the state-of-the-art because you have to go through all the qualifications, which takes a lot of time, and it has to be radiation hardened when you're in space.

And when it's a human vehicle, it has also got to go through human qualification.

The Space Station architecture is IBM 386 processor quality, so it is basically like maybe about 1986, '87 early laptop generation computers.

[AUDIENCE QUESTION] Oh, yes.

There were quite a few missions.

I don't think there have ever been any missions where they lost two.

The IMU failures don't seem to have been anything systemic but just sort of a random problem.

And I'm not sure since they have gone to the ring laser gyro systems that they have had any failures.

I think it was the mechanical ones from the early days that they had some problems.

Now, major requirements for the systems.

We had two different autopilots for three phase transmission which incorporated both the insertion and the orbit features and on-orbit, so we only had two different software loads on that tape drive for the primary flight control system.

The rules for Shuttle were that after any subsystem failure you have the capability to remain operational.

No critical functions were lost.

After two failures, safe operation, all critical things necessary to terminate the mission and bring them home would be possible.

But some of the mission objectives may not be achievable.

The system was mainly aimed at controlling rigid body characteristics and velocity changes within specification.

Only when we started to look at docking with the mirror in the Space Station did we start worrying about flexible body effects.

And it was because of what they were attaching to and not because of the Shuttle, all those appendages and those things.

If Shuttle does control Space Station and did control Mir when it was docked.

And so there have been some modes, which I won't really be talking about today, but were created to facilitate that control without causing unacceptable loads on those flexible appendages of the stations.

And 80 millisecond app cycle, two reasons that happened.

We originally planned to do 40 milliseconds.

The approach and landing test program was.

First there is less process of burden if you do it half as often.

And the other, when it came to the reaction control system, as we discovered in about early 1980, a little more than a year before the first flight that there was a water hammer effect in the propellant lines on the RCS jets were the opening of the valves caused an expansion wave which reflected as a compression wave.

The closing of the valves caused a compression wave.

The inner section compression waves, if the valves were opened and closed too quickly, could cause a catastrophically large compression wave that could burst the line.

So they deemed it better rather than redesign the entire feed system to limit us to never firing faster than 80 millisecond cycles.

Now, that differed from Apollo.

Apollo had 100 millisecond cycle time, but they had the ability to interrupt the cycle to turn out enough jets if they wanted a short firing.

We couldn't do that because of the water hammer effect.

And also because the propellant feed system involved a liquid in the tank with zero G acquisition devices around the surface of the tank directly exposed to the pressured helium, which means some of the helium dissolved into the fluid.

If the fluid was drawn too fast the helium could bubble out causing a gap in those zero G acquisition devices around the tank preventing flow.

If you get unbalanced flow of hypergolic propulsion systems you can also get an explosion.

So the solution to that was limiting how many jets you could fire at one time off of one tank.

Does everybody understand what the zero G acquisition problem is?

It's a surface tension base.

You have various types of rings and shapes on there that captured fluid by surface tension to there, which would begin to draw the fluid.

And once you began to get some flow because of firing things it would pull the blobs of fluid into the tanks and into the feed lines from the tanks.

As you recall, the origin of the problem is that the fluid would not be at the bottom of the tank so you risk drawing a bubble.

The surface tension holds enough there to start the firing.

When you fire you get some force.

The force draws the blob to the same parts of the tanks where you can acquire the fluid.

And, as long as you don't draw too fast, the communication between that part of the tank and the fluid remains.

This was a very complicated qualification program.

A lot of C135 parabolic trajectory time got used to test out various perturbing of the inside of the tanks.

And I am not going to talk about that in detail but I'm sure there are a lot of papers out in the literature about how they qualified these things.

And I don't think there were too many systems before the Shuttle that actually did it this way.

One used systems that tended to use membranes where you had the pressure on one side and the fluid on the other side, and the membrane would just force the fluid to stay in contact.

But the problem is the membranes would degrade over time on exposure to these hypergolic propellants.

Hydrazine and nitrogen tetroxide are very chemical reactive materials.

For instance, it was supposed to be used over many years up to a hundred times.

The idea that you would have periodically keep opening up these tanks to change a membrane was not attractive when you consider the tanks are deep inside of the structure.

So this may have been a unique issue because of a reusable system, but it also may be relevant to systems that even if they aren't reusable have to have a very long life in space.

Modes and submodes I will quickly go through, but you have rotation and translation modes.

These modes could be used simultaneously for the RCS system and then separately for the OMS system.

And you had special modes which to get extra oomph out of the RCS jets, if you had an abort, that would sometimes be done if the OMS engineers weren't available.

The OMS engines, there were two of them which were up on the back right and left pods from that picture I showed a few minutes ago.

And you could use one or two depending on what you were doing.

And in the RCS rotation modes, you had various ways you could use it.

Proportional meant you moved the stick.

The response you get is in proportion to what you do, how long the jets fire.

Discrete means you move the stick and you get a specific amount of rate change.

Pulse means you just get a single little pulse out.

And acceleration means as long as you're holding the stick out it keeps firing them.

And those are all.

There were push button displays that the crew could adjust.

There were some modes for each of those which affected how many jets fired, whether or not you wanted to force it to use something that approximated couples or you were in propellant conservation mode and you were willing to get accept getting a rotation rate.

With coupled in the translation you would care about that effect.

And in the translation there were various submodes as well.

And, in particular, you would use more jets when you were separating from the external tank to get away as fast as possible.

Yes?

On the previous slide, are there different modes for the RCS jets?

Was there one that they happened to use the most or was like supposed to be the primary usage or are they all part of the normal operating?

I think they would rarely use this or this.

I think these two were commonly used.

This is very fuel inefficient.

It would only be used as kind of an emergency measure.

That's also very difficult from the point of view of the pilot to have direct acceleration control.

Right.

I mean this might be something you would call upon if actually, for some reason, the vehicle started to spin up unexpectedly and you would have to neutralize that.

Does that adequately answer your question for now?

There will be an opportunity to collect a little more detail on that later.

But, again, you wanted to get off the tank quickly so you would use all the jets you had to get off of it.

You wouldn't do that later.

You would have more jets that you would use for roll control while you're on the tank because you had a much higher roll inertia.

You want to only spend a few seconds on the tank after the main engines shut down.

You could often be left with residual rates you've got to quickly kill.

There was an inhibit on the separation if you had more than half a degree per second on each of the axes.

There was actually a phenomenon on the first Shuttle flight which almost got us in trouble.

One of the first things that happens after the main engines shut down is you slew the engines back to stow position where you want the engines for entry.

The reason is the auxiliary power units are needed to move the main engines.

You want to shut those down and save the hydrazine for those until you get back to it just before entry.

On the first Shuttle flight they kicked those engines at about one hertz.

It turned out the first fundamental mode, the rock mode of the orbiter on the external tank had a subharmonic of about almost exactly one-fourth of that slew rate on the main engines.

The slewing of the engines then causes the rocky mode to be excited.

We were seeing oscillations very close to the inhibit for the separation.

The crew was getting a little worried but we just got it in bounds in the automatic mode.

