Failure is not an option!

SRE CON AMERICAS

SRE lessons 50 years after Apollo 13

@flyingbarron

Failure is not an option!

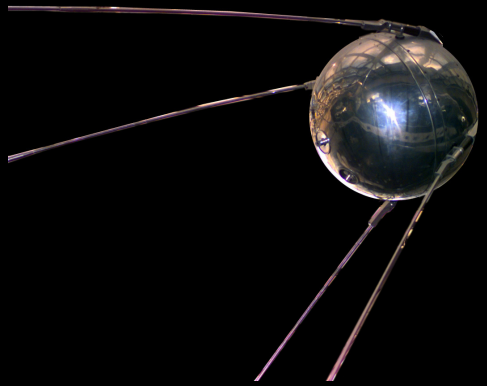
Robert Barron,
AIOps lead,
IBM Garage

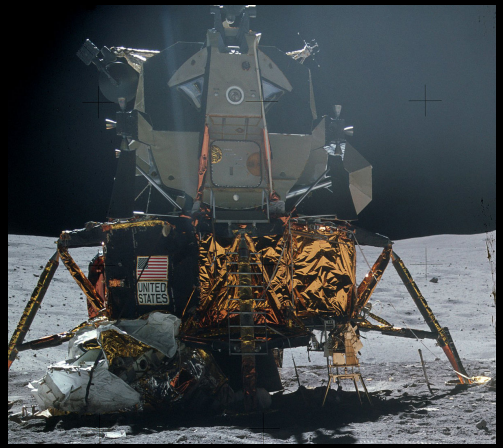
brobert@il.ibm.com

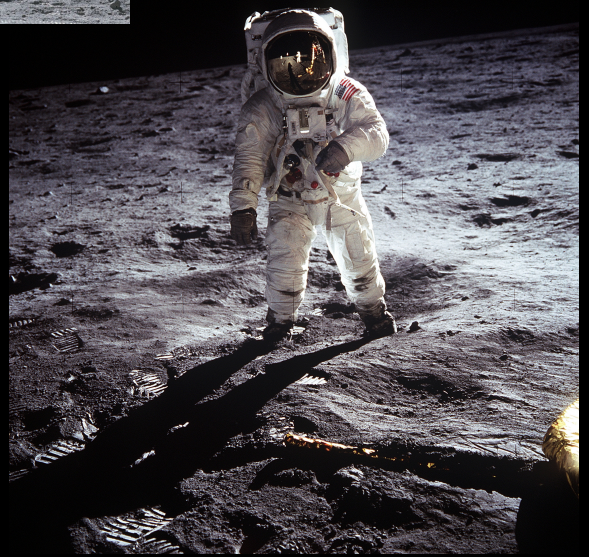
@flyingbarron

SRE lessons 50 years after Apollo 13

SRECON AMERICAS







SRE CON AMERICAS

@flyingbarron

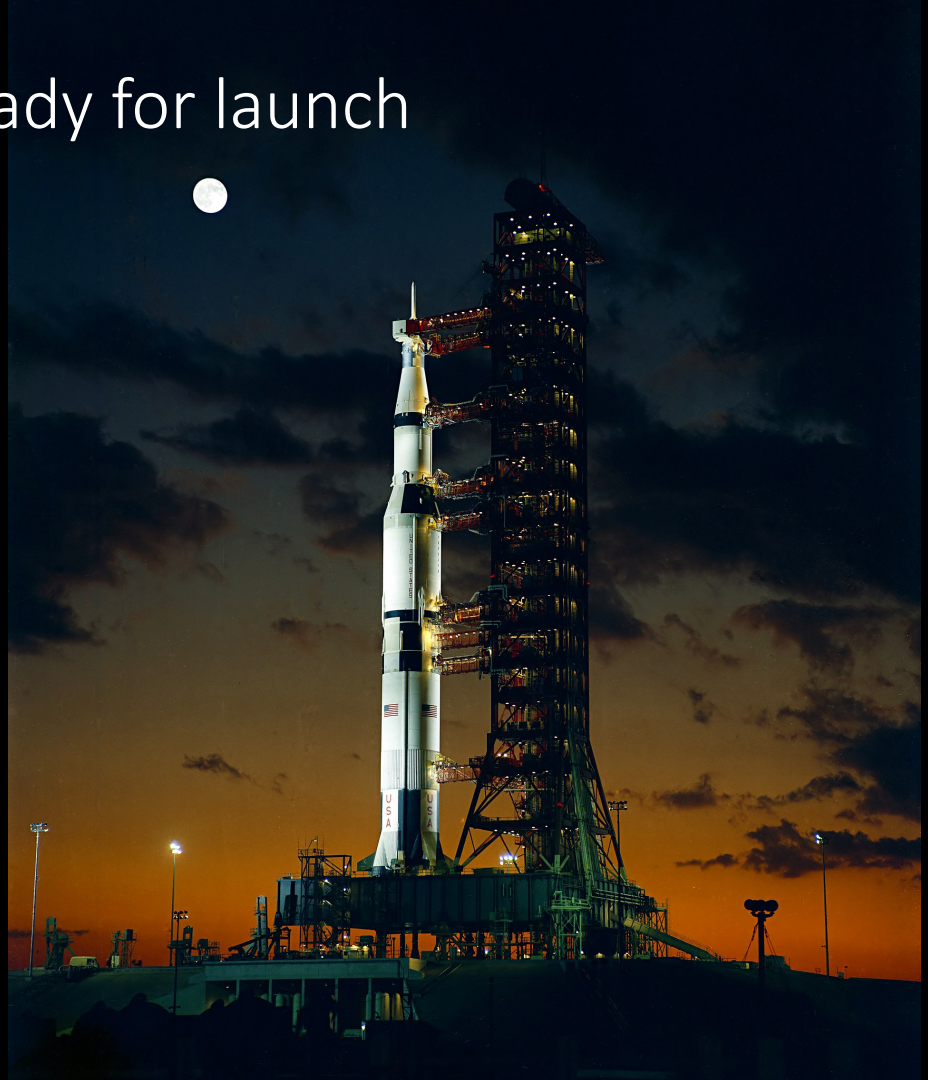
A perfect record of success leading up to Apollo 13

- Apollo 7 – First flight of Apollo
- Apollo 8 – First flight to orbit the Moon
- Apollo 9 – First flight with the full stack
- Apollo 10 – Dress rehersal of the landing
- Apollo 11 – FIRST ON THE MOON
- Apollo 12 – Pinpoint landing on the Moon

- Apollo 13 – First flight to be oriented towards scientific discovery

The *Odyssey* to the Moon

Getting ready for launch



Lesson I –
Train for failures and responses.

