

Safety and Space Shuttle



Sandia
National
Laboratories





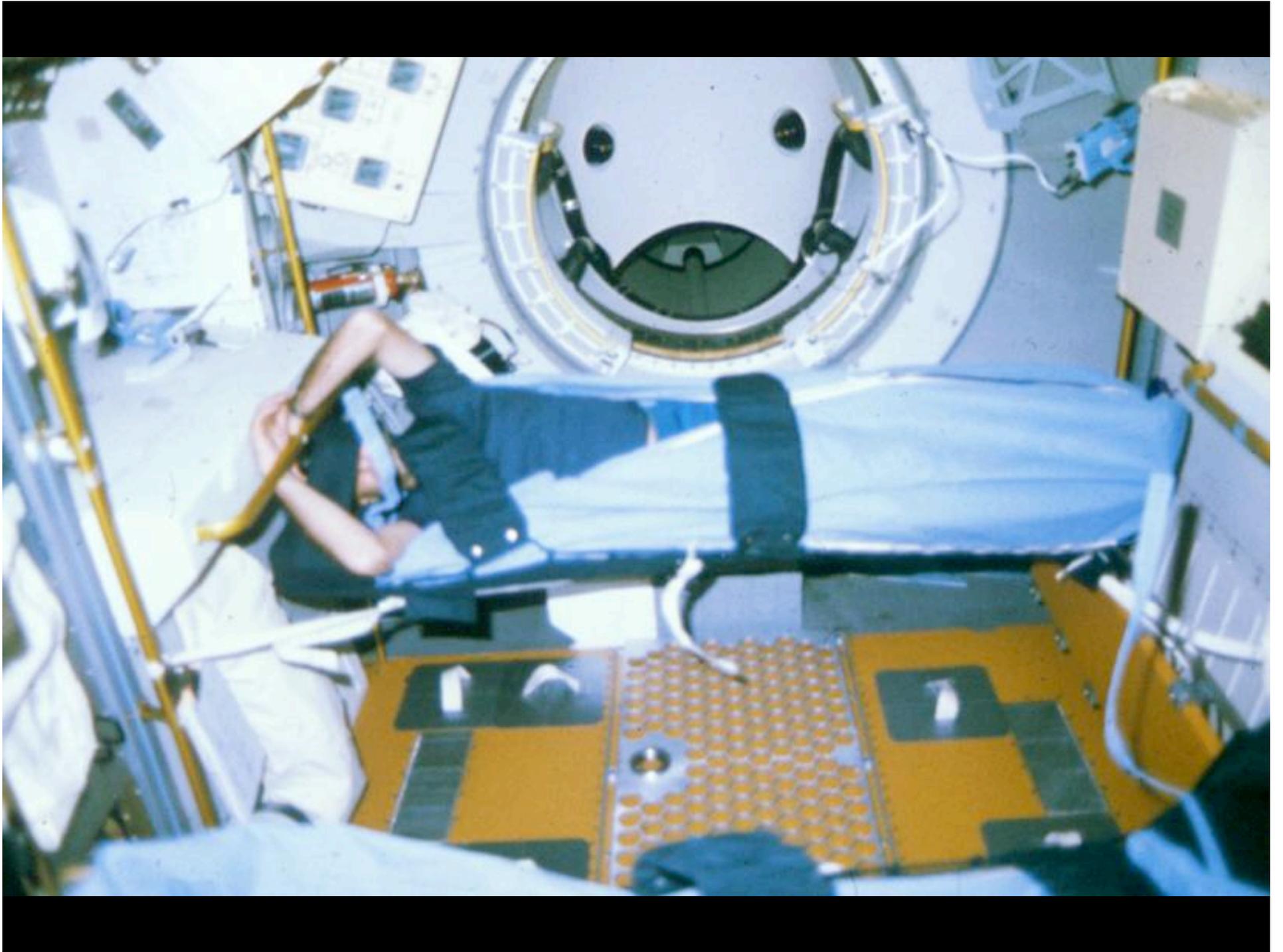




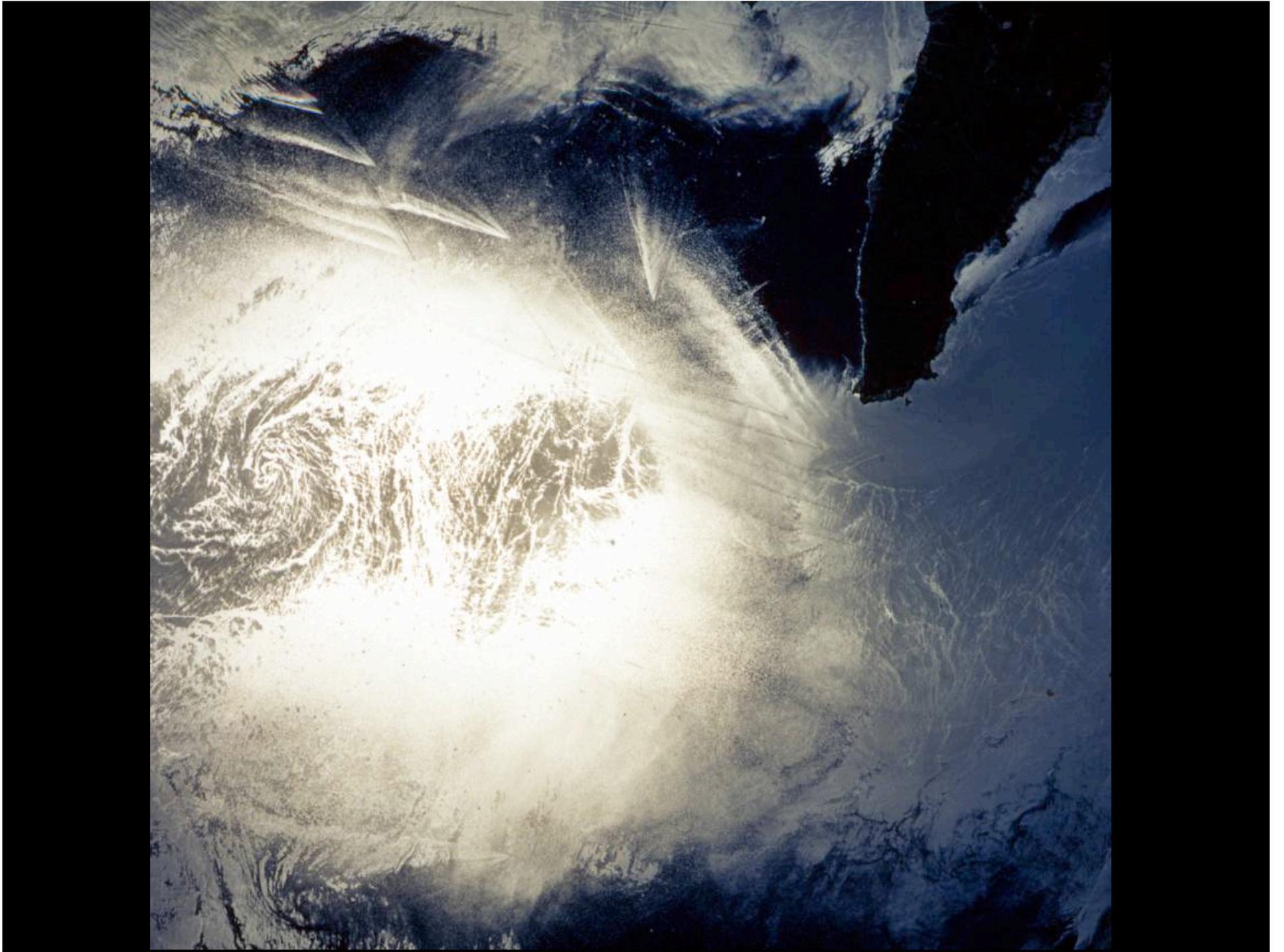


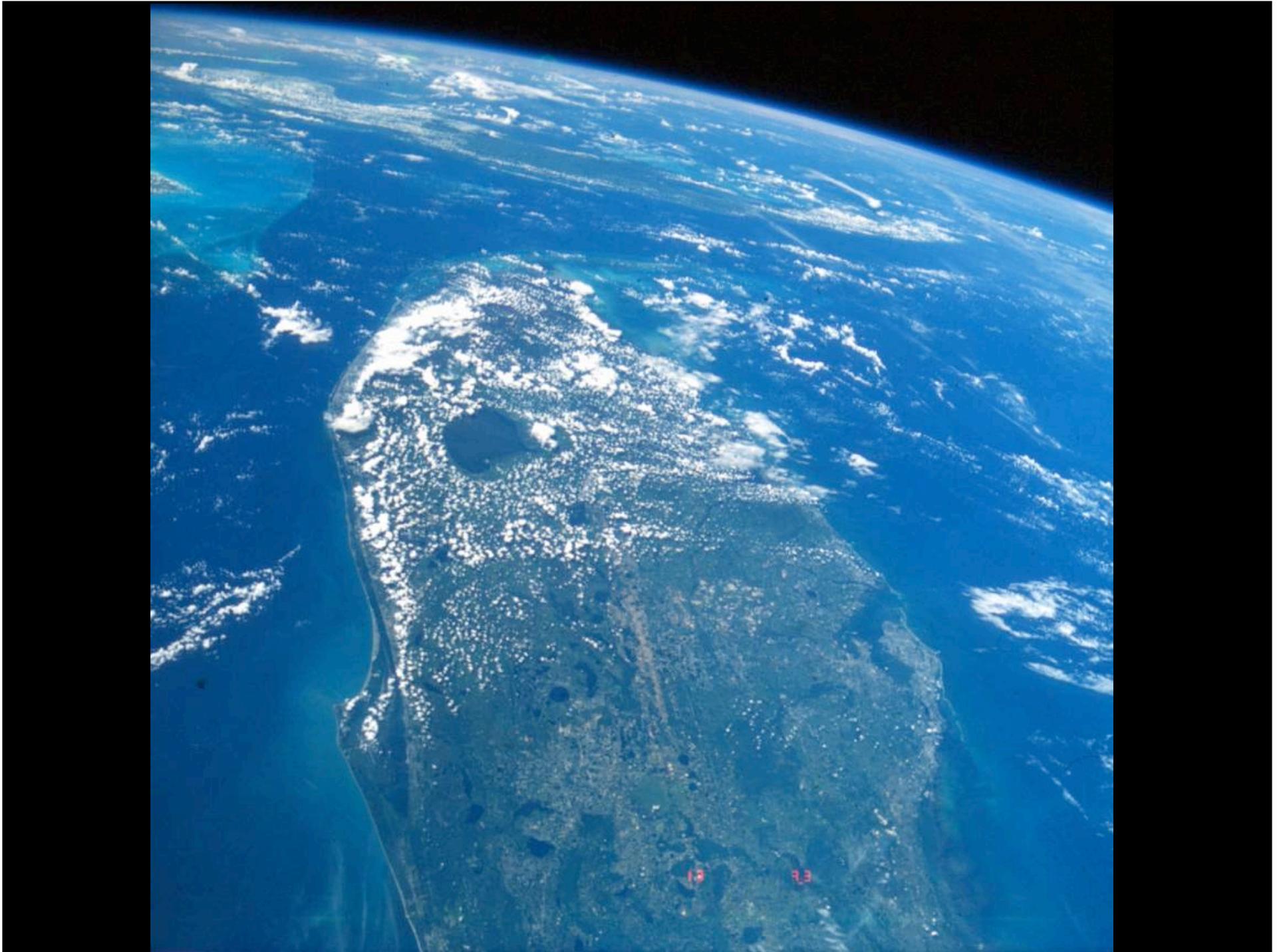