And if they hadn't separated in time it would have gotten pretty complicated to do it manually.

We made quite a few changes after that.

There were a lot of things we learned on the first flight, and I will point a few of them out as we go along.

There was also a launch pad phenomenology.

It is not part of my talk.

Has this come up in the class about the shockwave from the SRB ignition?

Yes.

OK.

They didn't have those waterbeds in there on the first flight.

What was relevant here, one of the things that you may or may not know is that the struts that held the forward RCS tanks on the first flight were buckled almost to failure.

That wasn't realized until they got home, but had they failed they probably would have burst and blown up the vehicle.

The on-orbit modes, we have both primary and Vernier jets which were only used separately, except under special circumstances which were designed substantially after the first flight.

We have local, vertical and inertial frame of reference control capability with respect to the discrete rate mode.

And, otherwise, it is pretty similar to what you saw in the previous picture.

And submodes, some features were added because of rendezvous.

You could fire a lot of jets on the fort side.

If you wanted to do a rapid breaking, you could inhibit all the jets to fire in that direction.

If you wanted to limit the use of plumes, it turns out that you didn't lose completely your translation control authority.

Because the jets, in the front and back, that were in the x-axis coupled about 20% of the trust into the z-axis.

So if you fired them simultaneously in both directions you could avoid pluming an object in front of you and still get enough translation to control that axis.

And, just to show how everything was hooked up, the inertial measurement units and rate gyros and hand controllers and panel controls all went in through these multiplexer devices feeding the signals then into the computer and displays.

And then you had outputs going through these similar types of electronic boxes specific to the reaction control jets that generated the commands that were needed by the solenoid valves that actually opened and closed the hypergolic feed lines.

Looking at the whole top level architecture then of the GN&C system is all those boxes feeding into what was inside of the computer.

Inside of the computer you have subsystem operation software managing each of the subsystems doing the redundancy management.

The specific guidance navigation control algorithms.

There was a moding and sequencing function which was based on both manual and automatic scripts.

Then the actual driving of the displays of controls is interactive with the flight control system both ways providing feedback to the crew members and accepting their inputs.

And then what was left was the system management function on this computer that didn't go into the separate computer.

By the way, anything related to robotic arm operations were operated through that separate computer.

One of the issues that came along later in the program is the flight control computer never knew what was happening with the arm.

If you take a space telescope sized payload and put it 40 feet out there, it drastically changes the mass properties.

And one of the features you will see a little later that we stuck in was the ability for the crew, by pushbutton, to select different tables about expected accelerations of the jets because we didn't know when we needed to respond to that.

There were also flexure issues with the arm which came up as they went along, too, and established constraints on how we operated.

But was there any thought given to having an adaptive system which would identify the current parameters?

That would have gone way beyond the capacity of the computers that we had.

It would be relatively easy to do with the programs we had but it would never fit in a 104k memory computer.

But there has been lots of work that some of my graduate students have done over the years of how we should

have done that.

Brent Appleby, who is now a division leader at the Lab, actually did some work back in the `80s, I think that may have been his master's thesis, on some of those issues.

[AUDIENCE QUESTION] But, in reality, we're approaching very large memories which would allow you to do it.

Well, when we go into CEV, we're probably going to assume that 100 megabytes is no big deal.

[AUDIENCE QUESTION] unfortunately was cancelled, but we were doing exactly that.

We knew exactly the position [NOISE OBSCURES] all the movement when we were grappling.

And we were changing all the tables based on the current angles [NOISE OBSCURES].

It is a real challenge to maintain stability on a system where you have no insight into that.

But you would never build a spacecraft that way today so I'm not sure.

The challenges we have are very interesting but probably no longer relevant.

The challenges that remain are the flexural dynamic interaction problems.

I just wanted to indicate that within the control laws you have a steering processor, which I will talk a little bit about more, an RCS jet processor, a state estimator and an OMS processor.

The state estimator is unique to the on-orbit flight.

And there is more that represents that in a minute.

So I am going to now, having entered the overview, go into each of the subsystems in more detail by pulling up this picture to talk about it a little more, these subsystems in the context.

The forward RCS system had 14 primary 870 pound jets and two Vernier 24 pound jets.

There were 24 and 4 respectively.

Those systems in back evenly divided left and right.

Each of the pods in the back had one OMS engine.

The forward RCS system had its own self-contained hypergolic tanks.

The aft system had RCS tanks and OMS tanks which could be interconnected from within the pod or could be cross-fed across the pods.

Now, the consequence to the flight control system, there were different constraints and simultaneous jet firings.

And how you counted, whether it was only left or right or both, depending on which mode you were in, if you had a mission and needed a lot of RCS propellant and you had spare space in the OMS tanks, it allowed benefiting from that.

Why are there so many thrusters pointing in the same direction?

For redundancy?

Yes, redundancy and maximum control authority.

You want to find control authority normally with redundancy but for external tank separation you wanted high acceleration in one direction.

For high rendezvous breaking you wanted high acceleration in the other direction plus or minus Z.

And for backup to the OMS engine you wanted to have higher acceleration in the plus X direction.

And then, when you were doing entry, which I'm not talking about today, you had an on-demand RCS control authority in the upper atmosphere during hypersonic flight.

And you would turn on one, two, three or four yaw thrusters in particular as needed.

I think one, two, and occasionally three thrusters had been turned on during disturbances.

One of the things we've learned from the telemetry of the Columbia accident is as this vehicle was falling apart for probably 20 or 30 seconds, the vehicle was controlling very nicely because they kept turning on more and more jets.

They were getting major torque imbalances from missing pieces of the vehicle.

But it was still controlling the attitude until the damage got so severe that was no longer possible.

Again, I already talked about the number of the thrusters.

The primary thrusters, for the reasons we talked about, there were many jets.

And also because translation and rotation control was accommodated by these Verniers, a feature I will mention briefly later.

It was only a rotation control system and fundamentally does not have redundancy.

I already talked about the on-time.

These are just typical propellant loads and thrust levels and specific impulse numbers.

You notice that large maneuvers are always a little more efficiently done with the primary jets and even more efficiently still with the OMS as you will see in another chart.

Life for duty cycles and on-time are relevant for a vehicle that is going to fly a lot of missions.

Flying control almost always will be done with Vernier jets, not just because of propellant, which it is much more efficient, but also because you will get a lot more mission life out of it.

This is a stick drawing of those.

There is a numbering system associated with it.

FRL for which pod it's in.

Up, down, forward, right, left.

The last character for which direction it fires.

And then the middle number is a manifold.

If you see a five that is the Vernier jets.

One, two, three or four, any pod that has got the same middle number is on one manifold.

If a failure shut that manifold or a string took down that manifold, all of those jets were lost.

When you lose a string, you would have one manifold per pod that you would lose.

That means under some circumstance, because the Vernier system is redundant, a single failure could take that out.

But that wasn't critical to carrying out most mission objectives or to safety.

That is probably enough said on that.

The OMS, typical propellant loads mentioned here.

On-time, never less than two seconds.

Never less than, with one engine, 12,000 pound second impulse with a 6,000 pound thrust not suitable for fine maneuvers.