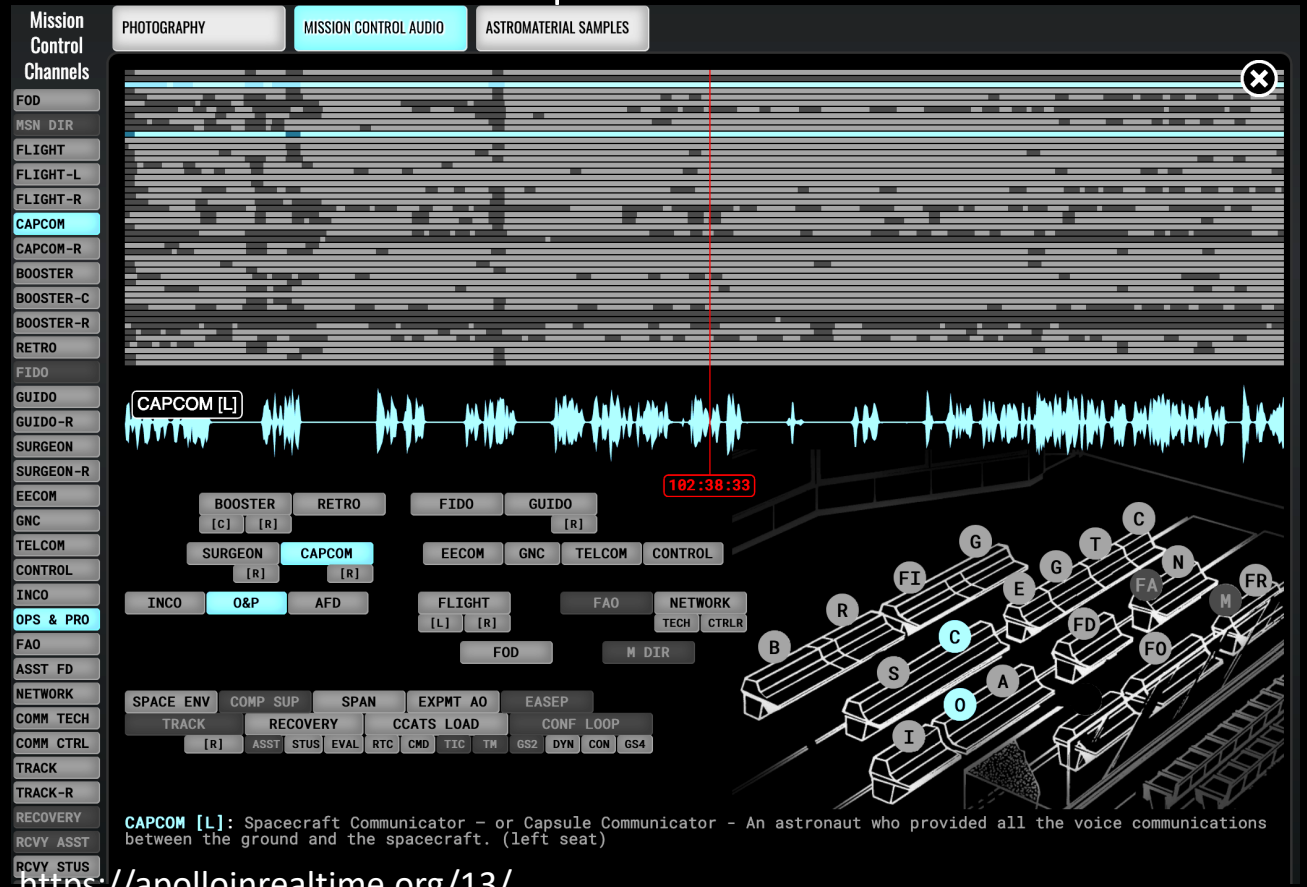
Training for success… and failure… in any shape or form.
Experiments and risks in training mean less risk during flights.

Lesson I –
Train for failures and responses.

ChatOps

Chaos Engineering

Lesson I –
Train for failures and responses.



ChatOps

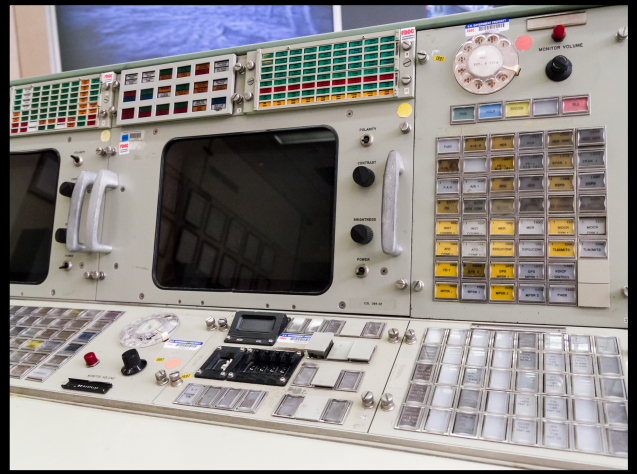
Chaos Engineering

https://apolloinrealtime.org/13/

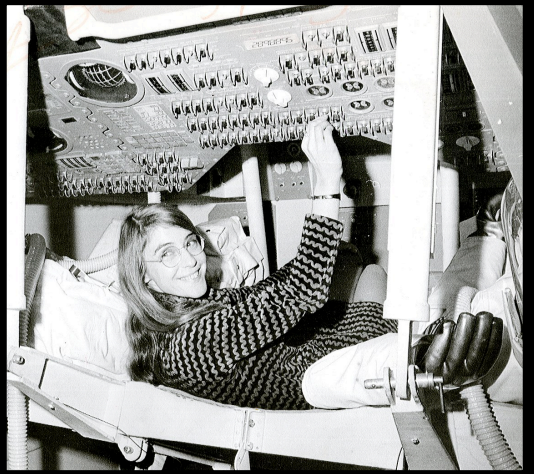
@flyingbarron

Lesson II –
Build/code for failure.

Software Engineering



Observability



Telemetry and Metrics

Alerts and Alarms

Lesson III –
Failure has many shapes and forms.

James Lovell
Commander

Fred Haise
Lunar Module (LM) Pilot

Ken Mattingly
Command/Service Module (CSM) Pilot

- August 1969 – Crew announced
- April 1970 – Launch planned

Jack Swigert
Command Module Pilot

- Three days before launch –
  Mattingly exposed to German Measles and removed from flight
- He is replaced by backup Jack Swigert