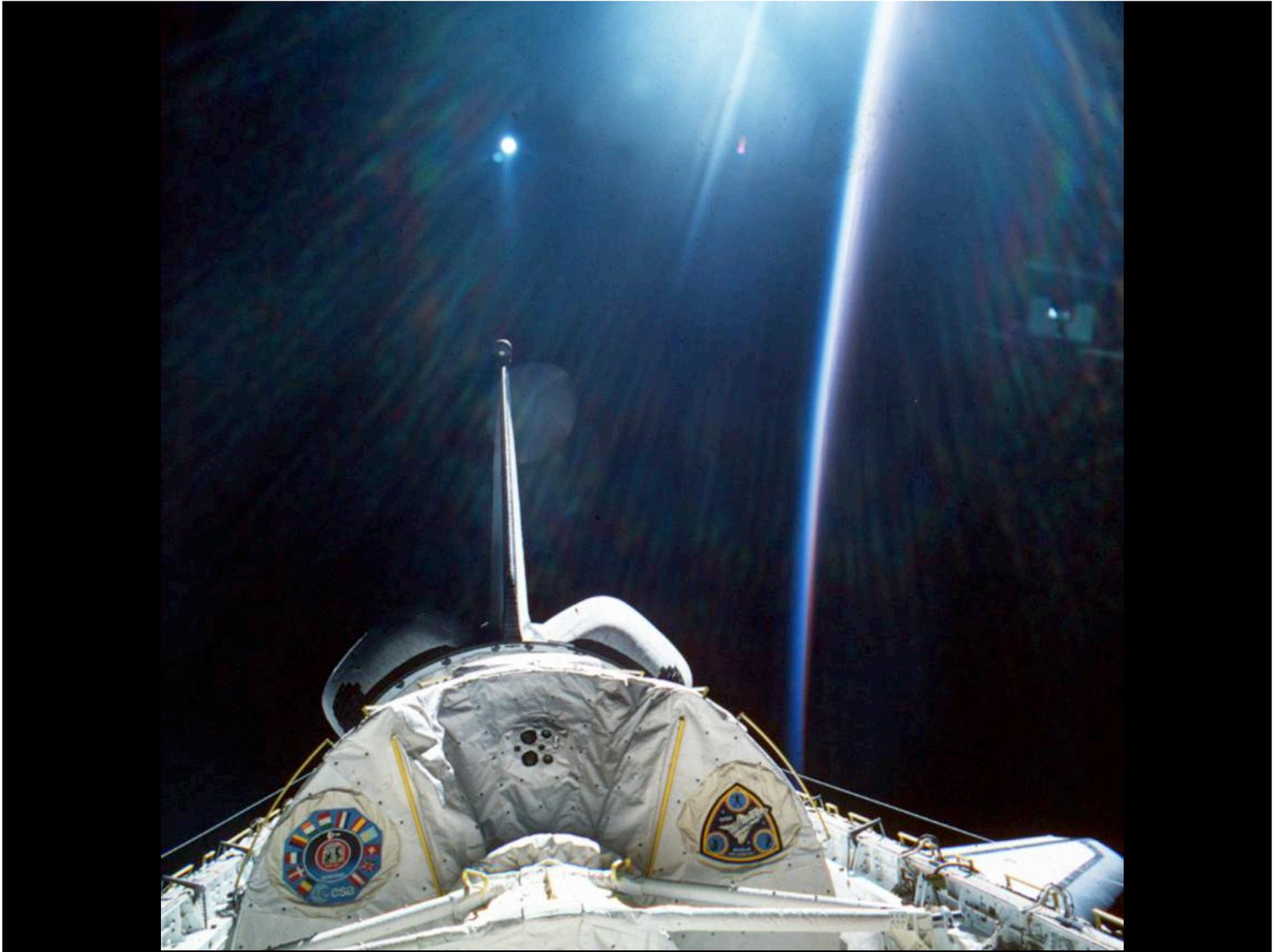










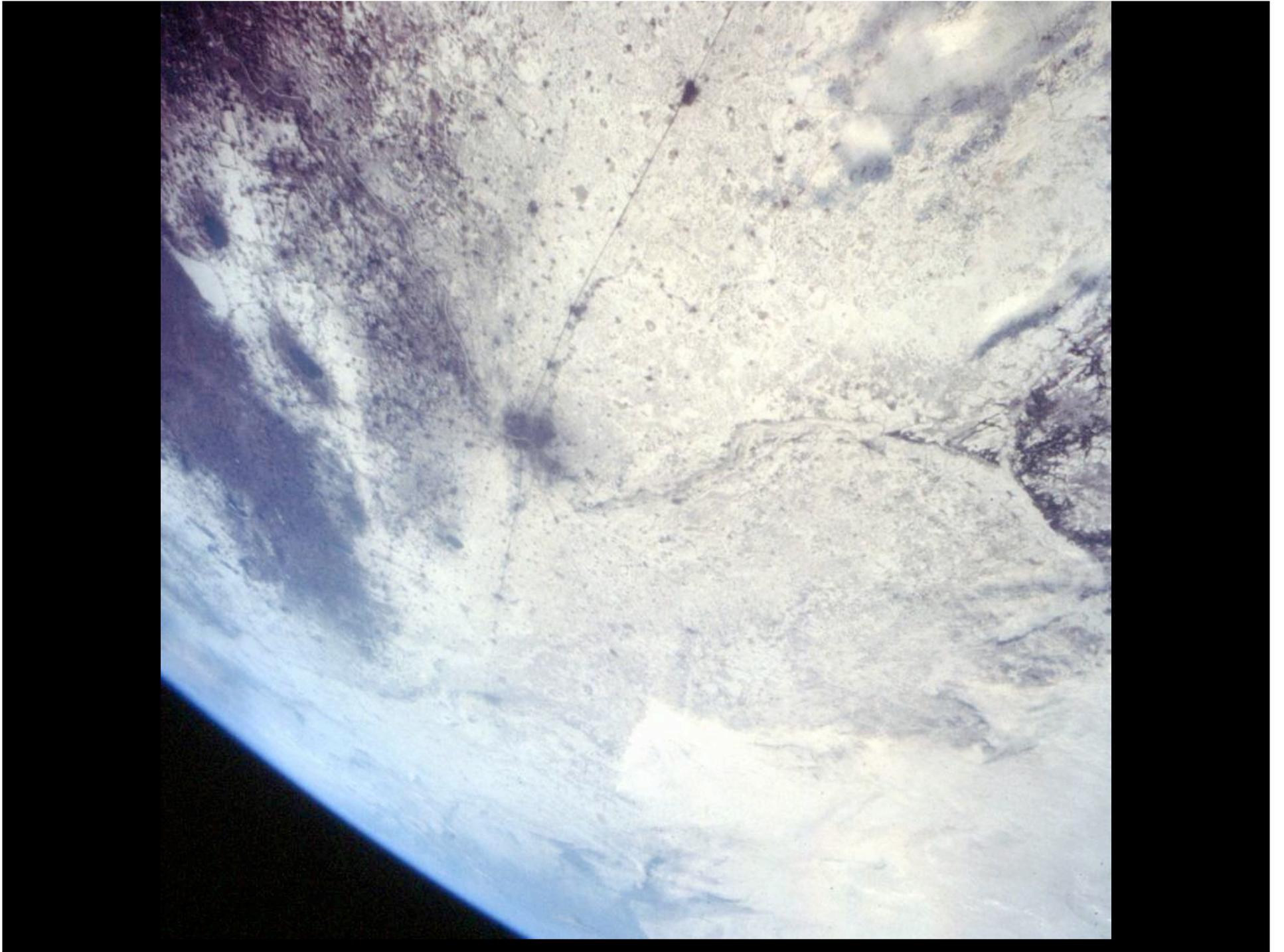


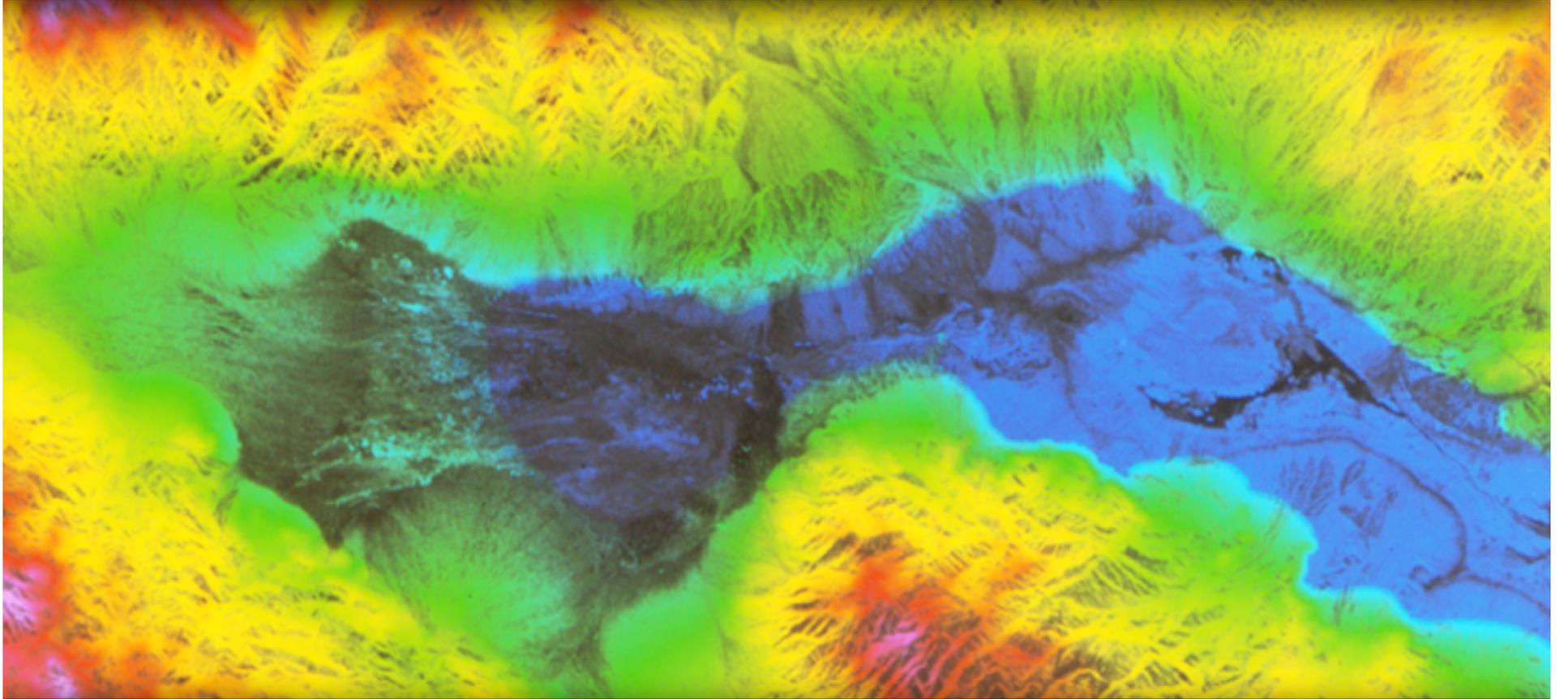




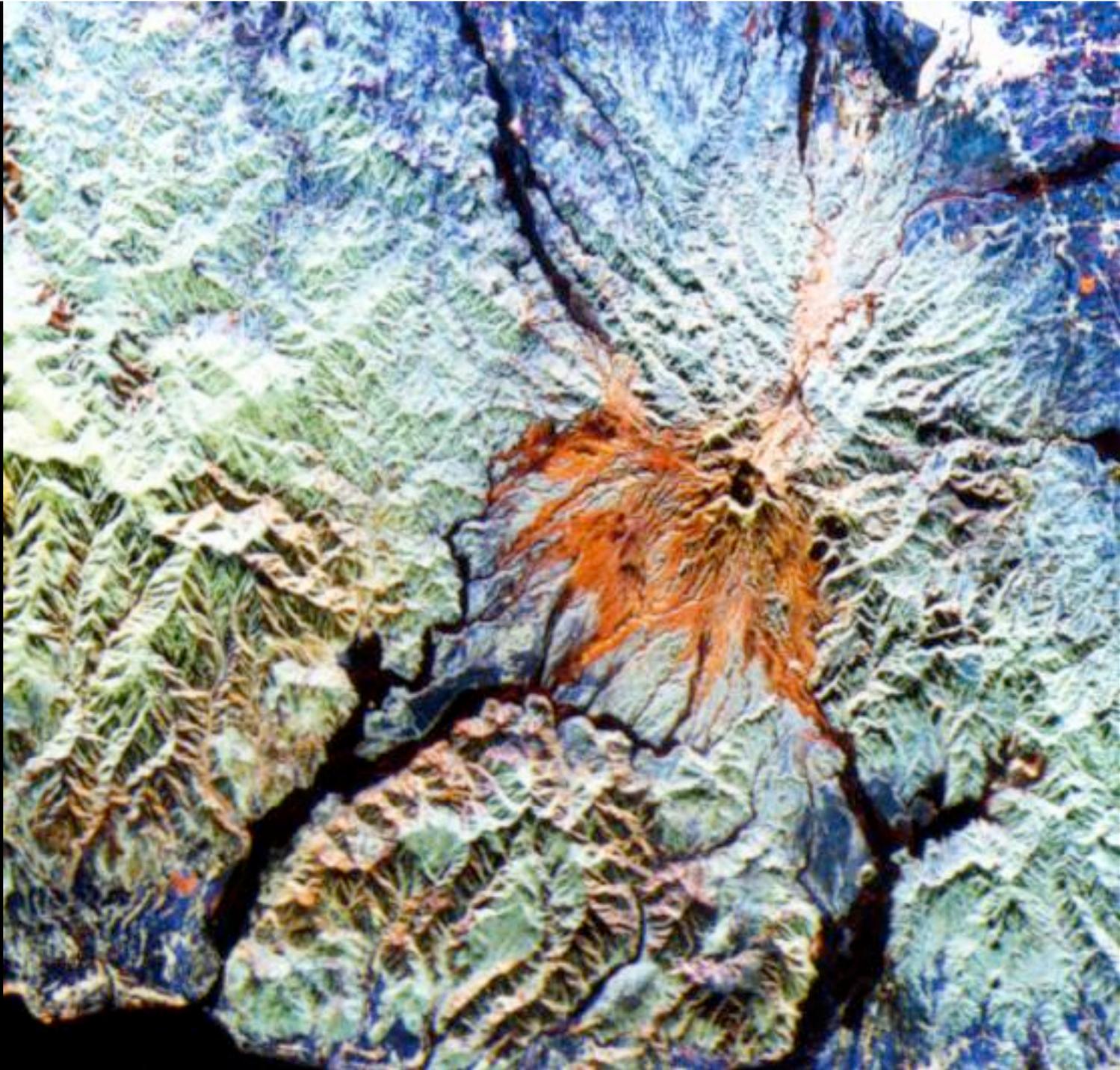


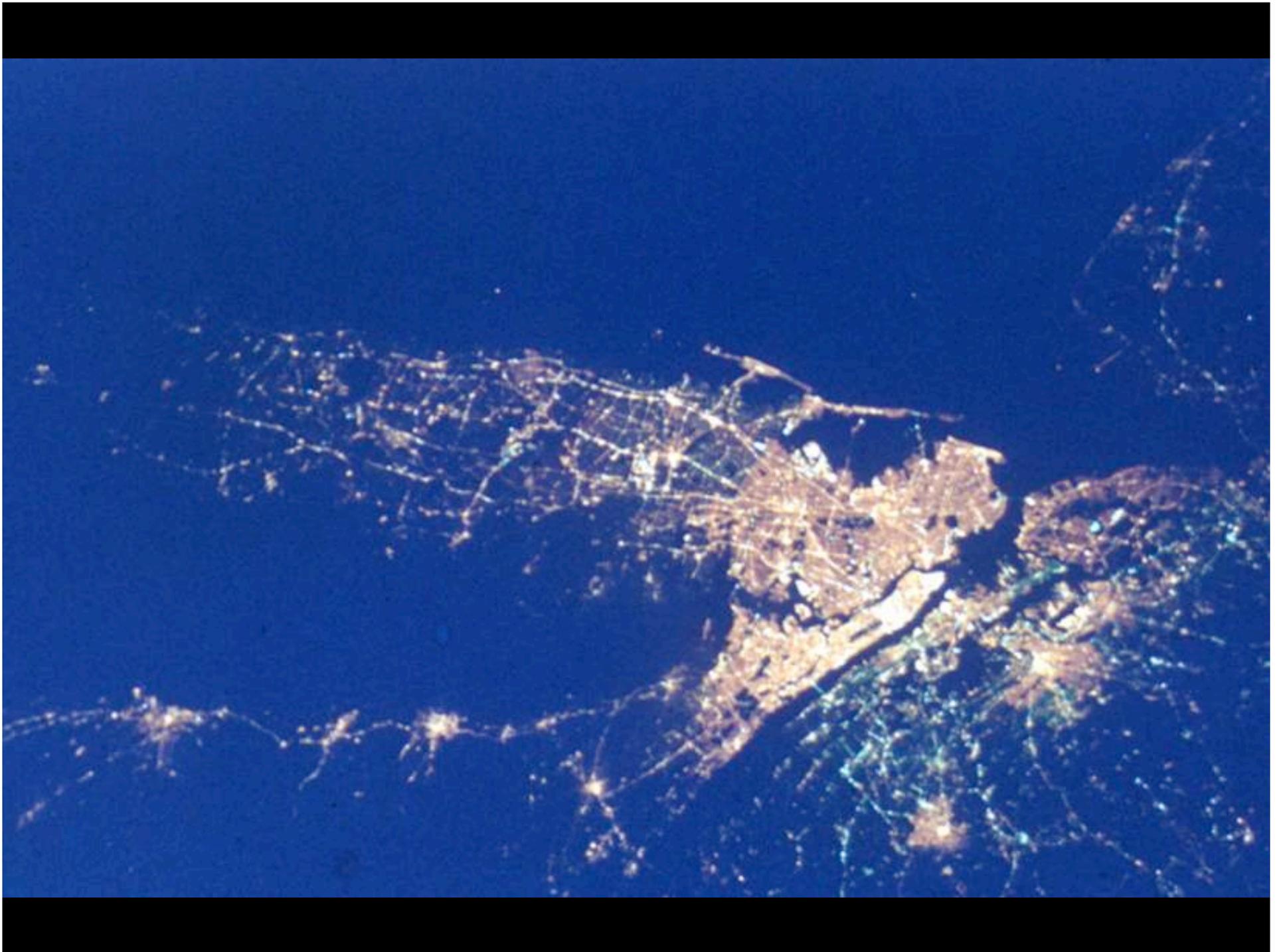