The RCS jets would always be used to trim out any large OMS burn errors.

Had a significantly higher specific impulse.

For large maneuvers you're clearly better off from a propellant weight perspective using that system.

Each of the engines had redundant gimbal control, redundant by having one mechanical screw system, but you could drive the nut or you could drive the screw.

And there were different electrical systems that did that.

This was the maximum authority.

And the two axes at each engine could move a portion of which was used to tract the center of mass as the vehicle consumed propellant or delivered payloads and a portion of which was for actual thrust vector control management.

We also had to subtract a little bit.

You never want to go too close to the hard stops because you risk mechanical failure by doing that.

And you always have a little bit of mechanical uncertainty of exactly where you are anyway.

A portion of that was a mechanical uncertainty and a portion of that was just a mechanical safety margin.

This is a drawing in the two different planes of the rotation of the engines showing the span between the center, say about 15 feet apart, no surprise given the general cross-section of the Shuttle.

An important thing to notice is that the engine, while I can point through the CG, is not pointing anywhere near the body access of the vehicle.

And, by the way, the vehicle body axes weren't -- There was a significant offset between the principle axis of the

vehicle and the body axis component of inertia, and the body axis was quite large.

Three units, even with the replacements they have gone through over the years, there remains three units for the INSSs now, but the IMU where mechanical systems with quanta for knowledge of state which were not all that small.

And the RGAs were even worse, the rate gyros.

These quanta were quite significant.

The reason was we had a half-word in that multiplexity multiplexer for translating the analog signal to a digital signal which determined, based on the maximum range, the maximum range being dictated by maneuver rates where possible during ascent and entry and not on orbit.

But we were stuck with that.

It was hardwired into the cards.

And so these quanta then, we discovered there was a one sigma probability of an every third cycle one quanta noise spike on the data that came across the MDMs.

And that was pretty significant when we were trying to do fine control during the transition phase.

Were the noise levels determined by this quantization, in effect, the [NOISE OBSCURES]?

The noise phenomenology was related to the electronics of the card, but it was directly related to the least significant byte.

But the mechanical sensors themselves were superior to that?

Yes, they were.

It was the MDM card that introduced the noise.

If you had used one word from the MDMs that would have [NOISE OBSCURES]?

Given the state-of-the-art to have processed that much information across the MDMs would have made it too slow.

We're talking orders of magnitude slower electronics from the late '70s than you have today, so the half-word was dictated by the data rates that we required of these boxes.

Now I'm going to go into specific features on the software side.

Yeah?

With the gyros, it seems on Hubble and Station, for example, we always hear bad news on the gyros having to be replaced every so often.

Well, first of all, what I'm talking about here, at the time the Shuttle first flew, are mechanical gyros.

Hubble may have started mechanical gyros.

They have been changed out at least once or twice.

And are probably fiber optic systems.

Hubble has the problem that it's in a fairly high orbit, 300 plus nautical miles high for the Shuttle anyway.

It has a significant radiation exposure, particularly when it goes through the South Atlantic Anomaly of the radiation belts which are 300 nautical miles.

Much more time they spend on that than at 100 nautical miles.

Cumulative radiation damage to the electronics in those gyros is probably a contributing factor to the failure rates that they're seeing on Hubble.

I would say they must spend a few percentage of their time in the South Atlantic Anomaly at that altitude.

Are the gyro replacements we're talking about measurement gyros or attitude control gyros?

Well, the fine guidance gyros are the ones that have been the big problem on the Hubble.

We're talking about quantitatively a different regime we're operating here.

The quantization, take away the noise effects, was something we could live with for operating the flight control system.

In Hubble, you want to be able to measure rates two or three orders of magnitude lower than what we're talking about here.

The actual design of the sensors is substantially different because they're trying to get very, very tiny little rates out.

These are trying to maintain the image lock when you're using the full magnification capability of the telescope and whatever target that it has.

Nevertheless, I would imagine that if the Shuttle gyros are staying at 300 nautical miles for five to ten years, they would fail, too.

Radiation is one of the fundamental drivers for all missions.

And it often that Atlantic Anomaly is one of the big drivers for low inclination.

Space telescopes are 28.5 degree inclinations.

So they don't have to deal with the magnetic fields coming in toward the poles which a polar mission has to, but there is this big dip in the Van Allen Belts off the coast of South America which poses a problem for everything that isn't low orbit.

The functionality we have in the autopilot, we use the rate gyros and the inertial measurement unit on the transitioned app to get states direction giving us altitude, giving us rate.

On orbit we have the gyro shutdown to conserve power, view data only.

That then dictates that we are going to have a state estimator on orbit.

We have to put some special features to overcome the rate gyro noise in the transition phase, which is irrelevant when the rate gyros aren't operating in the on-orbit phase.

We have the Vernier jets and the associated algorithm logic for on-orbit which isn't in the transition phase.

We worry a lot more about every detail propellant deficiency on-orbit because we spend so much more time there.

We have a lot of features we've added to minimize propellant there.

The OMS capability in the two phases is actually identical with both of them having a capability to wrap around the RCS jets to the thrust vector control should the thrust vector control not behave properly during that OMS burn.

And this just delineates the various features we have for steering.

OMS and RCS.

Where we add lots more features because there are a lot more things you are attempting to track when you're

doing your mission on orbit than when you're just trying to get to and from orbit.

Notice the rates that we're talking about.

Typically, you look at an INS box these days and you see hundreds of hertz data rates.

What restricted us here was how fast could we -- For instance, none of the software was in the sensor package.

It was in our computer.

And we had a severe throughput problem.

And the solution, since we had the rate gyros for rates and we only needed the IMUs for attitudes, and rates could be used to extrapolate attitudes for a reasonable period of time, was to greatly reduce the processing rate of the IMU down to on the order of one hertz, submultiple of 25 hertz which is why it is 1.04.

On orbit, since it was our only source of information, we had to eat a larger processing burden, operating on a 6.25 hertz, but we still were extrapolating in between the state estimate of one time constant.

We'll talk a little bit about what we're doing with that, but everything down here is operating at 12.5 and we're getting the data in at 6.25.

There are a lot of things you would do differently simply because you don't have these low rate constraints due to throughput limits.

The architecture then for the autopilot that is being representative on orbit is you would have a maneuver module where all the features for steering the vehicle would be, kind of an adjunct to guidance.

You would have these modes controlled by the crew and the push button display of what the stick deflections would do.

You would have the phase plane which would be tracking attitude error, rate error and whether or not you should fire jets as a function of those errors separate per axis.

Are there people here that don't know about phase planes?

OK.

Well, the concept of the phase plane, you go to optimal control theory and you look into a situation where you have a control effector which is on or off by directional, which is what thrusters are.

And you look at what it takes, given an error in a plane which is attitude error and rate error, and you want to get minimum time to neutralize that error to zero.

51:35 But you have lots of dead zones, which I will talk about more, to assure that you don't inefficiently use the jets so that you are not constantly trying to fire the jets to get exactly to the origin which is never possible.

The state estimator, which is a form of a Kalman filter.

And then the jet selection logic which is essentially for the primary jet lookup tables.