SRECON AMERICAS

@flyingbarron

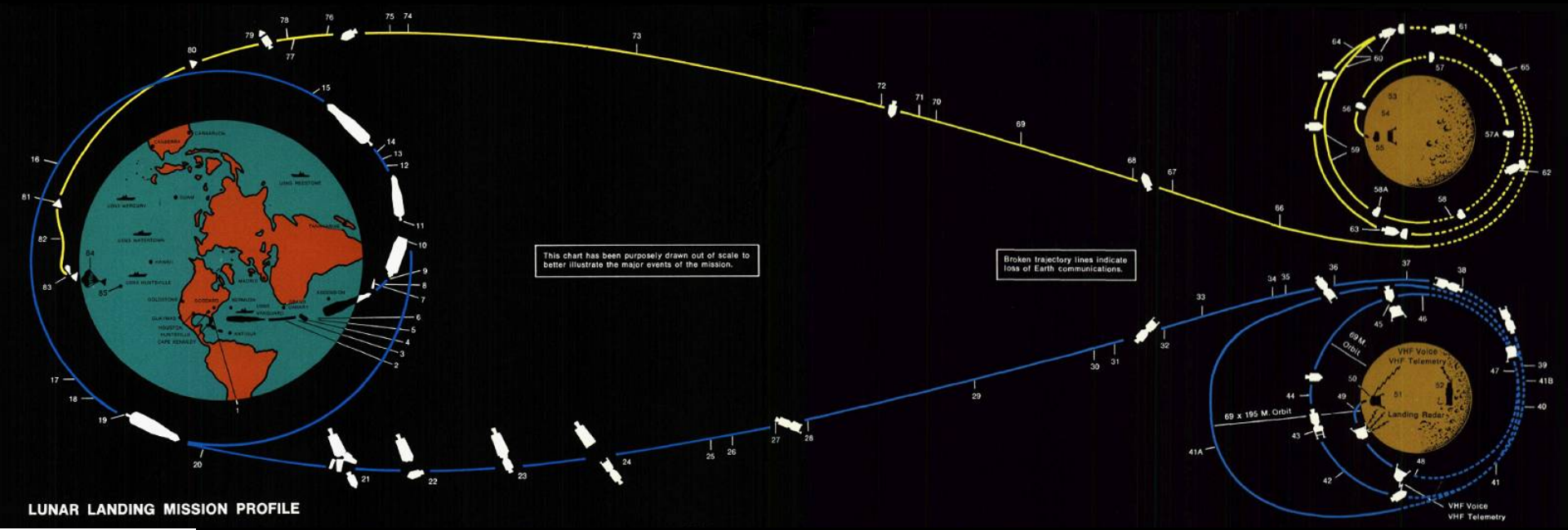
Failure is not an option!

SRE CON AMERICAS

SRE lessons 50 years after Apollo 13

@flyingbarron

The long journey to the Moon

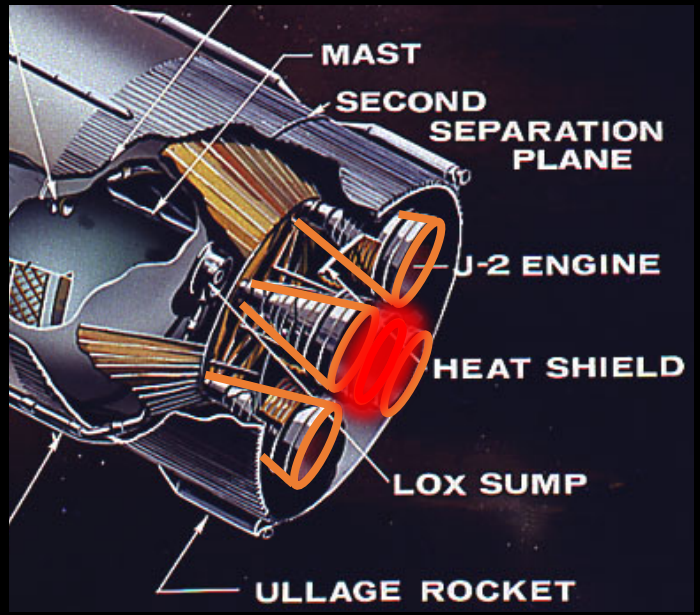


SRE CON AMERICAS

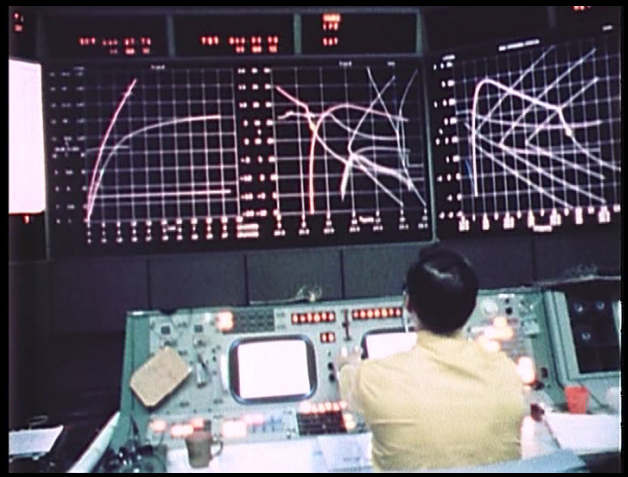
@flyingbarron

Lesson IV –
Self-healing deflects failure.

Apollo 13
launched April 11th, 1970 at 13:13 CST



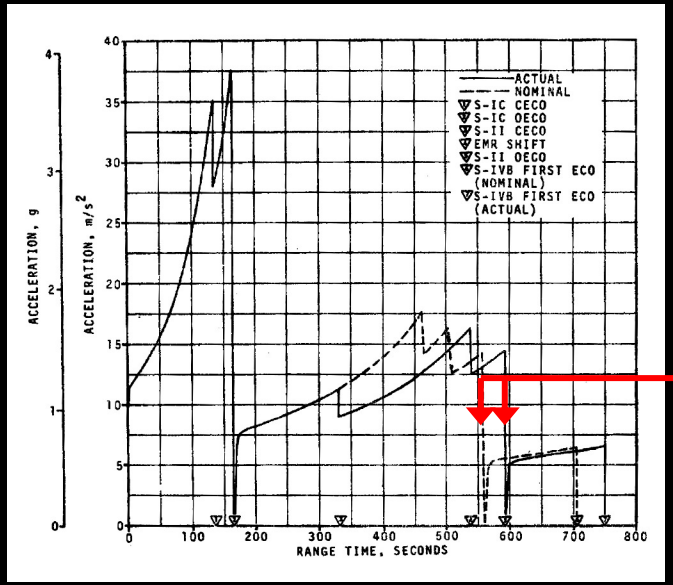
Lesson IV –
Self-healing deflects failure.



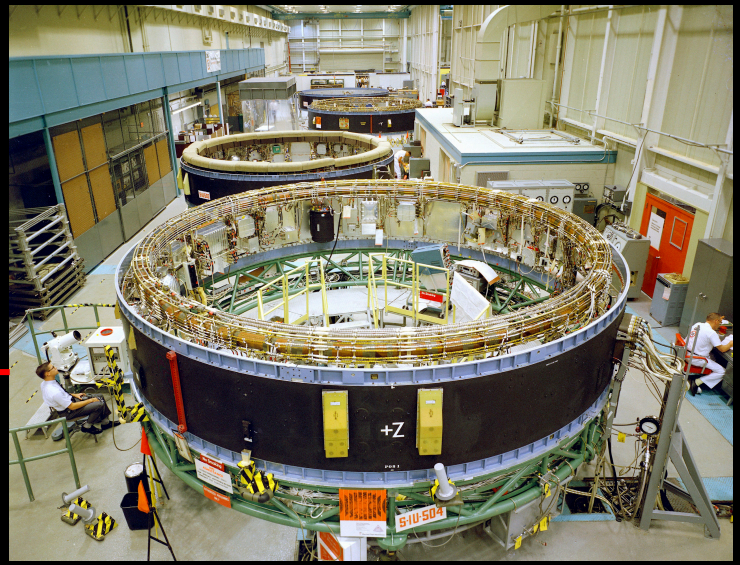
Trajectory displays filmed during the launch at Mission Control.
NASA 16mm capture. Via JSC.