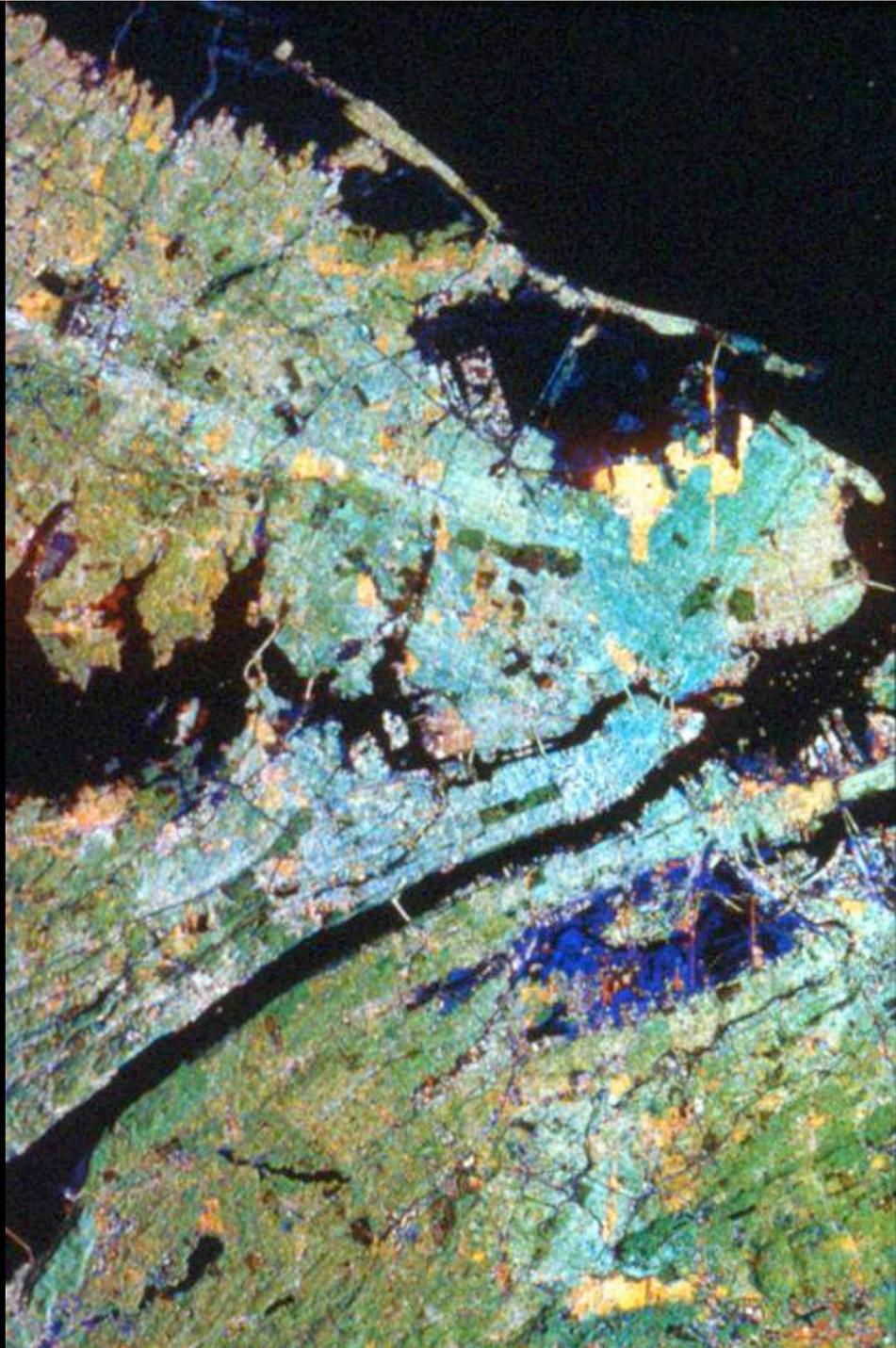






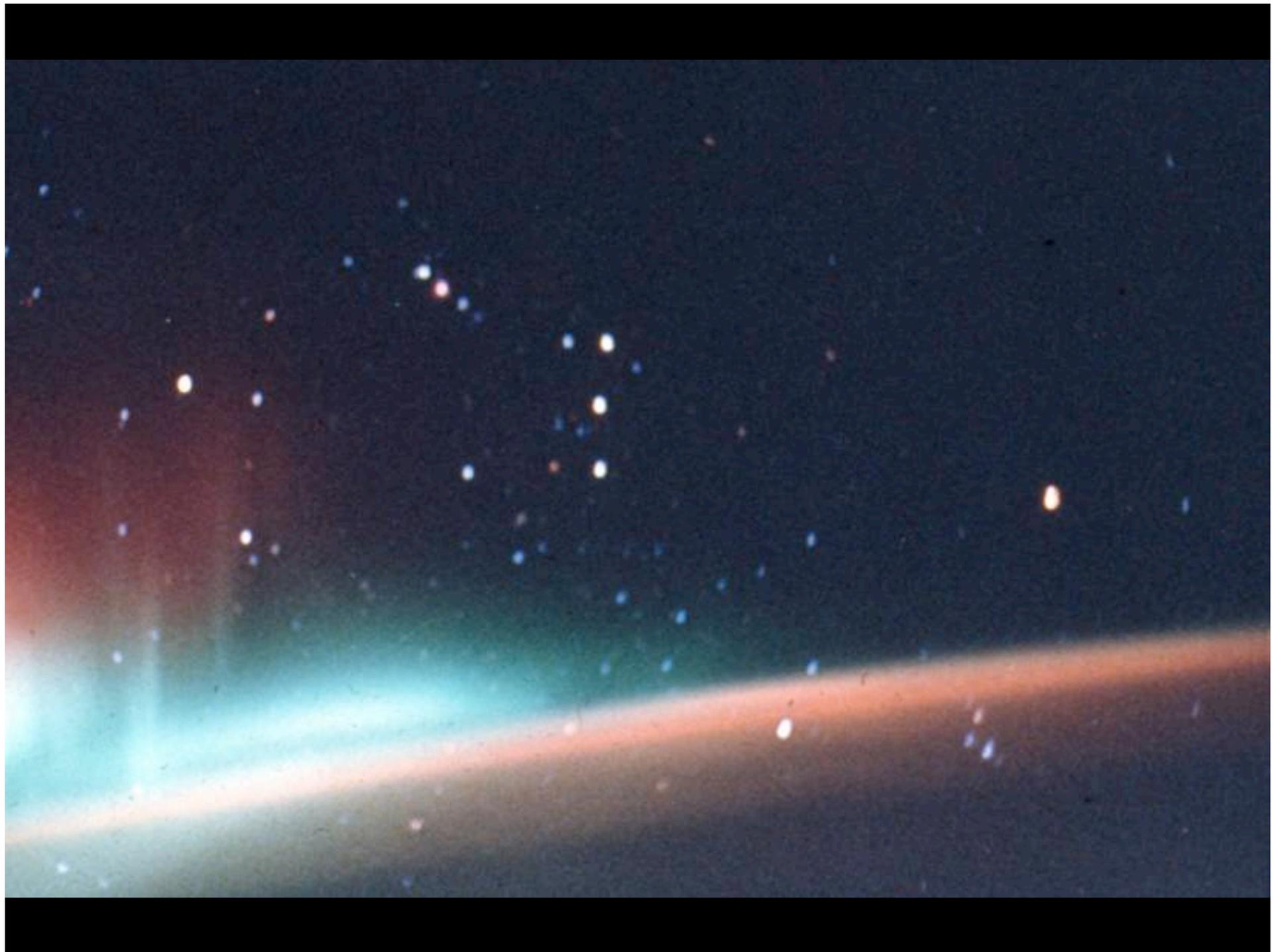


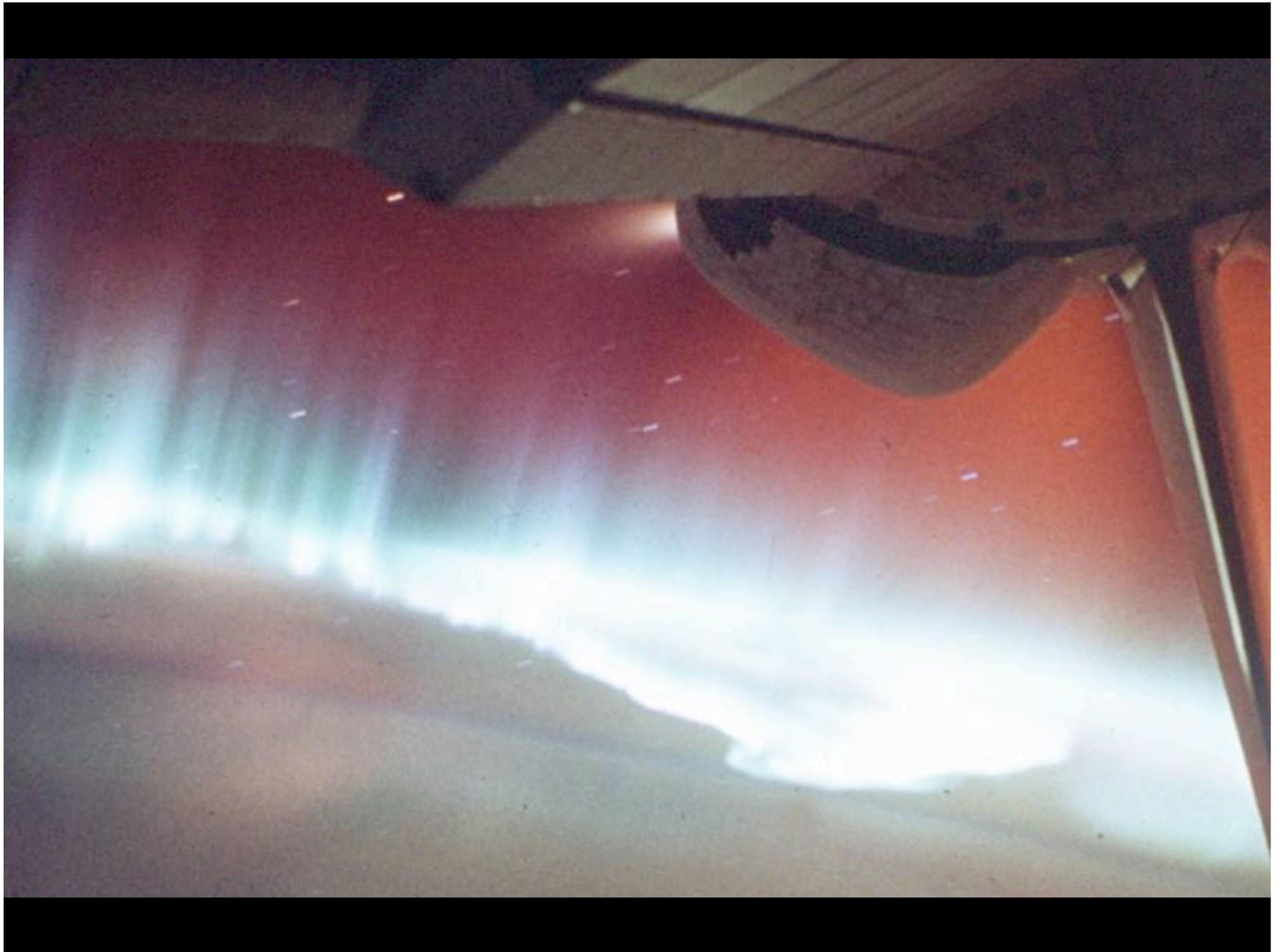
















Exceptional service in the national interest



