Sandia National Laboratories

*Exceptional service in the national interest*

SAND2016-3412C

NUCLEAR EXPLOSIVE SAFETY

NES

WORKSHOP 2016

# SpaceShipTwo Accident

Judi E. See, Ph.D., CPE

Sandia National Laboratories/ New Mexico

Org. 0151, Nuclear Weapons Systems Analysis

jesee@sandia.gov, 505-844-4567

27 April 2016

U.S. DEPARTMENT OF ENERGY

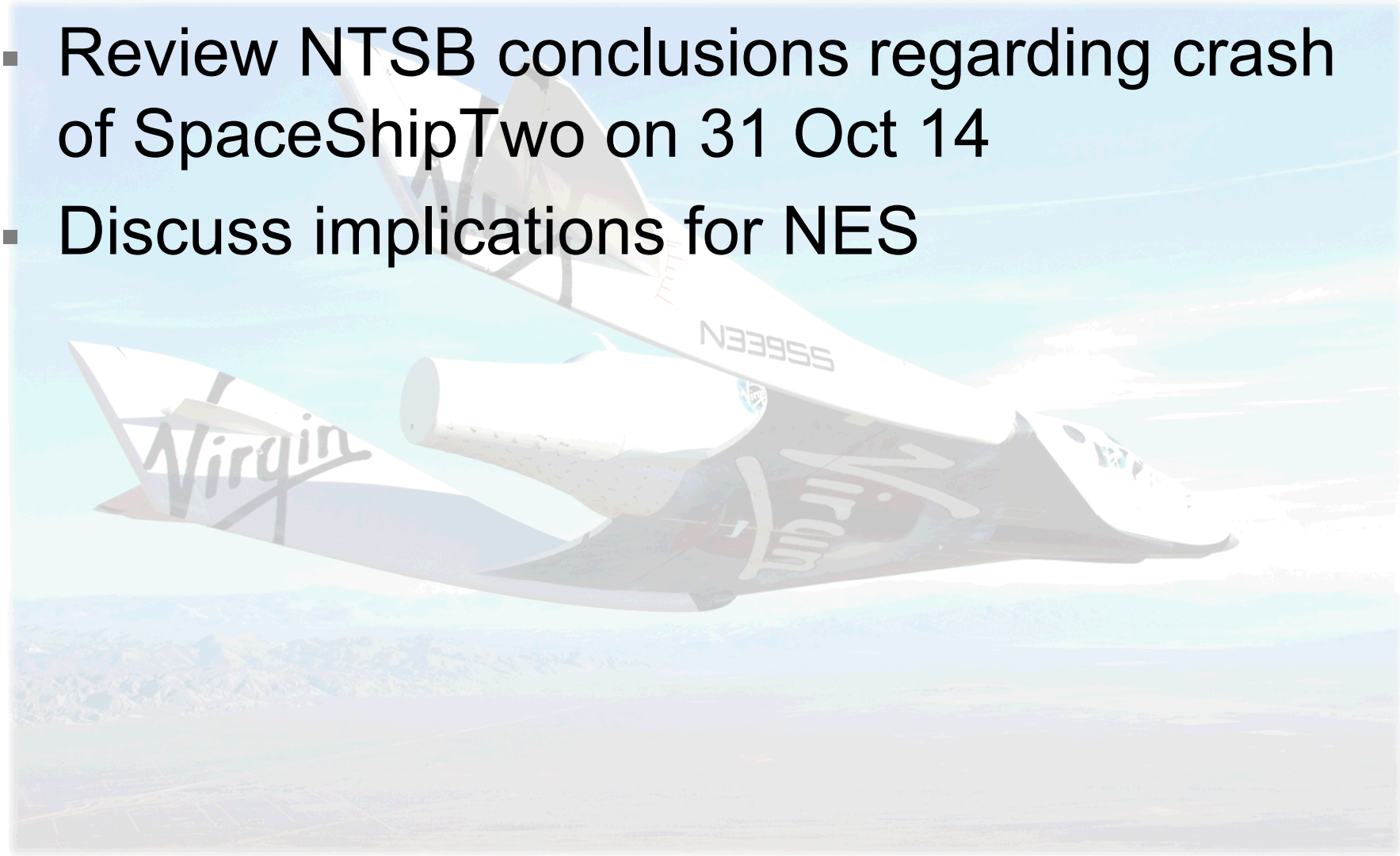
Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. SAND NO. 2011-XXXXP