Engine lights in the
Apollo Command Module dashboards

Lesson IV –
Self-healing deflects failure.

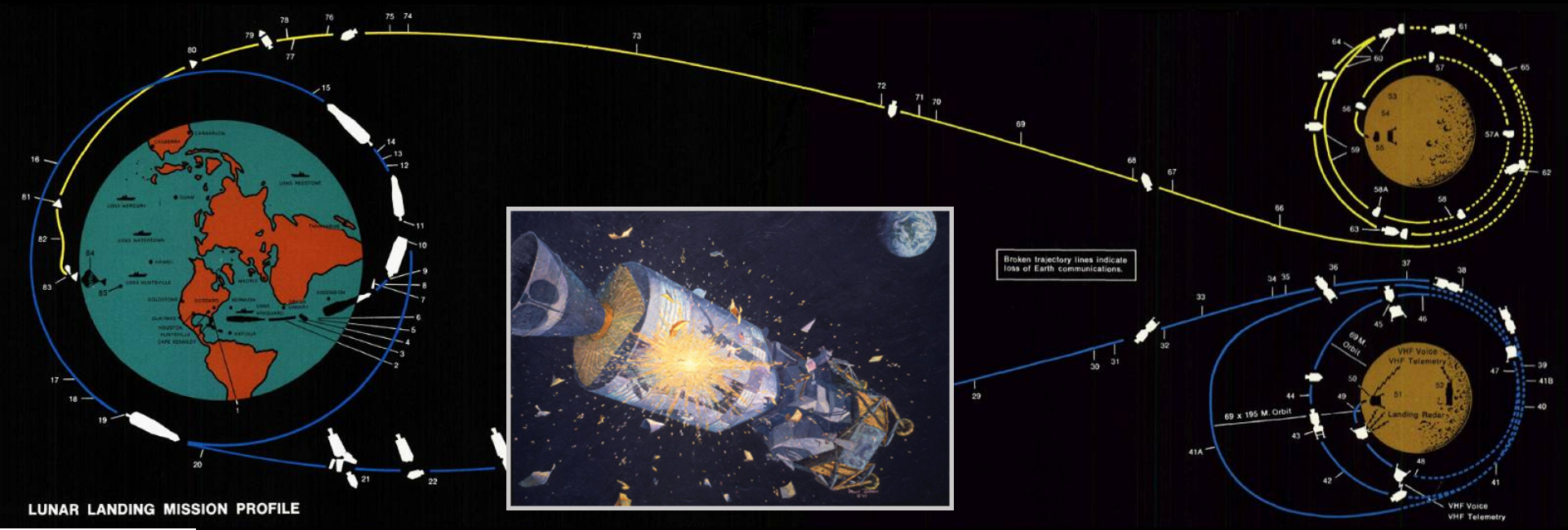


~60 second difference

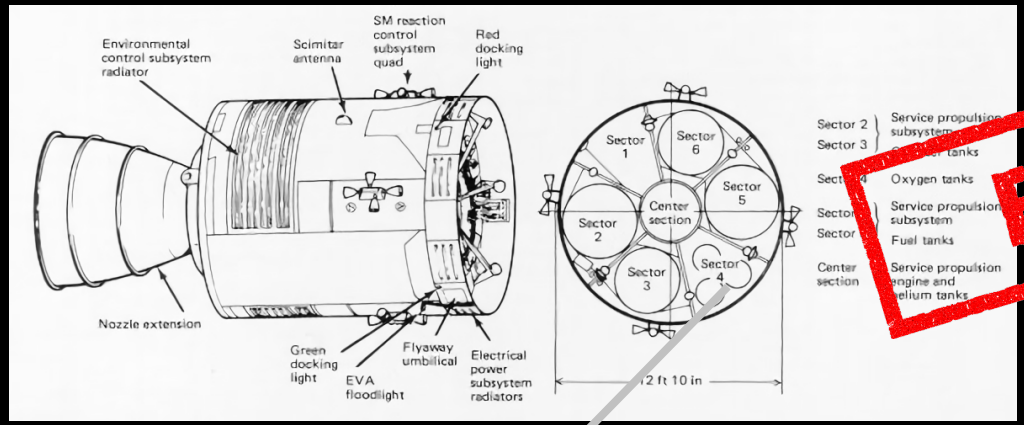


The “Brain” of the Saturn V:
IBM’s Instrument Unit

After the reliability issue of the mission, all systems go!



Lesson V –
Avoid failure through robustness & resilience.



FAIL

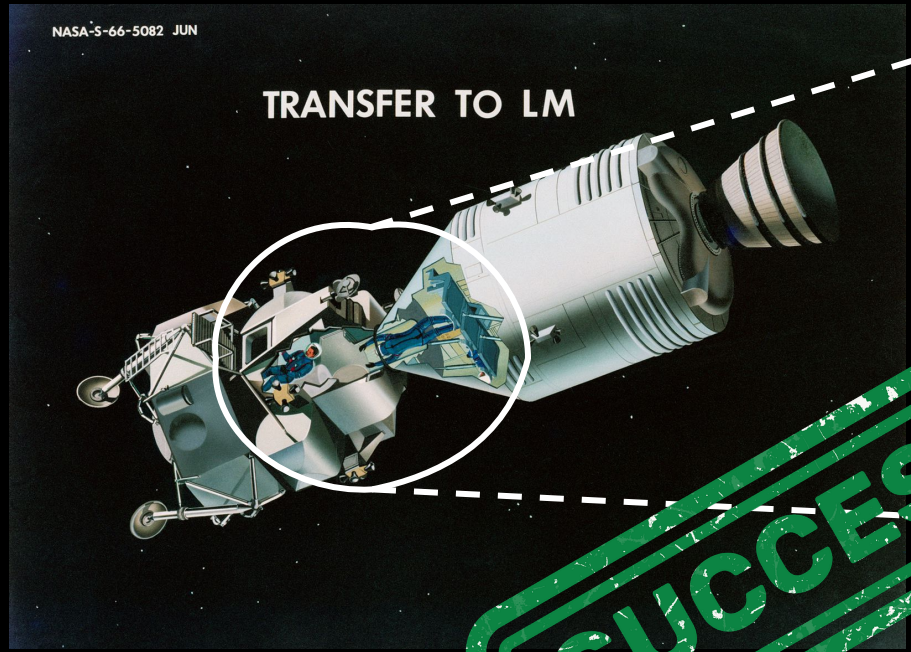
Oxygen tanks are robust – they are redundant.
But they are adjacent so when the one ruptured, the other was damaged and all the oxygen was lost