Thoughts on the Shuttle Accidents

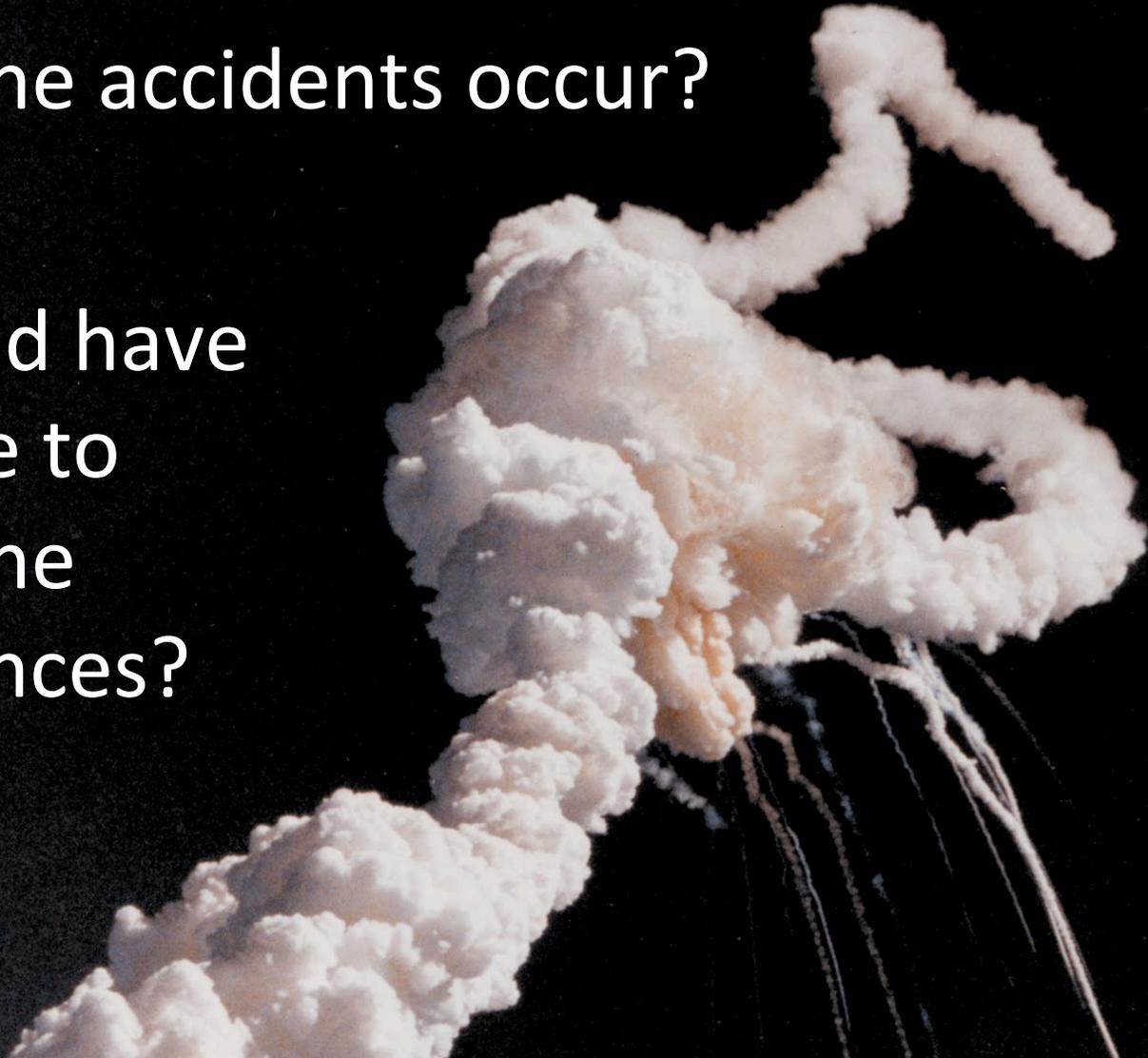
Sidney M. Gutierrez



Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

My Reflections / My Opinions

- Why did the accidents occur?
- What could have been done to mitigate the consequences?



Why Did the Accidents Occur?

- Rooted in the Apollo Culture
- Culture born of success
 - Great scientific and engineering achievement
- One of the two greatest engineering achievements of the 20th century



“This nation should commit itself to achieving the goal, before this decade is out, of landing a man on the moon and returning him safely to the earth.”

