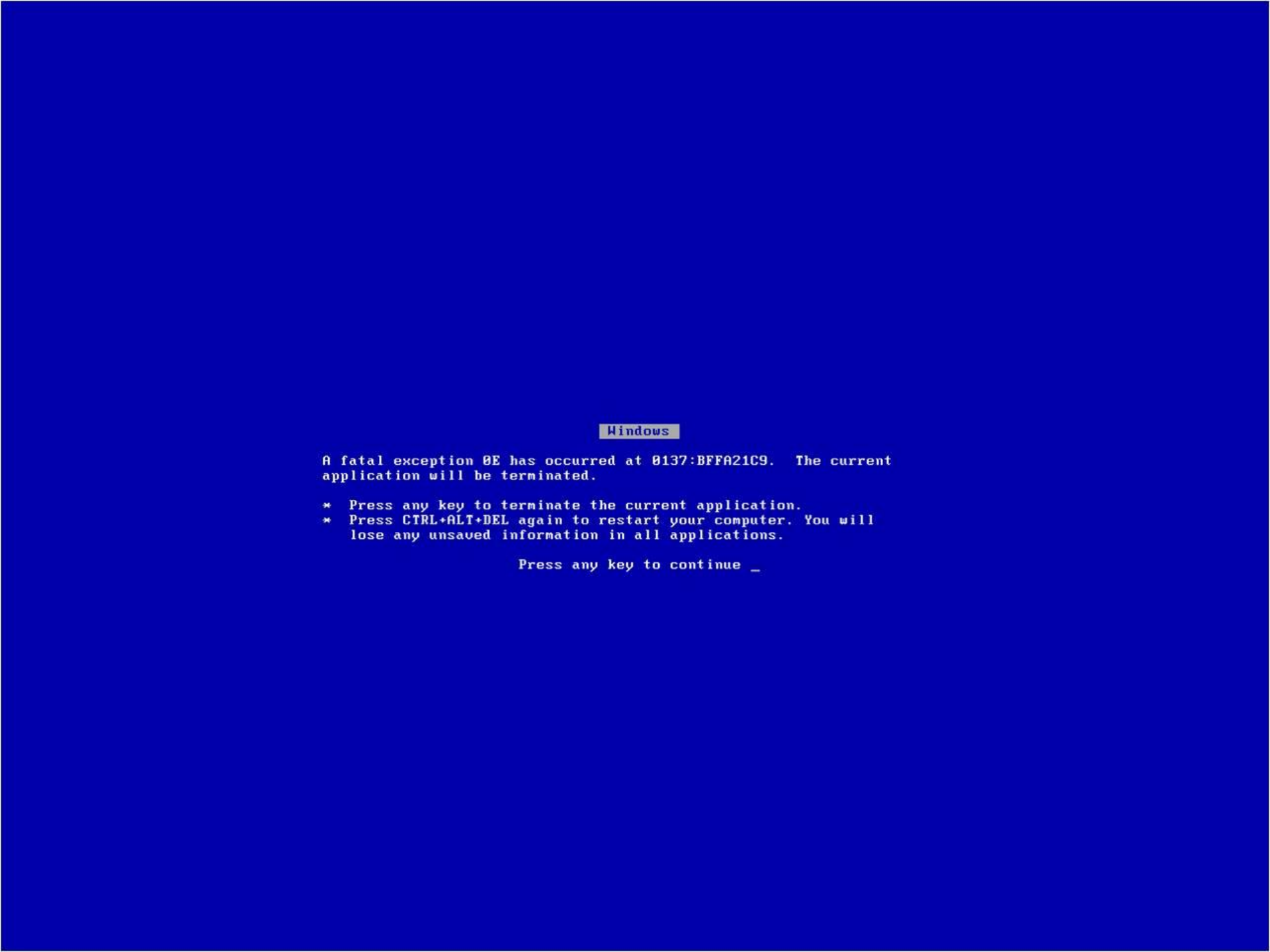
Space Related Software Development

Prof. Chris Johnson,
School of Computing Science, University of Glasgow, Scotland.
http://www.dcs.gla.ac.uk/~johnson

Introduction to Safety-Critical Systems.