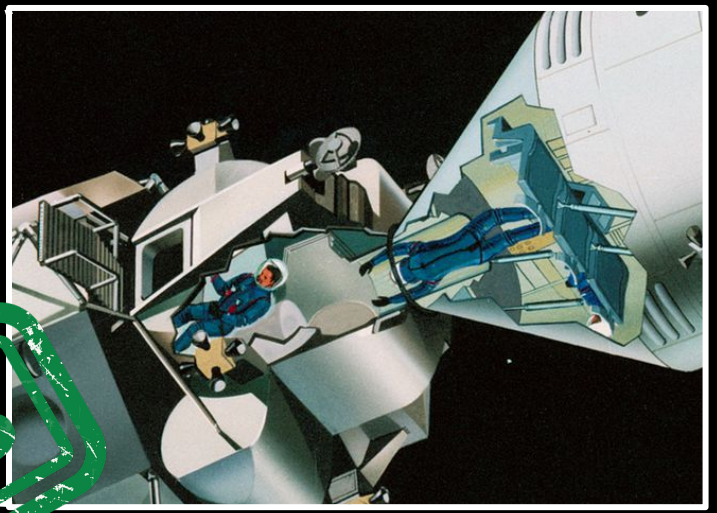
Mutiple redundant fuel cells generate electricity, fed by the redundant oxygen tanks – but when both tanks were empty, no power was generated

SRE CON AMERICAS

@flyingbarron

Lesson V –
Avoid failure through robustness & resilience.





Lunar Module as a lifeboat instead of a lander

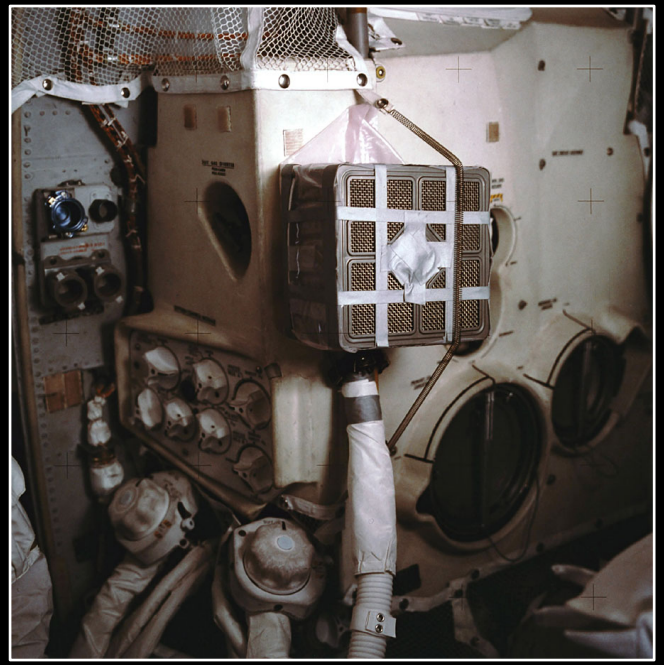
SUCCESS

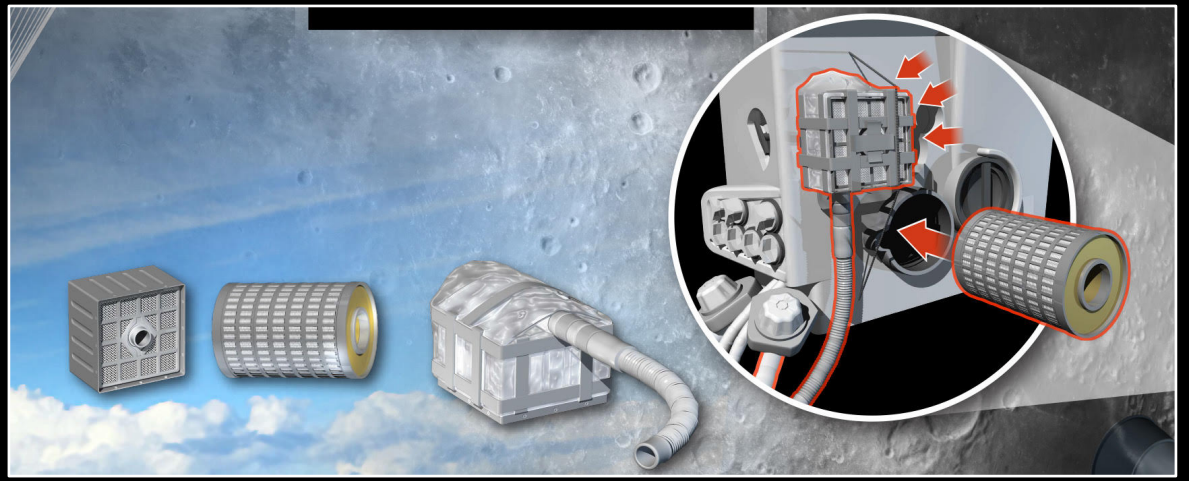
SRE CON AMERICAS

@flyingbarron

Lesson VI –
Failure is not an option – deal with problems

Lesson VI –
Failure is not an option – have a plan





Runbooks and Contingencies

SRECON AMERICAS

@flyingbarron

Lesson VI –
Failure is not an option – have a plan

Scenario	When tested
Lunar module as a lifeboat	Practised in Apollo 10
Navigating without the computer	Practised in Gemini
Maneuvering without the computer	Practised in Apollo 8
Fixing Carbon Dioxide ”scrubbers”	Practised in Apollo 8
Last minute crewmember change before launch	Backups trained for all missions

It’s not improvisation if you’ve prepared for it!

Lesson VI –
Failure is not an option – have a plan

Scenario	When tested
Lunar module as a lifeboat	Practised in Apollo 10
Navigating without the computer	Practised in Gemini
Maneuvering without the computer	Practised in Apollo 8
Fixing Carbon Dioxide ”scrubbers”	Practised in Apollo 8
Last minute crewmember change before launch	Backups trained for all missions
Changing mission parameters	IBM computers constantly running “what if” scenarios before and during flights

It’s not improvisation if you’ve prepared for it!

@flyingbarron

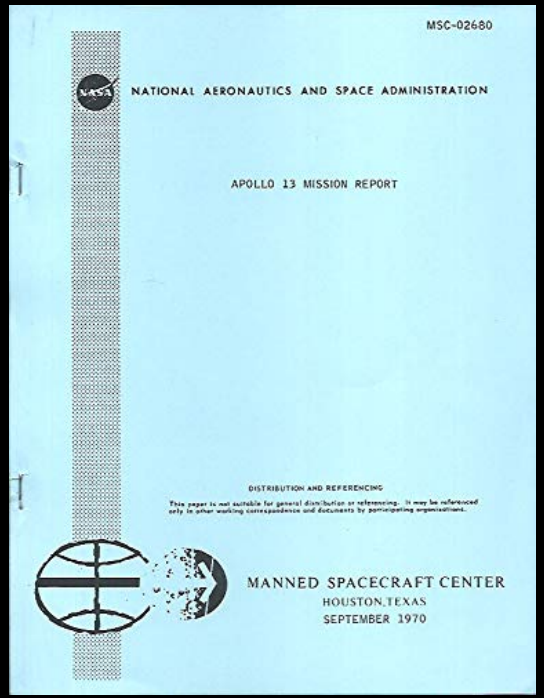
Lesson VI –
Failure is not an option – have a plan

Scenario	When tested
Lunar module as a lifeboat	Practised in Apollo 10
Navigating without the computer	Practised in Gemini
Maneuvering without the computer	Practised in Apollo 8
Fixing Carbon Dioxide ”scrubbers”	Practised in Apollo 8
Last minute crewmember change before launch	Backups trained for all missions
Changing mission parameters	IBM computers constantly running “what if” scenarios before and during flights
Restart all Apollo Command Module systems midflight	Never before

It’s not improvisation if you’ve prepared for it!