—President Kennedy, May 25, 1961

Project Management on a Grand Scale

Performance—Defined
“Men to Moon and Safely Back”



Schedule—Defined
“Before the Russians”

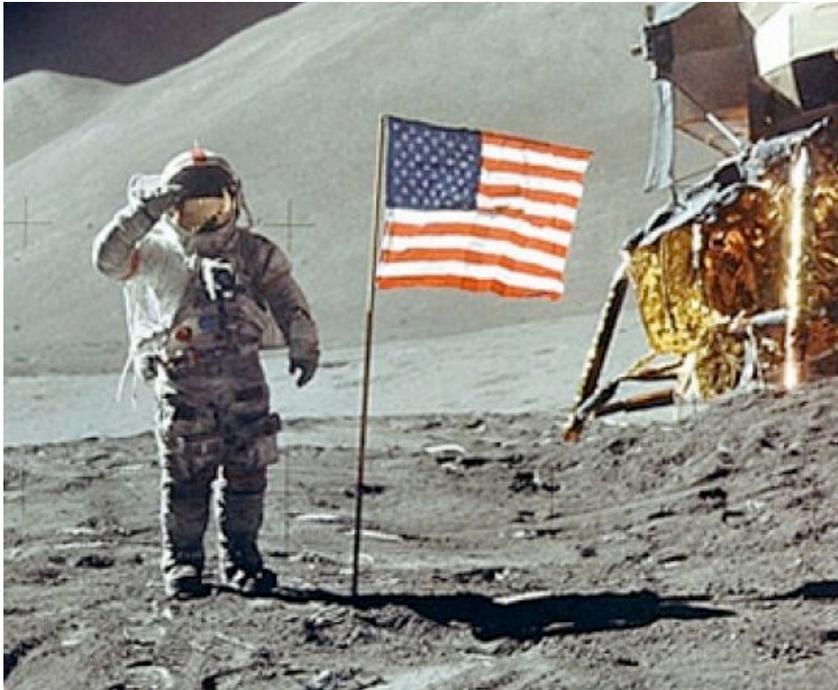
Cost—Essentially Unconstrained
“Billions and Billions”

Cost/Resources—Not a Constraint

- If unsure of estimate, double it and then double it again
- If undecided about best of two approaches:
 - Do them both
 - Liquid first stage
 - Solid first stage
- Safety—Do it as well as possible
 - Failure Modes and Effects Analysis
 - Drive number of Critical Items as close to zero as possible—Regardless of probability



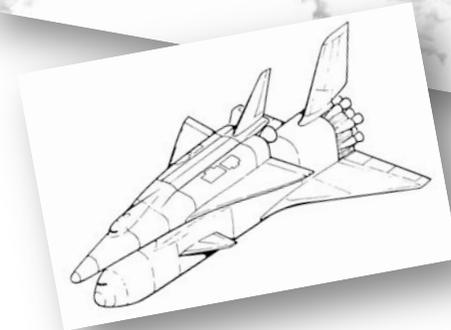
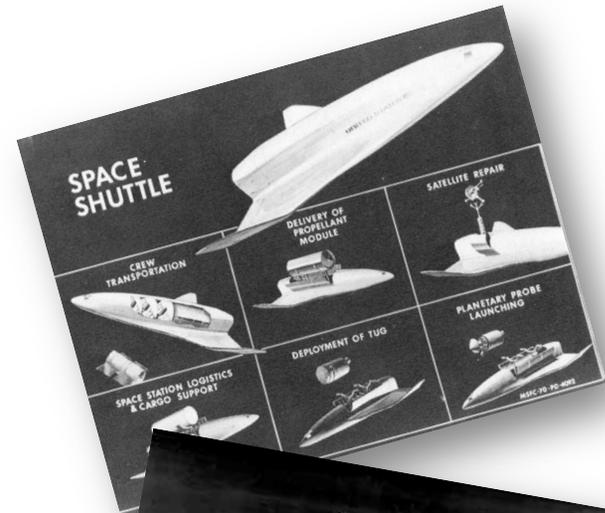
Result—Success



- Reinforced the Culture
- Culture—Achieve safety by doing things as well as you possibly can
- ***Excellence in all you do***
- Possible because of essentially unlimited resources/budget

Next Project – Shuttle

- Designed under severe financial constraints as President Nixon balanced the budget
- If two solutions, discard both and proceed with lower cost approach
- Pursue optimistic design, if testing discredits design, proceed anyway—no resources to redesign
- Explain failures as “anomalies”—
If you are tracking it and it has been signed off, you are OK



What Was Actually Happening?

Rather than designing safety in through sound approaches...

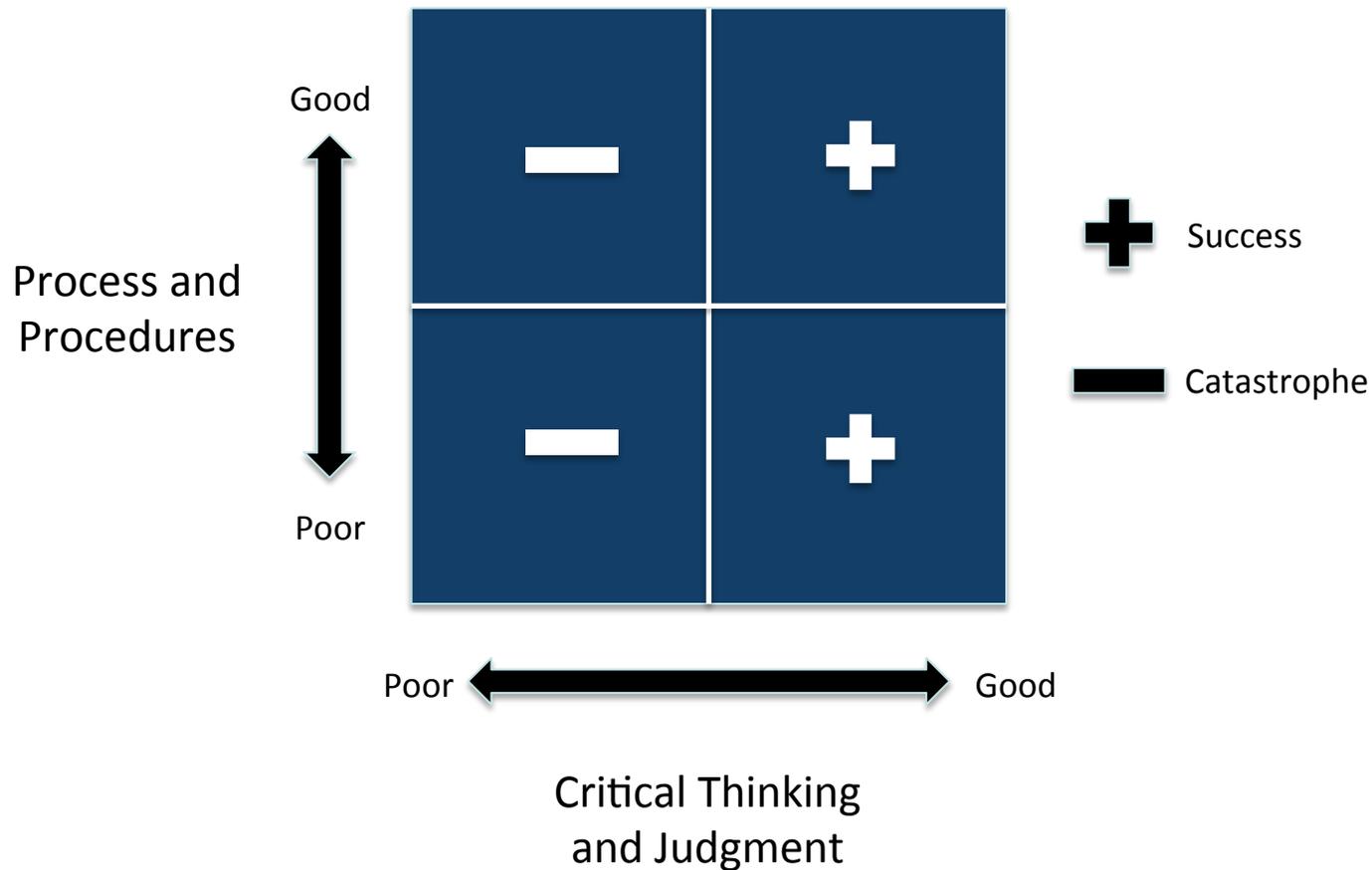
- Safety was assumed based on culture of “Do everything as well as you possibly can”
- But limited resources meant that was not happening—failures were not being fixed/resolved, only tracked and signed-off
- Living in denial
- NNSA stated probability of loss of Space Shuttle was 1/10,000
- Air Force calculated probability of loss of Space Shuttle as 1/25
- Challenger lost on 25th Mission

Processes and Procedures to Assure Safety

- Both critical failures that caused the “accidents” were identified in general terms during development and flight
- Both were identified specifically on each mission prior to the catastrophic events
- After identifying the issues, both underwent extensive reviews
- However
 - Challenger was cleared for takeoff
 - Columbia was cleared for reentry
- Intelligent, dedicated people

Why Did the Processes and Procedures With All the Right Data Fail?