But it turned out to probably be the first use of real based intelligence.

We didn't think about these things in that time.

And, when I talk about the stringing later, I think we were also using an early version of failure tree analysis.

But, in the 1970s, none of these things were named.

And then you have various loads for the parameters that determine these dead zones and tables and all that.

And the crew would select these from push button displays.

For the OMS, you could either have hand controller inputs or cross-product steering and based guidance inputs which would then go into roll and pitch and yaw.

Thrust vector processing channels were roll and pitch coupled.

Roll is only possible, of course, when you're firing two engines by differentially pitching the gimbals on the two engines.

This would actually be an RCS loop automatically with one engine, but you had to have the two pads coupled when you were trying to do both of them.

But the yaw axis was separate.

Just keeping in mind the time.

Go through one or two more charts before the break?

That's fine.

I will go through the state estimator and then we can take a short break.

The state estimator, again, we were only getting attitude information at 6.25 hertz from the primary thrusters trying to maintain an estimate of the vehicle rotation rates.

We also wanted to know what disturbances on orbit you can have out-gassing the vehicle.

You have gravity gradients.

You have aero torques which have a diurnal variation depending on where you are on earth orbit relative to where the sun is which are tending to torque the vehicle in a particular direction.

Having knowledge of how that torque is behaving in a certain time enables you to manipulate your phase plane switching lines to more efficiently use the jets.

We were trying to estimate that.

Given that we only had IMU data with noise and quantization effects, we also had flexure we weren't accounting for in doing that.

So we had a low rate filter which incorporated the measurements directly and a higher rate filter which was also taking in feed forward information we're going to fire the jets.

We expect these velocity changes, rotational and translational, to occur as a result of the jet firing.

And you can build that into the estimate to anticipate that effect.

And then, given all that information, basically use that in the form of a common filter.

We had different gains associated with primary and Vernier jet usage because, given the factor of 30 difference in the rotational acceleration authority of these jets, they were fundamentally different bandwidth systems on the basis of the actuators.

We accommodated those different bandwidths in the software.

That, by the way, affected us when we started worrying about flexure on the arm because we found that some of the modes with heavy payloads in the arm actually fell within this bandwidth.

And, in the case of the Vernier jets, were falling right near the roll off point, which was the worst possible place to have a flexure mode.

And there were some significant design issues that were addressed later in the program as a result of that.

And then this disturbance acceleration -- Question.

At the time that you were designing these, was there sufficient knowledge of the structural modes or the bending modes?

For the RMS payload operations, not at all.

We first learned about that when we started looking at use of the arm to deploy the SPAS one payload in STS-7.

Nobody understood at the time we were designing for the first Shuttle flight the kind of coupling effects you would get from payloads on the arm.

It hadn't been modeled yet.

I would say probably about the time the first flights were occurring is when we started to look at that stuff, but the Shuttle software for the first flight was 95% frozen by '78, even though the flight didn't occur until '81.

You then discovered them in simulations or from flight data?

No, it was from high-fidelity simulations with the arm dynamics included in that.

We understood it pretty well.

We refined it after the flights.

We did even do some flight tests on STS-8 with an object called a payload flight test article.

The original payload on that flight couldn't fly in time so they put this 8,000 pound dumbbell on there and the arm was able to manipulate.

Went through all kinds of exercises and pretty much validated it with the simulations.

Were towing us at that point in time.

But it was a real lot of work that went into those high-fidelity robotic arm simulations and coupling that to the flight control system to get those numbers.

And a lot of work into evaluating what it all meant in terms of restrictions on the use of the control system.

And then the last thing I will talk about before the break, the disturbance acceleration estimator had a 56 second time constant.

Mostly the disturbances we are talking about were either orbital or semi-orbit, half-orbit type of periodicity.

You wanted to allow adequate time to integrate and determine their effect, but not so long that you weren't able to properly respond to it.

Somewhere in the one-minute range seemed to be about right for something that would have 45 minute periodicity.

And I think the next topic will be RCS processor.

And that is a good point to take the break.

Before we break, let me ask one historical question.

The timeframe for the design of this was mid to late '70s?

We began the work in '75.

There was a famous phase of '76 which is the Hay Scrub which is where we realized that not everything can go onto one computer.

The computer memory had to increase.

The real design architecture of what was going to be the first flight started to gel in '76.

The original expected launch date of the Shuttle was '78.

It kind of stayed ahead of us a certain amount of time, but we had probably 90% or 95% of the design done by '78.

We're going through detailed flight verification and crew training with Jeff being one of the crew members that was assigned to us.

And we would go out to Downey to do that in the '78 to '80 period.

In the design, now, you refer to the state estimator and optimal control.

By that time, had that methodology been completely accepted as a substitute for the classical control design?

Oh, yeah, I think so.

I think the phase plane concept first appeared, actually, in Apollo.

And there was sort of a rudimentary application of optimal control theory that was quite successful.

By that time I think the aircraft zoom maneuver [NOISE OBSCURES], people were happy with that.

The Kalman filter work, an early form of that also made it into Apollo.

I don't think we were actually pushing the envelope that much in using these things.

We actually carried over.

But Apollo, applying any of these technologies in the mid to late '60s, was very groundbreaking.

Any other questions before the break?

OK.

Let's take five minutes.

Am I missing anybody?

I know Larry hasn't come back.

Close enough.

OK.

Well, I'm going to go into the RCS processor now.

We've talked a lot about the presence of the phase plane.

We're going to go into some of the details in the jet selection.

Important consideration of the jet selection is we had to accommodate failures, maintaining control authority for any type of single failure, thruster, manifold, string, which you will see those later.

And you also had to be able to maintain adequate authority for safety with two of those combined failures.

We also had to limit plume restrictions, accommodate the tank constraints.

We talked about having couples, not having couples, the balance propellant in tanks to limit fuel usage when you didn't worry about translational coupling and minor orbital perturbations and all those other special maneuvers

that we pointed out before they required higher authority.

You had your manual modes going in and then you had all these steering modes which without orbit, in addition to the ones we talked about, discrete rate and pulse and acceleration and all that kind of stuff, you had various landmark tracking modes, orbital object tracking modes which were a guidance function providing inputs to the control loop, that all had to be managed through a proper way of manipulating the phase plans.

They were tracking the errors of matter with respect to the mode that you were in and then sending, based on the errors being detected in the phase plane commands, they would be processed by the jet selection logic.

The principles of the phase plane, we figured you weren't important enough to get started.

[LAUGHTER] You had a phase plane per axis.

Roll.

Pitch.

Yaw.

You had switch lines which were shaped based on the expected torques.

You always had a parabolic feature, but much more complicated than just that.

You added dead bands because you didn't want to fire.

When you didn't know exactly where you were, you wanted to be able to get in the general vicinity far enough from a firing zone that it would stay in the general vicinity for a while and then only fire when you had to when you were diverging from that.

You had to deal in the transition phase with that rate gyro noise phenomenology.

And you had to get the disturbance acceleration on orbit.

What we did about all those maneuver modes is each phase plane had an origin, the origin being zero with respect to sun frame and attitude and position.