Sponsored by: NNSA National Nuclear Security Administration

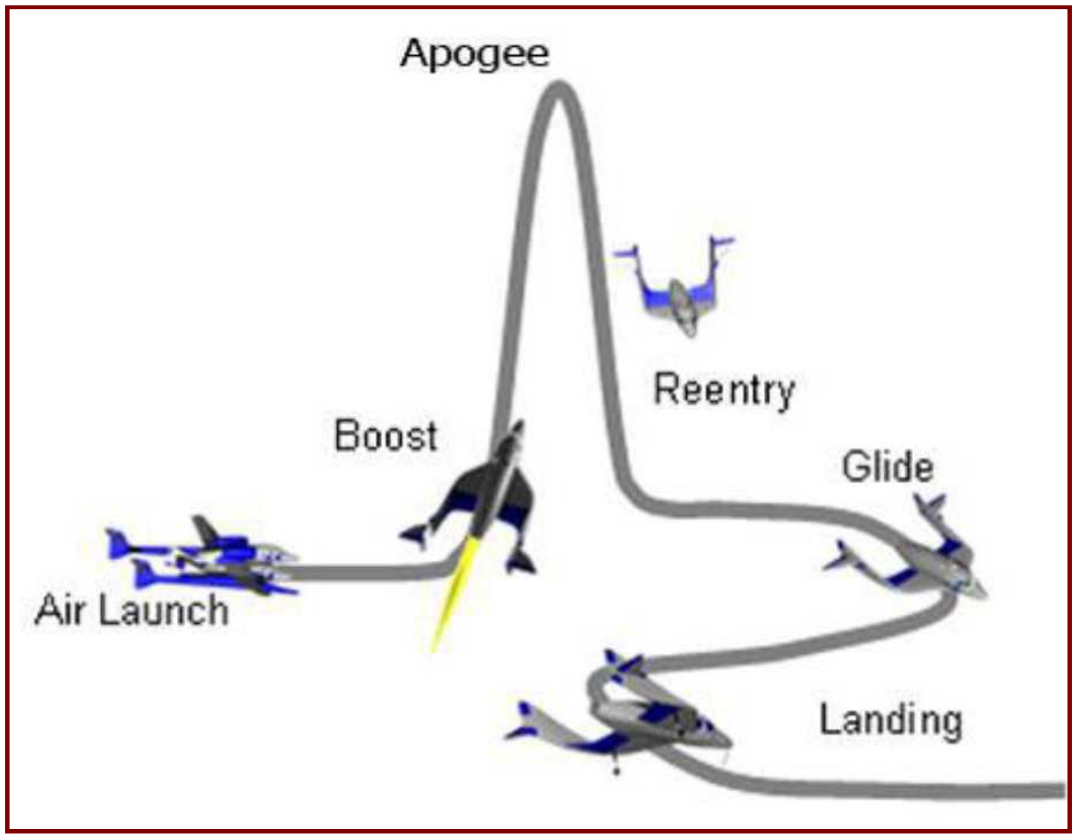
# Purpose

- Review NTSB conclusions regarding crash of SpaceShipTwo on 31 Oct 14
- Discuss implications for NES



# SpaceShipTwo Background

- Reusable rocket for future commercial suborbital operations
- Developed and operated by Scaled Composites for Virgin Galactic