After all the problems, a safe landing!

After the flight – Post-Mortems


MSC-02680

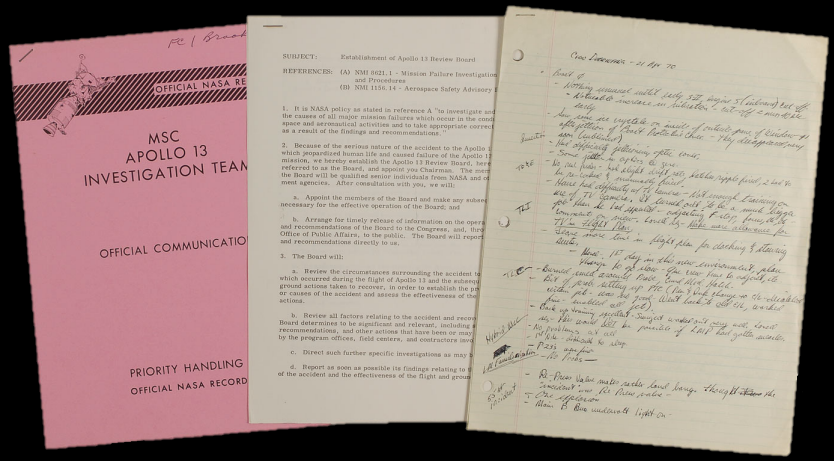
NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

APOLLO 13 MISSION REPORT

DISTRIBUTION AND REFERENCING

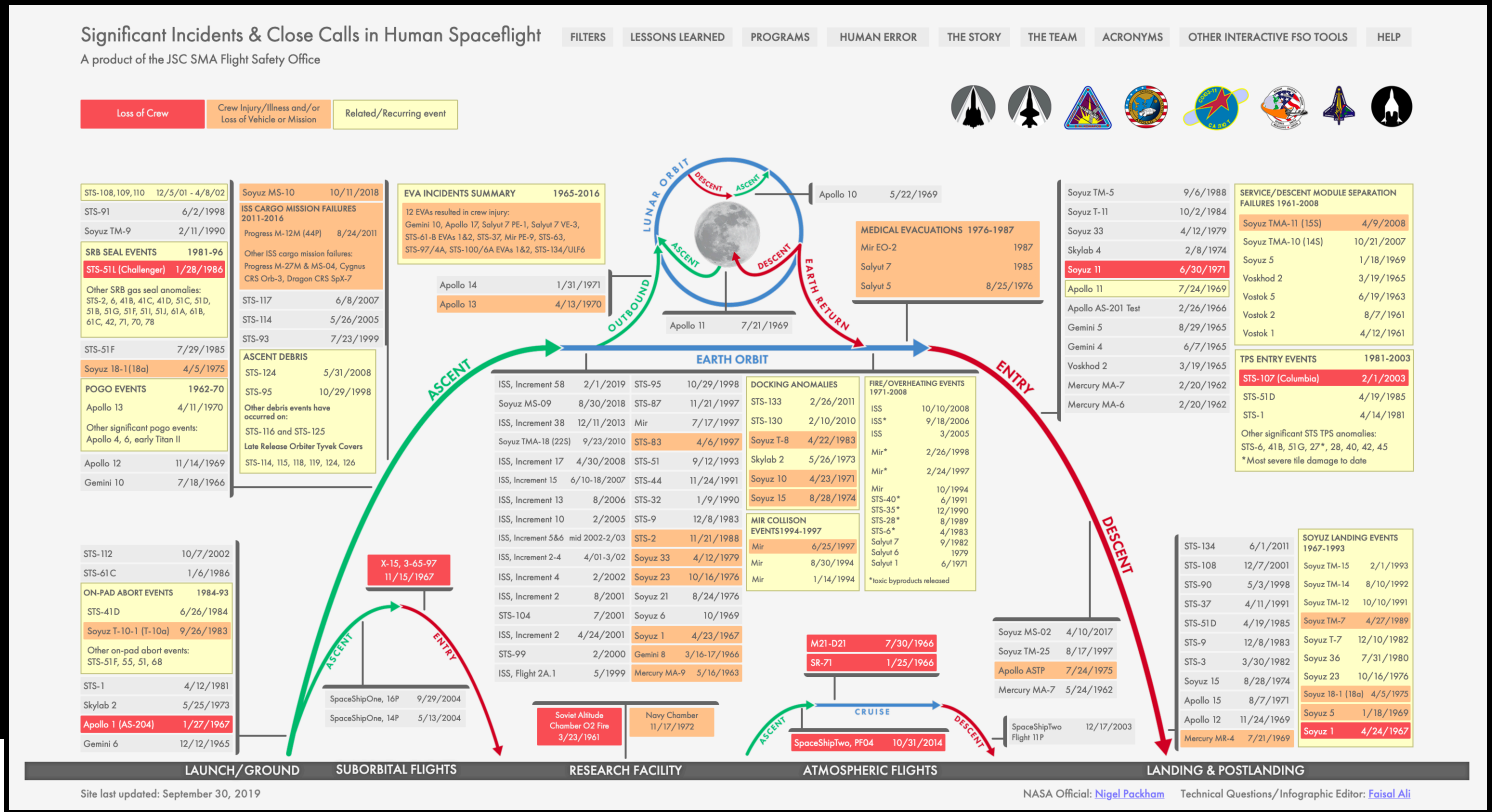
This paper is not suitable for general distribution or referencing. It may be referenced only in other working correspondence and documents by participating organizations.

MANNED SPACECRAFT CENTER
HOUSTON, TEXAS
SEPTEMBER 1970



https://www.hq.nasa.gov/alsj/a13/A13_MissionReport.pdf

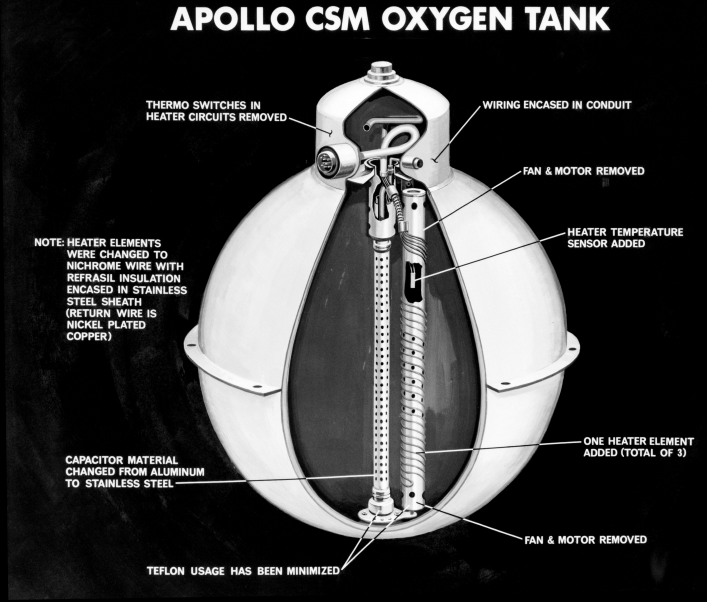
Significant Incidents & Close Calls in Human Spaceflight