You could move that origin at a rate or you could increment its attitude position if you were commanding the vehicle to do something such as a tracking maneuver or a discrete rate.

And that way the errors of the phase plane we're looking at with respect to where you wanted to be rather than in

absolute sense.

And you would always create [NOISE OBSCURES] in here so that if you had a big error you could spend a little bit of fuel to get to somewhere which would cause you to go in the right direction without continuously firing the jet.

Whereas, if you truly followed the parabolic switch curve you would just keep firing the jet until you were back to the origin which can be quite costly.

So I am going to show you this picture and then the on-orbit one.

These are the residual parabolic switch lines which, in the optimal control theory, would be going through the origin.

And then if you're out over in these region out here you will always fire a jet meaning a plus direction or the minus direction.

You're inside here.

You will fire until you hit another switch line on the other side.

The expectation is that you're coming in this way or you're coming in this way.

You want to get to a point where you're not likely to fire again for a while.

But then you also would be concerned because you don't automatically want to fire back right away because the rate gyro noise phenomenology could cause, where you think you are with respect to that line, to move back and forth causing you to fire too soon, causing the fire again to reverse that and get in trouble.

So what we actually did is if you actually hit this line and began to fire, each time you fired up to two or three times it would move the line out temporarily so that the quantum noise from that MDM would not make you think, even though you were moving this way, that you were going back out.

Because, if you fired that jet again, not only would you be spinning the propellant to go faster, you'd hit the other line a lot faster still.

For every time you double the size of the impulse that you use to reverse your rate, you're quadrupling the total propellant time.

Because, if you double the propellant each time, you hit a surface twice as fast before you get to the next one.

Now, on-orbit we didn't have that noise problem so we don't have that moving switch line there.

But we have this moving switch line.

If you're coming in you're looking to hit the zero line and cut off, but here you're not going to cut off until you hit the disturbance acceleration line.

It is expecting, when you hit that, that the predicted acceleration is going to say you're going to go up this way.

That means it will be longer before you hit another surface than if you start doing that over here.

So this one is a trick to lower the frequency of the jet firings based on other knowledge that we had about the acceleration.

Jet selection.

We had entirely different laws for the primary and the Vernier.

The Verniers had a very complicated configuration, had to be able to be fault tolerant, be able to handle simultaneous translation rotation commands.

It turned out, because of throughput processing limits, the correct approach was something like a table lookup.

But we had all kinds of rules we went through to say which kind of table did we want to go to?

What are the consequences of failures?

Do we want to start modifying the commands we've received because of what we basically know about which jets have failed and what we no longer can accomplish?

We actually had a Bullion implementation of those tables that actually got implemented as tables because we developed algorithms and IBM converted the software.

And they didn't necessarily do exactly what we told them.

Subsequent to that there was an experiment on the Shuttle called a phase space autopilot which is based on looking for velocity changes and optimal combinations of jets.

You would go through a linear optimal search and find the combinations.

That was flown a couple times for a few hours on Shuttle.

The experiment was quite successful but never converted into a basic shuttle capability.

But certainly with the processing capability that you have now would be a very good option as an alternative to what we did.

The Vernier jets, which were only used on orbit, only had six jets.

We weren't trying to deal with redundancies so an entirely different kind of scheme was done there.

We were looking to find the jets with respect to a three-axis command which best contributed to producing rates in that direction.

We could find a first jet that would be the best jet.

And then we could see, given how good that one is, is there another one which is half as good?

If so, we would pick it.

And, if we found one half as good, we might say if there is another one which is half again as good we might pick that and end up with an aggregate number of jets we would turn on to start producing the command.

This would be based not just on whether or not the phase plane said you should have a jet fire in an axis, but also on how big the error was but not yet to the point of hitting the phase plane line in the other axis.

And so the composite vector you were trying to neutralize would be a combination of the command and error reduction on the other axes.

And you would find the jets which would then respond your command and reduce the errors on the other axes.

Now, we would not re-compute that every cycle.

If we found that the ones or minus ones in the three axes for the commands were not changing, even though the fractional values and the uncommand of axes were changing for up to five cycles we would not re-compute the jets.

And that would minimize the duty cycles which was a life issue on the jets.

And then there was the other phenomenology I mentioned which is you start having large payloads or you're attached to Mir or something like that.

Mass properties are very different.

We don't know about that unless the crew tells us, but we could put a discrete number of alternative configurations in the tables for what we expected accelerations of the jets would be.

The crew could tell us which one applies, and then it would do this selection based on that.

The Vernier algorithm looks something like this flow chart.

Whereas, the primary algorithm would probably fill a 50 page flowchart.

The Vernier algorithm was very simple.

You go through and have a command vector which was ones and minus ones or fractional values, depending on whether or not phase planes have commanded an axis or just had a bias because of an error in that axis.

You would do a dot product of the six jets.

You would look for the maximum value of that dot product of the acceleration and the command.

And then, based on that value of that dot product, you would see if there was one that was half as good.

And, if there was one as half as good, you would see if there was one that was a quarter as good.

And then, if we already selected, we would be doing this counter of up to five times where we wouldn't recompute.

Now, I was just talking during the break about one of the constraints on here.

When we were using these computers, the dot product of a three vector by three vector took about one millisecond.

We had an 80 millisecond cycle.

And, in that 80 millisecond cycle, seven to ten milliseconds could be allocated to control some of the guidance and some of the other functions.

Six milliseconds was being used to do these dot products.

That is why we never could have considered doing something like that for the primary jets.

The TVC processor, we have instead of discrete control with thrusters, we have nearly continuous control because we're doing gimbal steering up to the nonlinear effect of a gimbal limit.

Remind them what TVC is.

Thrust vector control.

Moving the thrust of the OMS engine by steering the gimbals on which it is attached, which you cannot do with the RCS thrusters.

What we would do then is cross-product steering.

You have an error vector and a thrust vector, and the cross-product between the two could tell you the direction you needed to steer the vehicle to turn into the desired direction you wanted to thrust.

That steering command was then used to determine the commands we sent to the gimbals for moving the engines.

You had manual and automatic modes for doing that.

Generally, we were limited to two degrees per second because the gimbals were fairly slow.

We didn't want to get ourselves in a situation where we over-steered and had to correct back which would take a lot of time and maybe cost us some propellant.

But, if we got into trouble, the reaction control system could wrap around.

And that could happen automatically if the errors got big enough or the crew could induce that by hitting the hand controller.

And you have the two pads going into the manual auto mode.

And manual always overrides auto from any of these operations.

We had a lot of things we had to tolerate in determining our filter gains.

We didn't always know the thrust direction engines all that way because of mechanical misalignment.

When you build this thing an additional misalignment occurs after you launch the thing causing changes in the gimbal drive connections a little bit.

There are errors.

You rotate to a desired burn direction with the RCS jets before you light the engines.

You're never exactly there when you start up.

You can have failures during burns.

An engine can shut down.

An actuator can stop driving.

If it is the OMS-1 burn in the early Shuttle days, during that burn they were dumping the residual oxygen and hydrogen in the feed lines for the main engines during the burn causing torque disturbance on the vehicle that we had to overcome.

The OMS burn actually helped drive that fluid out of those lines.