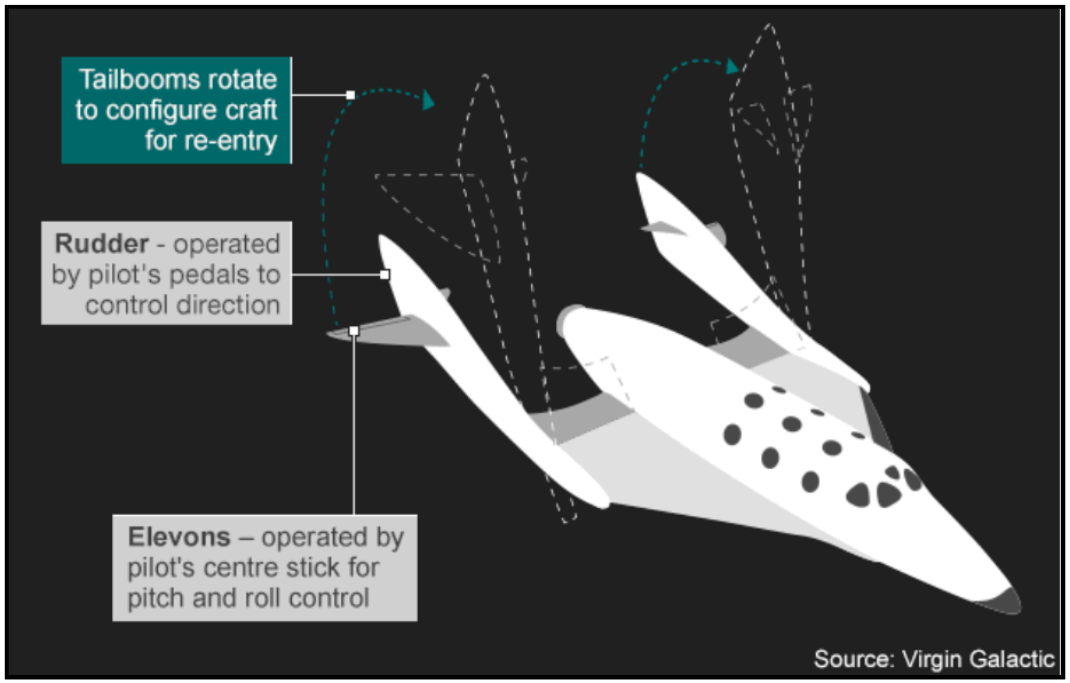



**SpaceShipTwo Design Mission**

- Released from WhiteKnightTwo launch vehicle at about 50,000 feet
- Climb at 2500 mph during 90-second boost phase
- Spend ~10 min at the edge of space (maximum altitude at 70 miles)
  - Weightlessness
  - Views of Earth's curvature
- Re-enter Earth's atmosphere and glide to conventional landing
- 2.5 hours total flight
- Seating for six passengers
- Currently $250k per seat

# SpaceShipTwo Feather System

- Feather system is a critical feature of SpaceShipTwo design
  - Operates a feather flap assembly with twin tailbooms
  - Includes actuators to extend and retract feather and locks to keep feather retracted when not in use
  - Assembly is rotated upward from normal 0°configuration to 60° during reentry in order to increase drag and slow the vehicle




Description

# Co-Pilot Tasks During Boost

## Flight Test Data Card

1. Call out 0.8 Mach

   *to prepare pilot for transonic "bobble" as vehicle accelerates from transonic to supersonic*

2. Call out pitch trim position in degrees as pilot trims horizontal stabilizers to -14°(nose up)
3. Unlock feather at 1.4 Mach

   *to mitigate hazard resulting from lock failure*

- Co-pilot memorized these three tasks
  - Boost is a dynamic and high workload phase of flight, which limits cognitive resources and can cause performance decrements
  - High vibration and loads during boost can generate stress
  - Remember – boost phase lasts only 90 seconds