Windows
A fatal exception 0E has occurred at 0137:BFFA21C9. The current application will be terminated.
* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.
Press any key to continue _

University of Glasgow

Shetland and Pessimism

University of Glasgow

China Competing on Safety…


WINDOW JETTISON HANDLE PIN
REMOVE BEFORE JETTISON


2
3

University of Glasgow

Overview

- Previous aviation mishaps:
  - Berliotz and the Habsheim accident.
- Previous space software mishaps:
  - Apollo Lunar Landing and Mars Climate Orbiter;.
- Reason's Model of Accidents…
- Looking to the future:
  - Software for the Mars missions…

University of Glasgow

Wright Brothers

Berlioz Sea-Plane Attempts

University of Glasgow

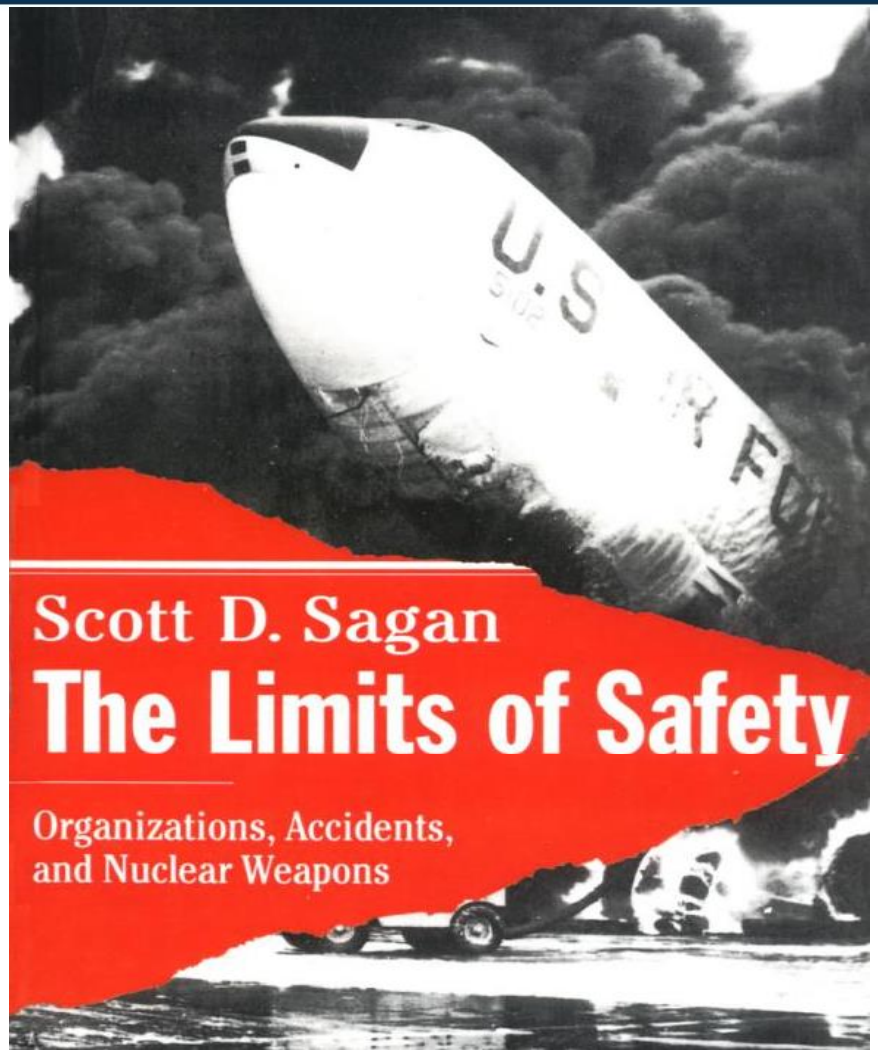
Edsger W Dijkstra (1930-2002)

Testing can prove the presence of errors, but not their absence.