And then, of course, we had steering noise and bias.

And then we had to have margins for things that all liquid propellant vehicles have.

Slosh, flexure, actuator nonlinearities and sample rate effects.

Now we had a design and then we had to change it.

And the reason we had to change it is we flew for a little while, and we discovered that these brushless electric motors being used for the OMS actuators were turning on and off at a high enough rate during the burns that they were overheating making a hundred mission life maybe two or three missions.

And they could take the pods off, but they were fairly hard to get and expensive to maintain.

So they asked us to change the bandwidth.

And that's what we did beginning with the twelfth shuttle flight making these changes here.

And that caused a little bit more sloppy behavior at the beginning and the end of the burn but didn't make very appreciable difference on the performance and made a big difference on the actuator life.

There was an outer loop just showing where the cross-product steering comes in and the fact that there are various filters and digital compensation effects that are going into this to deal in an adequate manner with all those effects that I listed a few minutes ago.

The wraparound was there because we have the means to cover for large perturbations.

Why not implement it?

I mean the situation you always have with human space flight, if there was a capability you can take advantage of in a contingency scenario put it in.

This also changed, though, between the first flight and the twelfth flight.

And the reason we found is that you put this contingency capability in, but when you really study it you realize you can actually take these two fundamentally different control laws and cause them to interact adversely.

We could perturb it and then induce the jets to fire in a way that would cause it to counteract the effect that the thrust vector control system was doing.

So, when we lowered the bandwidth, we also changed some of the parameters in there to, in combination, preclude that first flight.

This is a case where we continued to evaluate the baseline system after we were flying and discovered additional potential unanticipated deficiencies that we should fix, which is saying you're never done analyzing the system even after it starts flying.

The maneuver and track modes, I mentioned that they were there, but we had this universal pointing display that the crew could manipulate.

Yes?

On that last general comment, on the last subject of discovering issues and potential problems after the system is flying.

You're doing the analysis.

You're doing your research.

What, in general, were the reactions of your NASA counterparts when you bring that to their attention?

Would they call for an immediate fix before the next launch?

It depended on the nature of the problem.

And let me mention two or three of them at one time.

I mentioned one about that phenomenology for the excitation or the rocking motion on the tank.

And then another one with the Vernier jets which I will explain in a moment.

The external tank one had to be fixed before a second shuttle flight.

There was one that potentially created a dangerous situation.

Tank separation violated safety of flight rules.

This one was a potential wraparound interaction.

It could only occur if you already had a significant contingency under fairly complex conditions.

And, if the crew knew about it, there was a procedural way to temporarily inhibit the reaction control system interactions stopping the effect.

Because there was a crew workaround, they knew about the problem, it was deemed acceptable to go some number of missions for an already scheduled software update to insert it.

Now, the third problem discovered as a result of analysis of STS-1 and 3 was a plume and pendulum phenomenology of the down firing aft jets.

The body flap sticks out as kind of a random position on orbit, and the down firing thrusters, part of their plume hits it.

They had evaluated that effect for the primary jets because they knew in the direction they pointed and their lower expansion ratio in the Vernier jets there was going to be a problem.

And that was properly dealt with in the flight control system.

They never modeled for the Vernier jets, but only discovered that the state estimator was not converging as well as expected on the first Shuttle flight when using the Vernier jets.

And it turned out there was probably a 20% or 30% net reduction in thrust and a 15 or 20 degree effective change in the direction of the thrusts, those two down firing Verniers.

And the feed forward estimation from the RCS jets, as a result, was giving the wrong data in the state estimator causing a jump in the value and a long time constant to settle out.

And that was causing a few percent increase in the propellant consumption but probably a factor of ten increase in the duty cycles of the jets which was unacceptable from the life of the jets.

That was compounded by a problem in STS-3 which is the first time they used the arm.

And they actually put a few hundred pound payload and tried controlling the attitude of the vehicle in moving that payload.

The combination of those things they went back and, by STS-5, had to make serious changes to the phase plane estimation logic and tables for the accelerations for those Vernier jets because they didn't want to burn those jets.

I think, after STS-2, they actually changed some of the jets.

And then they didn't want to have to change them again.

The maneuver mode.

You want to do various types of [NOISE OBSCURES] maneuvers with respect to various frames of reference which could be landmark tracking, local vertical tracking, second spacecraft if you're doing a rendezvous tracking.

Guidance to provide that.

That would be broken down into components by axis.

And then there was an additional level of hysteresis about what you were telling the face plane to do.

And I talked about adjusting the origin.

This would decide whether or not you would adjust the origin.

If you're error in a given axis with respect to what you wanted to do with the maneuver was less than twice the dead band, you would not adjust the origin.

And if it was more than twice you would.

And, again, it is a case of why force it to do things it doesn't have to do if it's going to get there eventually anyway?

And that is actually an adjustable parameter which, for certain payload missions, they might change that value from something else.

There were these various direct manual translation rotation modes and the auto modes that I think bit by bit I have talked about.

The reason you have these different references, inertial and local vertical, if you're doing an earth observation

mission, almost everything is going to be in a local vertical frame.

You're going to have your payload bay pointing down.

You want to keep it pointed at a certain spot.

If you're doing a solar telescope mission, everything is going to be in an inertial frame.

You're going to want to keep it pointing at the sun or within a few degrees where maybe the telescope will have a limited travel of its own.

If you're doing rendezvous then it's going to have to be you're accounting for the orb rates of the two vehicles.

You're going to want to keep your rendezvous radar pointed in the right direction.

By the way, the rendezvous radar, there is a deployable dish antenna that goes out of the payload bay, the side of the payload bay of the Shuttle.

That is a dual-purpose antenna.

It can be used to point at the TDRS satellite to send data at high rates to the earth and track the satellite.

Or it can be used to point a radar beam at another spacecraft.

It was not used for TDRS in the beginning of the program.

It was only used for radar because the first TDRS was launched by STS-6.

Electronic string, and I think we're about at the right point of time on this, too, to allowing me to get into this in a little bit of detail.

This was something that kind of crept up on us in importance.

It was thought it would make the systems redundant, have separate strings, don't put them all on the same computer.

All those things were recognized, but I don't think until about a year, a year and half before the first flight actually occurred that we realized how difficult it is to be sure that all the interactions of these strings, the power string, the plumbing string and the electronic string and the possible combinations of failures, how difficult it is to assure that you meet those high level failure tolerance requirements.

And that is what I think I did in 1980, '81, probably was the early form of fault tree analysis.

And I have in a handbook I developed for the first flight, a series what if tables with all these different breakdowns of what could happen.

And actually a person that didn't know about probabilities and all looked at it.

It was a pretty scary table when you looked at all the possible bizarre two failure combinations.

But first you've got to understand what the strings are.

You would have one forward, one aft left, one aft right, so three boxes, three half boxes and multiplexers-demultiplexers on a string.

And there were two MDM boxes in each pod, forward left right aft.

And the electronics were broken apart into each half box.

So you actually had, in effect, four sets of electronics in each pod, even though you only had two boxes.

And one card from each of those boxes would be dedicated to string, but each string would have a card per pod.