# SpaceShipTwo Crash Timeline

31 Oct 14

SpaceShipTwo's fourth powered flight test

| Time (PDT) | Event |
|---|---|
| 05:00:00 | Flight crew and test team attended briefing |
| 07:30:00 | Flight crew began preflight inspection |
| 08:15:45 | Pilot and co-pilot entered SpaceShipTwo |
| 09:19:30 | WhiteKnightTwo departed (with SpaceShipTwo mated) |
| 09:58:45 | Co-pilot verified feather lock operation and display indicators |
| 10:07:19 | WhiteKnightTwo launch vehicle released SpaceShipTwo |
| 10:07:26 | Co-pilot called out speed of 0.8 Mach |
| 10:07:28 | Co-pilot unlocked feather prematurely at 0.82 Mach |
| 10:07:32 | SpaceShipTwo broke into multiple pieces and was destroyed |

13 seconds

**Premature unlocking of feather system** → **Uncommanded feather extension** → **Aerodynamic overload in boost phase** → **In-flight breakup of SpaceShipTwo**

# Aftermath of the Crash

- Primary impact site was a 5-mile area near Koehn Dry Lake, CA
  - Smaller pieces of wreckage were found northeast of main site
  - Full wreckage site encompassed area of 33 miles
- Co-pilot Michael Alsbury died
- Pilot Peter Siebold received serious injuries
  - Survived 10-mile fall back to earth
  - Temperatures of -40 degrees Fahrenheit
  - Unable to activate his oxygen system
  - Right arm was broken in four places
  - Collarbone was fractured
  - Debris in his eyes (ice, fiberglass, and pieces of silver)

# Factors Ruled Out as Causes

- Weather
- Crew fatigue and medical/pathological factors
  - No medications 72 hours before accident
  - Negative tests for alcohol and drugs
  - No major changes in health, finances, or personal lives
  - Schedules met new 2014 rest requirements
    - At least 10 hours of rest between shifts
    - Eight hours of uninterrupted sleep
- No feather system anomalies, as revealed during post-accident CT scan and disassembly
- No evidence of structural, system, or rocket motor failures before in-flight breakup in recovered vehicle components

# Primary Cause of the Crash

Albuquerqu

Tuesday, July 28, 2015

NTSB: Crash of SpaceShipT

Scaled Composites simply didn't consider that the crew would make the mistake that occurred. The assumption was that these highly trained test pilots would not make mistakes in those areas.


- Scaled Composites did not consider and protect against possibility that a single human error could lead to a catastrophic hazard
  - Assumed pilots would correctly operate feather system every time at the right time because they were highly trained and experienced
  - This oversight set the stage for the events that unfolded on 31 Oct 14

# Lack of Human Factors

- Scaled focused on feather system reliability and DID NOT emphasize human factors in design, procedures, hazard analysis, or crew training
  - Focused on mitigations for feather system unlock failure, not pilot error
  - Counted on pilots to "do the right thing"
  - Did not design redundancies to minimize human error

*Scaled did not have a human factors department or a dedicated human factors expert on staff*

*Several Scaled engineers and one test pilot had taken a college-level course or had professional experience in human factors*

*Scaled addressed human factors by relying on pilots to identify and resolve ergonomics and human factors issues.*