https://sma.nasa.gov/SignificantIncidents/index.html

@flyingbarron

Lessons VII –
Tools fail, validate your assumptions

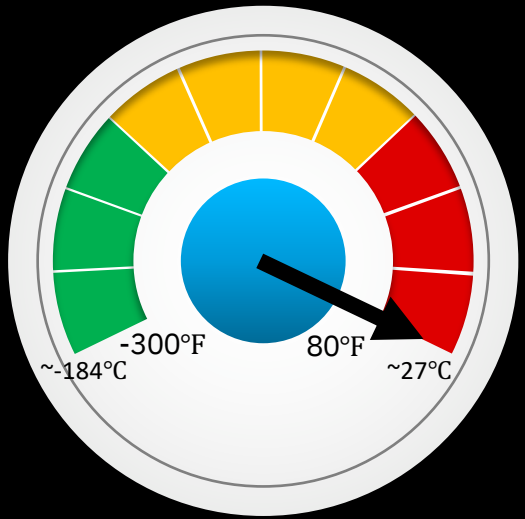


The tank was dropped in early 1969
(a year before the flight)

Tank passes all tests
till pre-flight testing
(April 1970)

After the last test, the tank
is heated to “boil off”
the liquid oxygen

Tank reaches 1,000°F!
(~540°C)



Insulation of wires is burnt off, exposing them to
the liquid oxygen in the tank…

SRECON AMERICAS

@flyingbarron

Lesson VIII –
Avoid future failure by reducing technical debt

Add reliability

Add observability

Add redundancy

The cryogenic oxygen tank design will be changed to eliminate the mechanisms which could initiate burning within the tank and ultimately lead to a structural failure of the tank or its components. All electrical wires will be stainless-steel sheathed and the quantity probe will be made from stainless steel instead of aluminum. The fill-line plumbing internal to the tank will be improved, and a means of warning the crew of an inadvertent closure of either the fuel cell hydrogen or oxygen valves will be provided. A third cryogenic oxygen tank will be added to the service module for subsequent Apollo missions. The fuel cell oxygen supply valve will be redesigned to isolate polytetrafluoroethylene-coated wires from the oxygen. Warning systems at the Mission Control Center will be modified to provide more immediate and visible warnings of anomalies in all systems.

A more thorough discussion of this anomaly is presented in reference 1.

This anomaly is closed.

Not improvisation – preplanning!


MSC-02680

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

APOLLO 13 MISSION REPORT

DISTRIBUTION AND REFERENCING

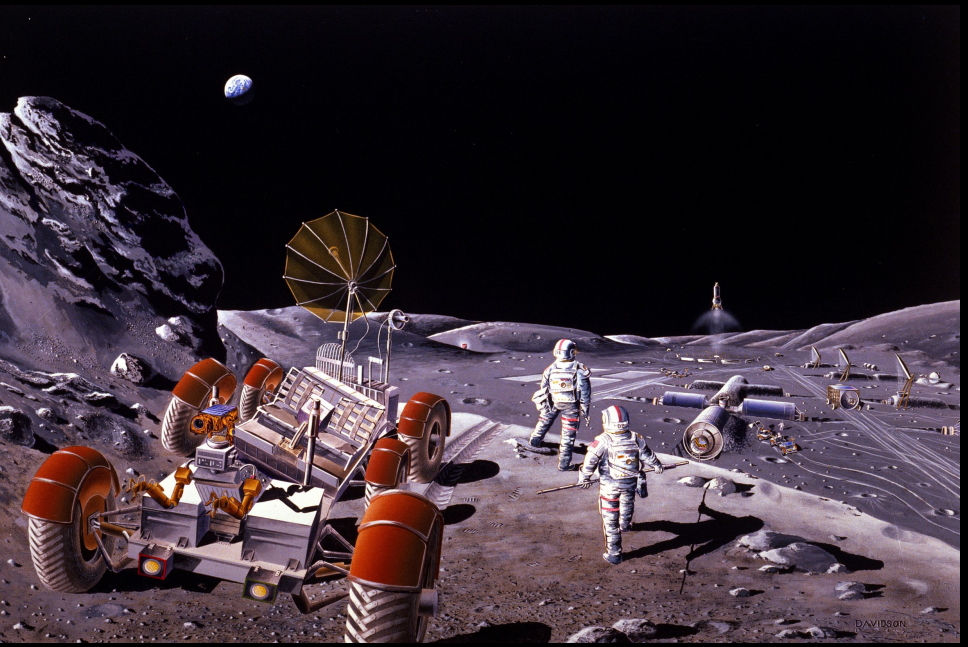
This paper is not suitable for general distribution or referencing. It may be referenced only in other working correspondence and documents by participating organizations.

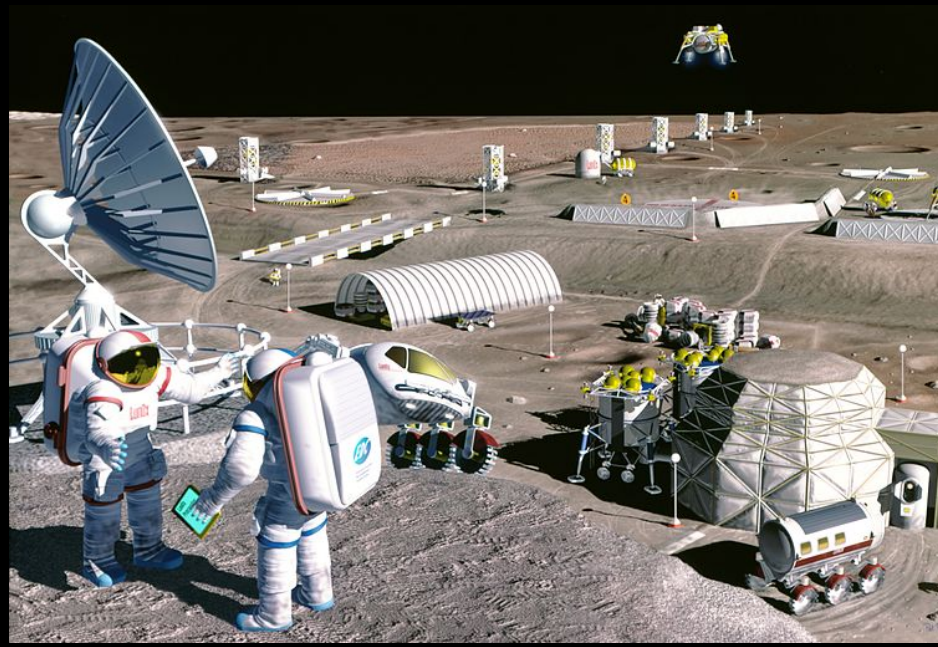
MANNED SPACECRAFT CENTER
HOUSTON, TEXAS
SEPTEMBER 1970

There are several aspects of the mission which deserve special note although these do not appear in the narrative. First of all, the procedures used in recovering from the anomaly were, in a great many instances, fairly well thought out premission. For example: The LM jettison sequence and time, the LM operation at minimum cooling, the midcourse alignment technique, and the procedure to separate the LM and the Saturn S-IVB stage communication frequency to name a few. When new procedures were required or when existing procedures had to be reviewed, the core of the premission planning team was used. This resulted in well coordinated, quickly defined procedures.