The Habsheim Accident

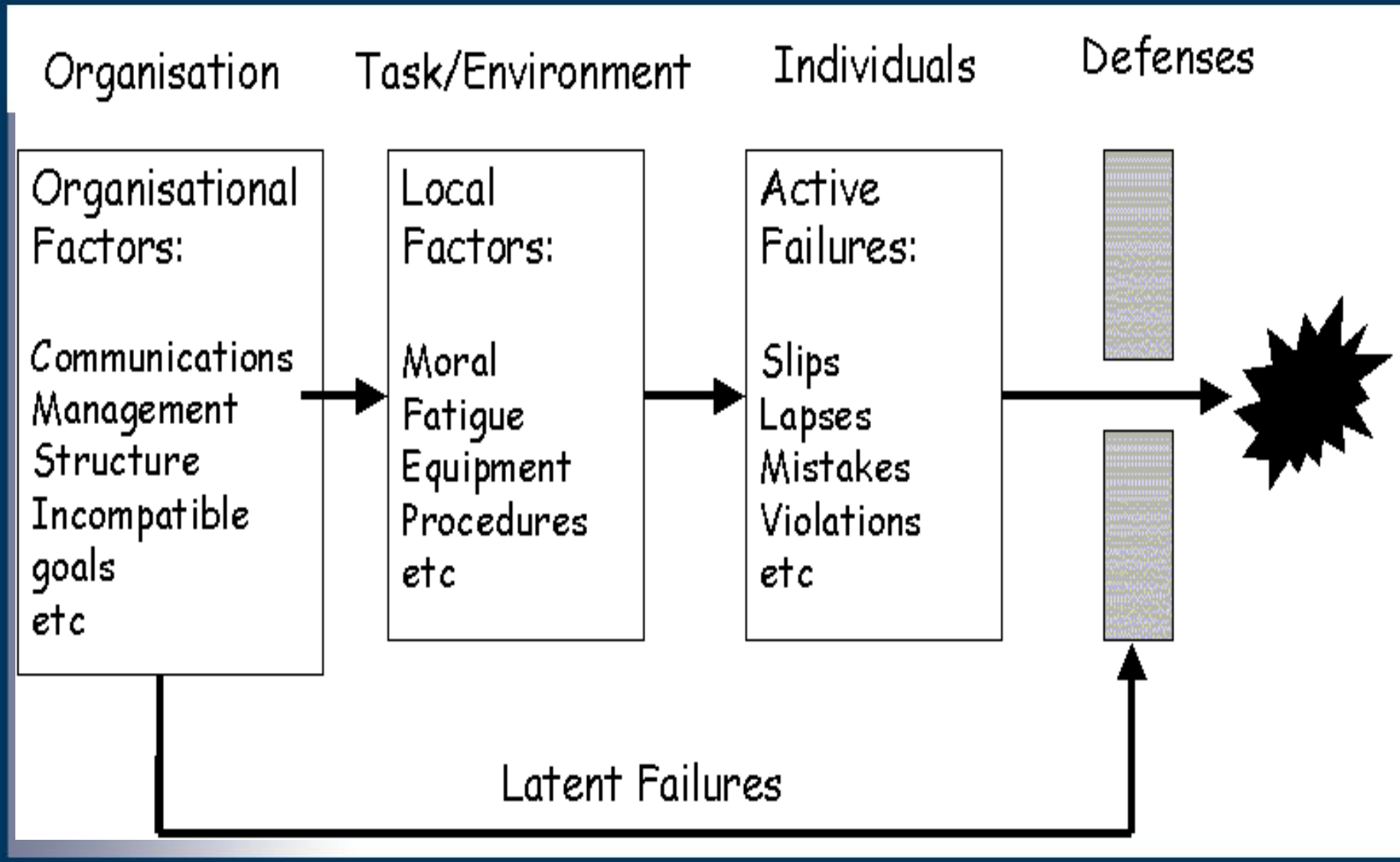
University of Glasgow

Normal Accidents…



University of Glasgow

Reason's Model of Accidents