So three cards would be tied electronically to one computer anomaly.

Now, you couldn't take a string that could be commanded by more than one computer.

The computer saw the data from all four strings so they could vote the data to decide whether or not each of the computers was healthy, but they could only command one string.

I should say each string could only be commanded by one computer, but you could, if you started losing computers, latch up more than one string to one computer.

Even though one string could only take commands from one computer, more than one string could take commands from the same computer if that became necessary.

If you lost a computer and were in a benign environment and you wanted to recover all those systems, that happened with the first computer failure in STS-9, then you would manually re-latch those strings to a healthy computer.

Of course, if that computer went down then it would take two strings down.

There was a unique latch up of these string components to power systems, but it wasn't necessarily one-to-one.

And that is where things got very complicated, when you start crossing the subsystems where one power system could cause some subsystems to fail on more than one string.

Then you take a string down.

That would be a very different failure scenario than taking two strings down.

This is showing how the thrusters laid out.

You can see there are a lot of thrusters on each string.

If you go back and look at the vehicle carefully and you look at the down firing thrusters, you will see that in the front of the tank there are two thrusters that point down to the left and two thrusters that point down to the right candid out about 40 degrees.

That means that if you lose two thrusters, two strings or two manifolds it was possible to lose both of them on one side.

That is very important because that's one of the phenomena we had to protect against for separating from the external tank.

And it becomes a highly coupled separation maneuver.

And there were some special jet select tables created for that and some special control logic loops that were created just for that one scenario.

You go through these things and certain critical events where things cannot fail even if your subsystems have failed twice.

And the subsystems may not have been designed to make it very convenient, but you still have to do it.

That happens to be one of the scenarios we looked at a lot.

And that we see forward down left down left or forward down right down right.

So somehow you lose the thrusters, these strings or whatever.

That became a special design case.

And there were a lot of those kinds of things.

I would say 70% or 80% of our design time goes into learning those special cases.

With the thrusters the manifolds are basically the valve lines, so there is a commonality between the electronic stringing of manifolds in those valves.

With the OMS that's not really true.

The way the OMS engines work, each engine [NOISE OBSCURES] is actually an oxidizer and fuel tank going into two loops of lines each with two valves.

At least one valve in each path had to open to feed fuel.

At least both valves in one loop had to close to stop fuel from flowing.

Any combination which would leave two open after a burn started or would leave two closed before the burn started was a problem.

Then you have pressure sensors.

And there was only one per engine.

You lacked insight into whether or not the engine started based on pressure if one of those failed.

The stringing of this was not the same as the electronic string, so we had to start looking at the possibility of individual valve failures and electronic string failures.

Taking down other valves.

Did that happen before an engine started, after an engine started?

How did that correlate with then influence on the same engine's actuator control?

We could get situations where we could start the engine but we couldn't steer it, engines that we could steer but couldn't start it, and so we ended up with this maze of tables looking at those situations coming up with contingency designs.

Sometimes reverting to using the XRCS jets under severe multiple failure scenarios that actually do deorbit burns.

We talked about what could go down.

All of these things could be lost with a single failure, though not all strings have an IMU because there are only three.

And only two of the chamber pressure.

Some strings were more important than others with respect to a subset of the systems.

And since there are only two thrusters on one manifold per pod of the Verniers, there are also only three strings that affected those.

All this got set up so that any one failure was quite manageable, but the moment you talked about any possible two failures was when it became much more complicated.

Generally, where we ended up, after lots and lots of special design accommodation was we tolerated loss of translation control in the axes that were not necessary for managing deorbit.

We tolerated degradation and rotation control but assured that we retained it, at least in a time average sense, in all three axes.

The biggest complexity here was assuring we still had adequate time averaged translation and rotation control for tank separation.

So we would pull away without recontacting the tank.

Remember, recontacting the tank meant tiles hitting the tank.

Those tiles are really fragile.

They can survive thousands of degrees but not much impact.

We accommodated the scenario where we could lose all thrust vector control on the OMS engines and still do a deorbit burn usually with RCS wraparound properly designed.

And we had to accommodate the situations where MDMs did not reset, so everything tied to an MDM would be lost.

And that is the kind of situation where you start having valve here, a valve here, a valve there being shut down along with a bunch of jets.

And the real pain was understanding what things could collectively go down together.

You had to lay out all the faults, all the things that could happen with each of the faults and then overlaying the combinations of those.

And then you would find it wasn't everything you were worried about.

It was usually a small fraction, but those few fractions drove the design details and effort to a great degree.

Now, on orbit, because you would often be using one IMU and you only had two computers, one of those strings going down meant you lost your navigation base.

But because you're in a relatively benign environment, restringing and bringing up another system wasn't a problem.

If you were doing terminal rendezvous with the Space Station, you would not be in a one IMU mode.

You would be in a three IMU mode on two computers, but you would not lose your navigation base.

If you lost a computer at a critical point in that, you would probably abort the rendezvous, reconfigure again and resume your operations.

One of the ground rules for all rendezvous operations with the Shuttle, and I think will be true of the CVE is an rendezvous operation planned to do has to be able to be repeated at least once.

The way I want to end this, and then we could have questions, is two pictures, before and after cockpit upgrade on the Shuttle.

This was the way the Shuttle was for many flights.

Those are CRT displays, green monochrome where no images could be drawn except little sticks, dots and lines and rudimentary.

These are analog tape measures, analog eight ball with analog needles for attitude and rate information.

And really very 1970s.

Comment on that.

One of the things that we did as payload specialists is we got some training in the cockpit, and that was the version that was available in the early '90s when I was down there.

And you would go from your desk at the Johnson Space Center when you were using an IBM Think Pad or

something, and you felt as though you had gone through a time warp when you went back to the simulator on what was the world's most expensive vehicle.

It was extraordinary.

And, of course, you could explain why this was kept on so long.

Well, it was this multi seven digit figure for its upgrade, as well as the issue about recertification.

And let me mention both of those in a moment, point out a couple of things and get back to that before I show you the current configuration.

[AUDIENCE QUESTION] The amount in the Shuttle versus the amount to support the Shuttle?

In the Shuttle because [NOISE OBSCURES].

Well, you only have a 104k memory computer.

You have the actual number of lines that are [NOISE OBSCURES].

Yeah, you had the 104k for the backup system, the 104k for ascent and entry, the 104k for on-orbit, the 104k for system management.

And then there have been other things where their own software capabilities have been added in subsequent years.

So it is a lot of software now, but human validation means if you make small change everything has to be reassessed for possible interaction to a degree that you would never do for a mission that doesn't put human safety at risk.

That means the cost of doing that each time is probably an order of magnitude higher than it would be for an unmanned system.

You look at what it was going to take to put a cockpit upgrade in there.

We're talking hundreds of millions of dollars to do it for the fleet.

And when I say hundreds of millions, a couple hundred million.

It did eventually get done, as I will show you in the next picture, but the main reason was obsolescence rather than wanting to be contemporary.

You cannot buy these pieces to replace them anymore.

The companies that actually made some of these systems may not exist.

Or, if they do, they have no economic incentive for maintaining the base for a customer that may buy another five of them.