Another important aspect is that premission work with LM systems and CSM systems in minimum power configurations contributed greatly to the ability to provide suitable systems configurations for the Apollo 13 case. This work also provided an additional capability that was available through minimum duty cycles. Fortunately this was not required, but the point should be made that there was a level of operations availabe that would have resulted in LM water and battery power usage rates well below the final stabilized rates obtained.

Lesson IX –
Business failure despite technical success





SRECON AMERICAS

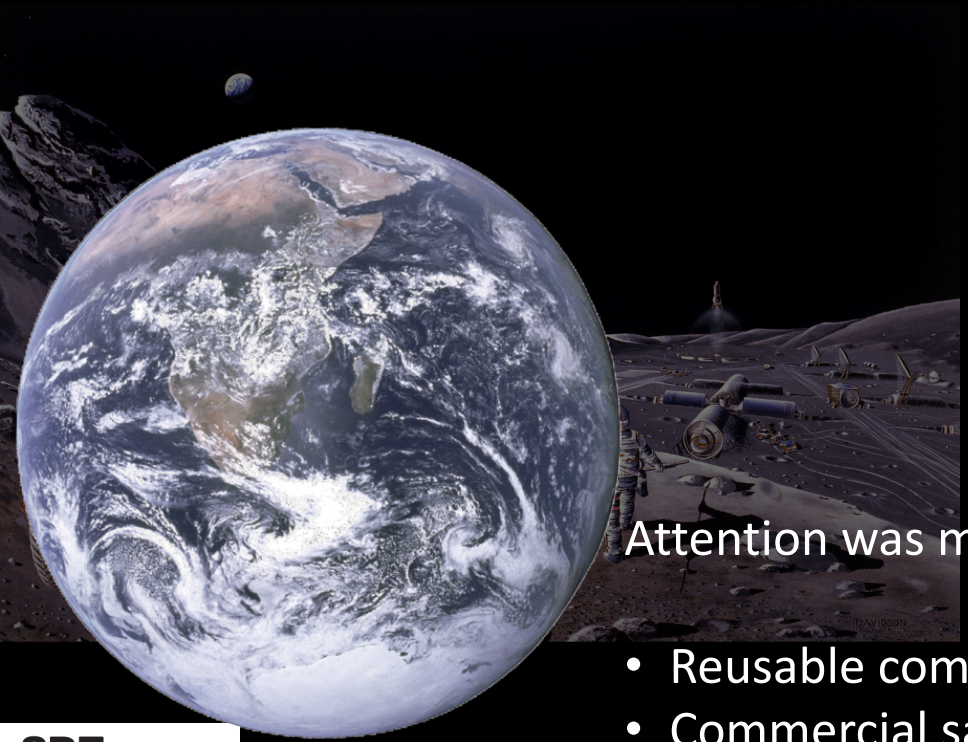
@flyingbarron

Lesson IX –
Business failure despite technical success

SRECON AMERICAS

@flyingbarron

Lesson IX –
Business failure despite technical success



Attention was moved to

- Reusable components (saving money & other resources)
- Commercial satellites
- International cooperation in Space

Lessons

- Lesson I – Train for failures and responses.
- Lesson II – Build/code for failure.
- Lesson III – Failure has many shapes and forms.
- Lesson IV – Self-healing deflects failure.
- Lesson V – Avoid failure through robustness & resilience.
- Lesson VI – Failure is not an option – deal with the unexpected
- Lessons VII – Tools fail, validate your assumptions
- Lesson VIII – Avoid future failure by reducing technical debt
- Lesson IX – Business failure despite technical success

Prepare for failure

Adapt to failure

Reduce future failure

Build for reliability

Learning

Reserve Capacity

Culture

Resilience

Runbooks and Playbooks

Performance Tuning

Leadership

Simulations & Chaos Engineering

Robust

Blameless

Skills

Automation

Change Management

SRECON AMERICAS

@flyingbarron

Build for reliability Learning Reserve Capacity
Culture Runbooks and Playbooks
Resilience
Performance Tuning Engineering
Leadership Robust
Simulations & Chaos Blameless
Skills Automation
Change Management

Failure is not an option;
it's a certainty – be prepared for the things you're not prepared for.

SRECON AMERICAS

@flyingbarron

Resources used / Further information

- Apollo 13 in real time – https://apolloinrealtime.org/13
- BBC *13 minutes to the Moon* – https://www.bbc.co.uk/programmes/p083wp70
- NASA database of Significant Incidents & Close Calls in Human Spaceflight – https://sma.nasa.gov/SignificantIncidents
- Apollo Infographics – http://www.tonybela.com/
- Remastered video – https://www.youtube.com/c/Dutchsteammachine

Further information

- https://ibm.biz/apollo-lessons & https://ibm.biz/apollo-lessons-first & https://medium.com/@flyingbarron
- IBM and the Apollo missions – https://newsroom.ibm.com/apollo & https://www.ibm.com/thought-leadership/the-apollo-missions

Be sure to stop by the IBM booth for products, services and solutions.

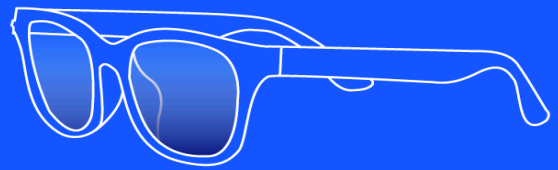
IBM

Enter to claim one of 50 blue light blocking glasses from IBM.

AI and automation allow you to deliver greater reliability, with less risk, and higher visibility.

Do you want to reduce headaches, eye strain and site reliability issues? We can help you on all fronts with a pair of blue light blocking glasses and IBM solutions.

Be the first of 50 attendees from SREcon to enter below for your chance to win!



Claim yours today →

ibm.biz/SREcon

Learn more about IBM solutions by visiting: **ibm.com**/products/watson-aiops

This offer is only valid in the United States and is not available to employees of government entities or government-owned or controlled entities, IBM employees or its contractors. Subject to official IBM contest rules. Supplies are limited. Winners will be drawn and contacted after 12/15/2020.

SRECON AMERICAS

@flyingbarron

Failure is not an option!

Thank you for watching

SRE CON AMERICAS

SRE lessons 50 years after Apollo 13

@flyingbarron