University of Glasgow

Failures in Early Rocket Designs

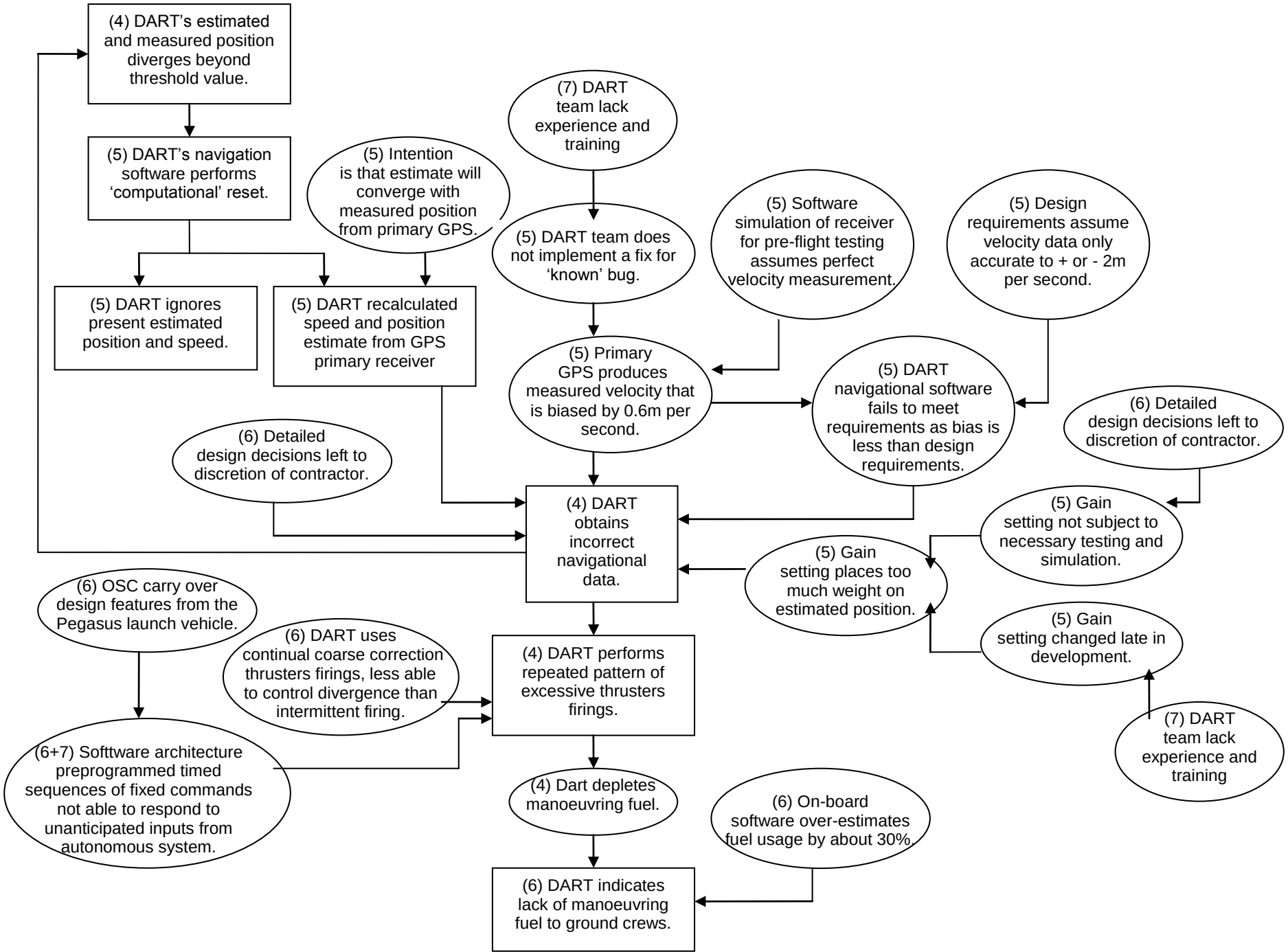
Software Failure During Moon Landing

20th July, 1969 Neal Armstrong and Buzz Aldrin:

Lunar Module:	"1201 . . . 1201." [running out of cycles]
Houston:	"Roger 1201 alarm."
Houston:	"MIT, what's 1201?"
Houston:	"The computer is running out of cycles."
Houston:	"Trajectory's good, we're go for flight."
. . .	
Lunar Module:	"2000 feet . . . 1202." [Computer reset]
Houston:	"Roger 1202, we copy."
Houston:	"MIT?"
Houston:	"Go!"
. . .	
Houston:	"Eagle, Houston, you're go for flight."
Houston:	"One minute [of fuel left]."
. . .	
Lunar Module :	"100 feet, 3 l/2 down, 9 forward."
Houston:	"30 seconds."
Lunar Module :	"OK, engine stop."
Houston:	"We copy it down Eagle."
Lunar Module :	"Houston, Tranquility Base here, the Eagle has landed."

University of Glasgow

Mars Climate Orbiter


(4) DART's estimated and measured position diverges beyond threshold value.
(5) DART's navigation software performs 'computational' reset.
(5) DART ignores present estimated position and speed.
(5) DART recalculated speed and position estimate from GPS primary receiver
(5) Intention is that estimate will converge with measured position from primary GPS.
(7) DART team lack experience and training
(5) DART team does not implement a fix for 'known' bug.
(5) Software simulation of receiver for pre-flight testing assumes perfect velocity measurement.
(5) Design requirements assume velocity data only accurate to + or - 2m per second.
(5) Primary GPS produces measured velocity that is biased by 0.6m per second.
(5) DART navigational software fails to meet requirements as bias is less than design requirements.
(6) Detailed design decisions left to discretion of contractor.
(6) Detailed design decisions left to discretion of contractor.
(4) DART obtains incorrect navigational data.
(5) Gain setting not subject to necessary testing and simulation.
(5) Gain setting places too much weight on estimated position.
(5) Gain setting changed late in development.
(7) DART team lack experience and training
(6) OSC carry over design features from the Pegasus launch vehicle.
(6) DART uses continual coarse correction thrusters firings, less able to control divergence than intermittent firing.
(4) DART performs repeated pattern of excessive thrusters firings.
(6+7) Softtware architecture preprogrammed timed sequences of fixed commands not able to respond to unanticipated inputs from autonomous system.
(4) Dart depletes manoeuvring fuel.
(6) On-board software over-estimates fuel usage by about 30%.
(6) DART indicates lack of manoeuvring fuel to ground crews.

Looking to the Future?

“We leave as we came, and God willing, as we shall return, with peace and hope for all mankind"

Gene Cernan, Commander, Apollo 17, December 1972

Looking to the Future?

2011 – End of Shuttle. (ESA Manned ATV)
2020 – Orion Lunar missions (2025 ESA)
2030 – Mars Missions (2030-2035, ESA)
2060- Long Term Occupation?

University of Glasgow

Software in Mars Mission Planning

- Moon:
  - Ave distance: 238,855 miles or 238,857 (ESA);
  - Cruise lasts weeks;
  - Communications delays will be seconds.
- Mars:
  - Opposition distance: 35 to 70,000,000 miles;
  - Cruise lasts 9 months or more;
  - Communication delay 20 (MIT) to 40 (ESA) mins.
- Software systems:
  - Ship maintenance: requirements very hard;
  - Crew physiology: radiation & telesurgery.
  - Crew psychology – HAL and Noordwijk groups.

University of Glasgow

Mars 105 Experiment

- International crew:
  - 4 Russians, a German and a Frenchman;
- Inst. for Biomedical Problems, Moscow.
  - 3 windowless steel capsules 550m^{3}.
  - 520 days, 30 day sejour on Mars;
  - 5,600 people applied.
- “Evacuation of crew members due to illness or their own free will equal ‘the death’ of a cosmonaut”
- 20 minute communication delays...

University of Glasgow

Overview

- Previous aviation mishaps:
  - Berliotz and the Habsheim accident.
- Previous space software mishaps:
  - Apollo Lunar Landing and Mars Climate Orbiter;.
- Reason's Model of Accidents…
- Looking to the future:
  - Software for the Mars missions…

University of Glasgow

Thank You and Any Questions?