And so, one of the things you have to deal with when a system is going to do this many years, another example of that is the B-52 or the Triton missiles or things that stay in operation for a long time, is you have to plan, as part of your operation cost, for periodic upgrades to mitigate obsolescence.

[AUDIENCE QUESTION] In some program they had some support.

It was Digital microcomputers.

We had a room over in the Hill building that had about 100 of them stacked up as backups.

I don't think the boxes ever got opened.

I think the program did the buy, but the program never lasted as long as it was supposed to.

But you are right.

You can try to buy it.

But, even so, even unused systems had a shelf life.

And you don't know how good they are going to be 30 years later.

If you had asked me in 1978 how long the Shuttle was going to fly before it was replaced, I would have said ten years, maybe 15.

Before the Columbia accident they were talking about another 20.

It is only the safety issues now that are going to make them stop it soon.

Anyway, the other thing I want to point out here, this is the crew interaction mechanism, a push button display.

No such thing as GUI.

That is unheard of in the Shuttle.

Can you talk a bit about the hand controllers?

Are they the same ones used for landings that are also used for docking?

I mean was it the same hand controller for everything?

It is the same hand controller for everything, except there is another station in the back, I didn't bring a picture of it, which is used for docking.

The cockpit, you're looking out the forward windows, you turn around and there is another set of cockpit instrumentation, hand controllers.

And there are two windows above you and two windows looking on the payload bay.

And there are also controllers there for the arm.

Everything related to the arm is done looking out toward the payload bay.

The arm is attached there.

When you are doing rendezvous you're looking out at the overhead windows of the vehicle you are approaching.

So, in effect, you have a couple of these CRT displays and identical hand controller and the equivalent then or the updated equivalent now of these displays on a back station.

To avoid any issues of changing controllers and changing viewpoints, you might note that normally the controls that are done out of the back window with that separate controller and separate displays are done by different crew members.

That is typically a mission specialist's job, not a pilot or commander job, and so they are separately trained.

Right.

That's an important point.

For rendezvous and docking, it is the pilot or commander who uses the aft controls to control [NOISE OBSCURES].

Do you know?

I believe that everything related to the RMS that you said is correct.

But for a rendezvous the commander is always involved.

But the point was that in that case that is done out the rear window.

It is still done at the rear window, so he has got to mentally reverse his frame of reference while he is doing that.

That is correct.

[NOISE OBSCURES] And that is something that I think will not be done with the CEV.

The same frame of reference will be used on the CEV because I think that has always been a little bit of a point of contention in the problems of maintaining simultaneous proficiency.

For remote manipulation with the arm that has been an issue.

Yeah.

And I think that has always been done by uniquely trained mission specialists.

That's right.

Today's cockpit looks a lot more like what you will see on a commercial airliner vintage mid `80s, the late `80s perhaps, but still more familiar where you've got glass multicolored displays.

The eight ball still exists in image form because that is what a lot of the astronauts used to learn how to fly these vehicles.

They still fly with respect to it, except it is a digital representation, but you're still not with the gooey environment.

You still won't have touch pads or a mouse.

It is all pushbutton displays.

And there is a case to be made that touch displays or touch screens don't work very well in a vehicle where you G environments keep changing.

It is very difficult to get a touch display that works with a light touch and a heavy touch when you're in zero G or when you're pulling several Gs.

Even if the technology was space qualified, it is not clear that they would use it, except on a vehicle that stays in a constant environment.

At this point, let me introduce Dr. Hayashi.

Miwa Hayashi is, in fact, at NASA Ames Research Center now, was here at MIT and worked on the design of the next generation of the Shuttle cockpit upgrade.

In fact, that is what you will be talking about in ten minutes across the hall in the 16.400 class.

It is essentially what would have been done if Shuttle life had been extended.

I might add that, although the room is very crowded, if a few of you would like to sort of hear where this story would have gone, you're welcome to come across the hall to 419 and hear Dr. Hayashi.

And you are also giving a lab meeting lecture at 1:00.

Could you tell us that subject?

That is about the astronaut scanning behavior.

Our team had a model about the astronaut's scanning behavior in the cockpit, this upgraded cockpit.

Anyone interested in this kind of topic you are welcome.

It is from 1:00 PM 33206.

Thank you.

Go ahead, Phil.

Well, at this point, I think I'm open to a few more questions.

We have a couple of minutes for further questions, any topic we've covered or that's related that we didn't cover.

Yeah?

You talked a lot about the constraints of the invented computers.

[AUDIENCE QUESTION] Well, we had very large facilities for that purpose that evolved over time.

The first major facility was the Flight Simulation Laboratory in Downey, California, which was then Rockwell.

You had a room with a couple cockpits, you had another room which had the digital interfaces of the cockpit, and a half a floor with the analog computers that provided a lot of the information generation at a rate that was not

achievable with digital systems.

You had this hybrid system for driving what were man-in-the-loop simulations.

And we spent 24 hours a day, 7 days a week using those labs for several years.

I would often go out to California and be on the 5:00 PM to 5:00 AM shift often spanning weekends.

By the way, I was doing that, I think, when I was still a graduate student, which was kind of an interesting experience.

But then NASA built the Shuttle Avionics Integration Laboratory in Houston which eventually superseded the laboratory at Rockwell.

That became an all-digital system.

The hybrid systems went away.

The high capacity computers, they could fit in one good size room everything they needed, and were able to get much more digital displays for the crews.

Sometimes what they used to do for the imagery of the crew in the early days is they would actually drive a camera across a simulated scene because you couldn't generate the scene.

By the time they got the sail facility developed they were able to do scene generation with fairly high computers.

Now everything could almost be tabletop.

I mean it is just so dramatic as how this evolved over the years.

The one thing they had at Rockwell that never got replaced, though, is they also were able to put into the loop actual hydraulic systems.

When they were doing entry they could turn on aero surfaces and hydraulics with simulated loads.

And you always knew when they were doing it because the high pitch scream of the APUs, when they were doing it, you could hear two blocks away.

OK.

Last question.

Sir, I was wondering if you could give kind of a concept of the cost of developing the software either in man hours or in comparison of what they spent on the hardware.

Well, the initial development of the system probably involved the equivalent of 15 or 20 full time people for a few years.

And this was to develop the algorithms and support the validation.

The actual flight software was actually produced by IBM separately.

And they had a small team of people that would take the detail design specifications and create the software.

It is a big effort but a very small part of the cost of developing a Shuttle.

I mean you measure the Shuttle in billions.

You measure the flight software development in millions.

One thing that I remember when the software was developed and we were working and validating it, IBM wanted every line of code change in million dollars.

A million dollars for one line of code change because they had to verify the whole software.

That is why you would never, unless there was a flight critical thing, do that.

NASA wanted generally, whenever possible, to aggregate changes for a year or maybe two years sometimes.

And then put them in there just for that reason because there was this huge cost of revalidating.

And that was the IBM cost.

It would be a cost to bringing us back in to certify that, too.

Well, it worked and you should be very proud of it, you and your colleagues.

Thank you very much, Phil.

Thank you.

[APPLAUSE]