Sid's Matrix



Sid's Axiom

- “The best processes and procedures can always be overcome by lack of thinking and poor judgment”
 - Corollary #1
 - “Processes and procedures will not save you”
 - Corollary #2
 - “It's the decision, stupid”



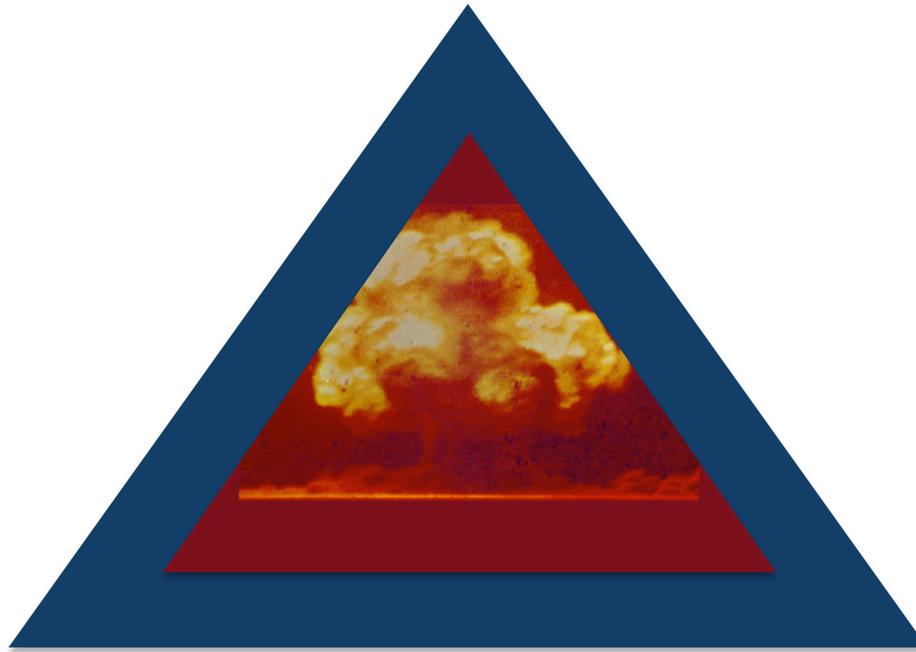
Lest You Feel Comfortable

- The Manhattan Culture—DOE/NNSA
- Culture born of success
- Second of two greatest engineering achievements of the 20th century
- “Build an atomic bomb before the Germans or the Japanese”



Project Management on a Grand Scale

Performance—Defined
“Build a deliverable atomic bomb”



Schedule—Defined
*“Before the Germans or
Japanese”*

Cost—Essentially Unconstrained
*“Was General Groves ever
limited by funding?”*

Cost Not a Constraint

- If undecided about approach, do them both:
 - Plutonium and Uranium
- Performance / Safety—do it as well as possible
- Make it reliable to 6 nines
 - Make failure essentially impossible
- **Excellence in all you do**
- Possible because of budgets



Today

- Budgets limited—severe financial constraints
- Maintaining old complex systems built under concept of doing everything with excellence
- What assumptions are we making?
- Are we vulnerable to our culture?
- Are we relying on process and procedures to protect us?



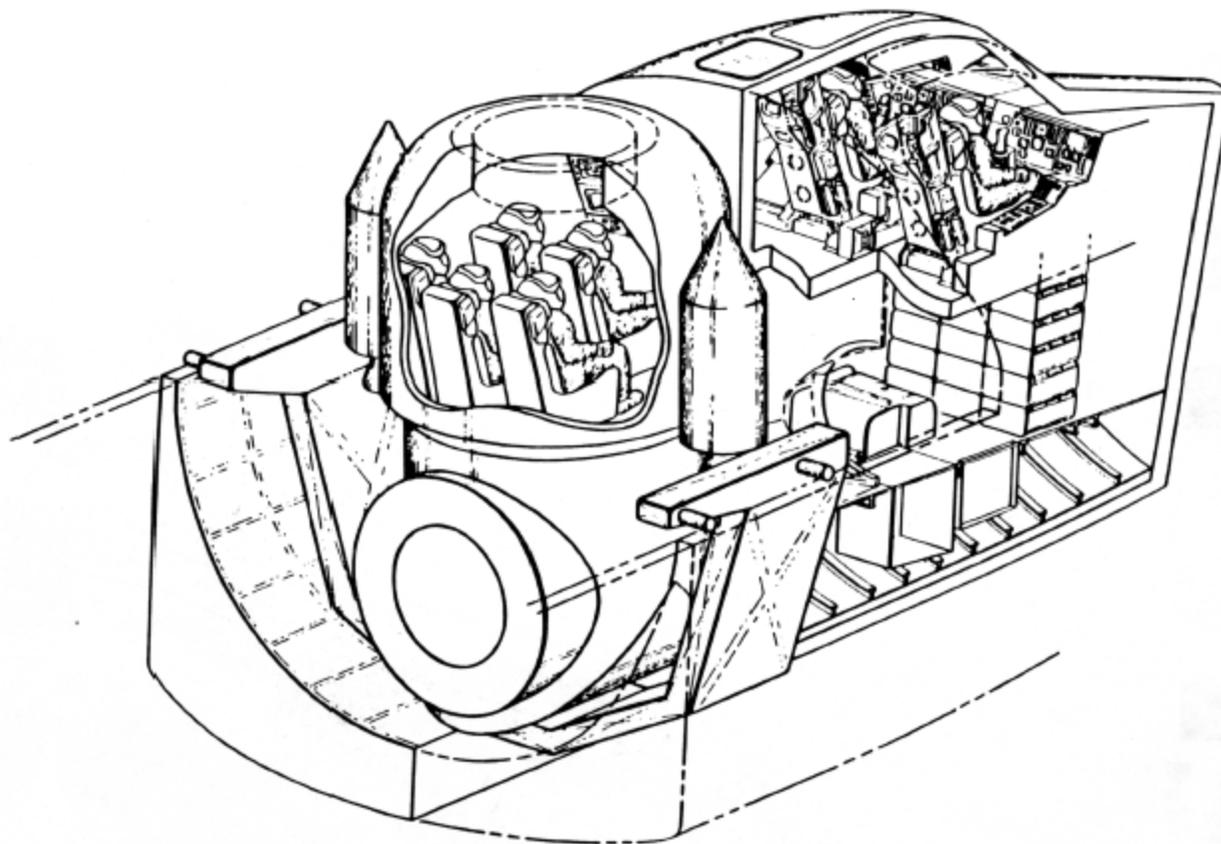
What Could NASA Have Done to Mitigate Consequences?

- What was NASA's objective?
 - "Return him safely to earth"
- NASA translated to:
 - "Return vehicle and crew safely to earth"
- Both accidents were survivable
 - Crews lived for significant periods of time after breakup
 - Relatively crude escape system would have saved both crews



NASA Aerospace Safety Advisory Panel

ORBITER CREW EJECTION ESCAPE



NASA Today

- Quit flying Space Shuttle
- Replacing with new vehicles with safety designed in and full-envelope escape systems

Can we learn from NASA?