# Simulator Training

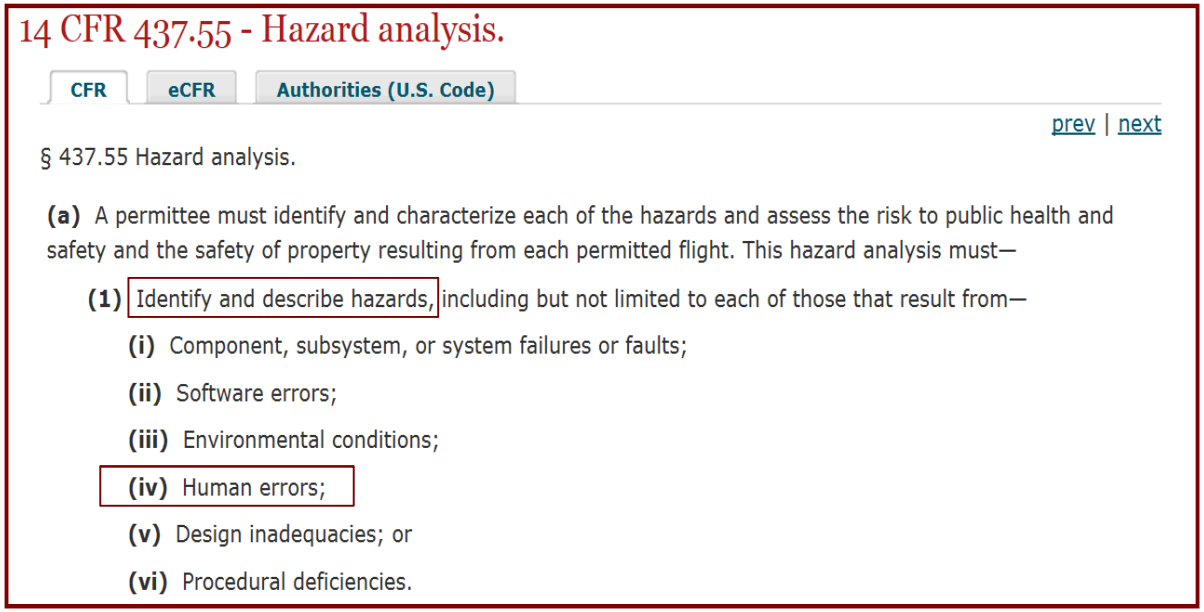
- Fixed-base SpaceShipTwo simulator lacked fidelity in critical areas
  - Did not present realistic vibration and loads of powered flight
  - Did not model uncommanded feather deployment with feather unlocked
  - Force required to unlock simulator feather was reduced
  - Pilots were not required to train in flight gear
- Scaled relied exclusively on training—the lowest mitigation strategy—to address risk of prematurely unlocking feather

*It is difficult to effectively validate training alone as a sufficient measure to fully eliminate occurrence of a single human error because many factors independent of training can influence human performance.*

***~NTSB Report***

# Scaled Hazard Analysis

- Did not identify and describe hazards that could result from human error, as required in 14 CFR 437.55(a)



14 CFR 437.55 - Hazard analysis.

CFR | eCFR | Authorities (U.S. Code)

prev | next

§ 437.55 Hazard analysis.

**(a)** A permittee must identify and characterize each of the hazards and assess the risk to public health and safety and the safety of property resulting from each permitted flight. This hazard analysis must—

**(1)** Identify and describe hazards, including but not limited to each of those that result from—

**(i)** Component, subsystem, or system failures or faults;

**(ii)** Software errors;

**(iii)** Environmental conditions;

**(iv)** Human errors;

**(v)** Design inadequacies; or

**(vi)** Procedural deficiencies.

- Did not identify human error as a failure mode for uncommanded feather operation
- Estimated likelihood of uncommanded feather operation during boost as "extremely remote" at $p = 10^{-6}$

# FAA Experimental Permit Application

- Pre-application process did not begin until after vehicle had been designed and manufactured
- FAA issued initial permit in May 12 and renewed it annually
- FAA reviewed hazard analysis again after first renewal in May 13 and determined it did not comply with human error requirements
- FAA issued a waiver from the requirements
  - Hazard analysis was deemed "sufficiently rigorous" for public safety
  - Scaled did not request the waiver or participate in waiver evaluation
  - Scaled was not asked to modify its hazard analysis or correct areas of noncompliance
  - FAA did not assess mitigation effectiveness or verify Scaled performed mitigations identified in waiver

*FAA evaluations failed to recognize the hazard analysis did not meet regulatory requirements to identify hazards caused by human error.*

# Parachute System

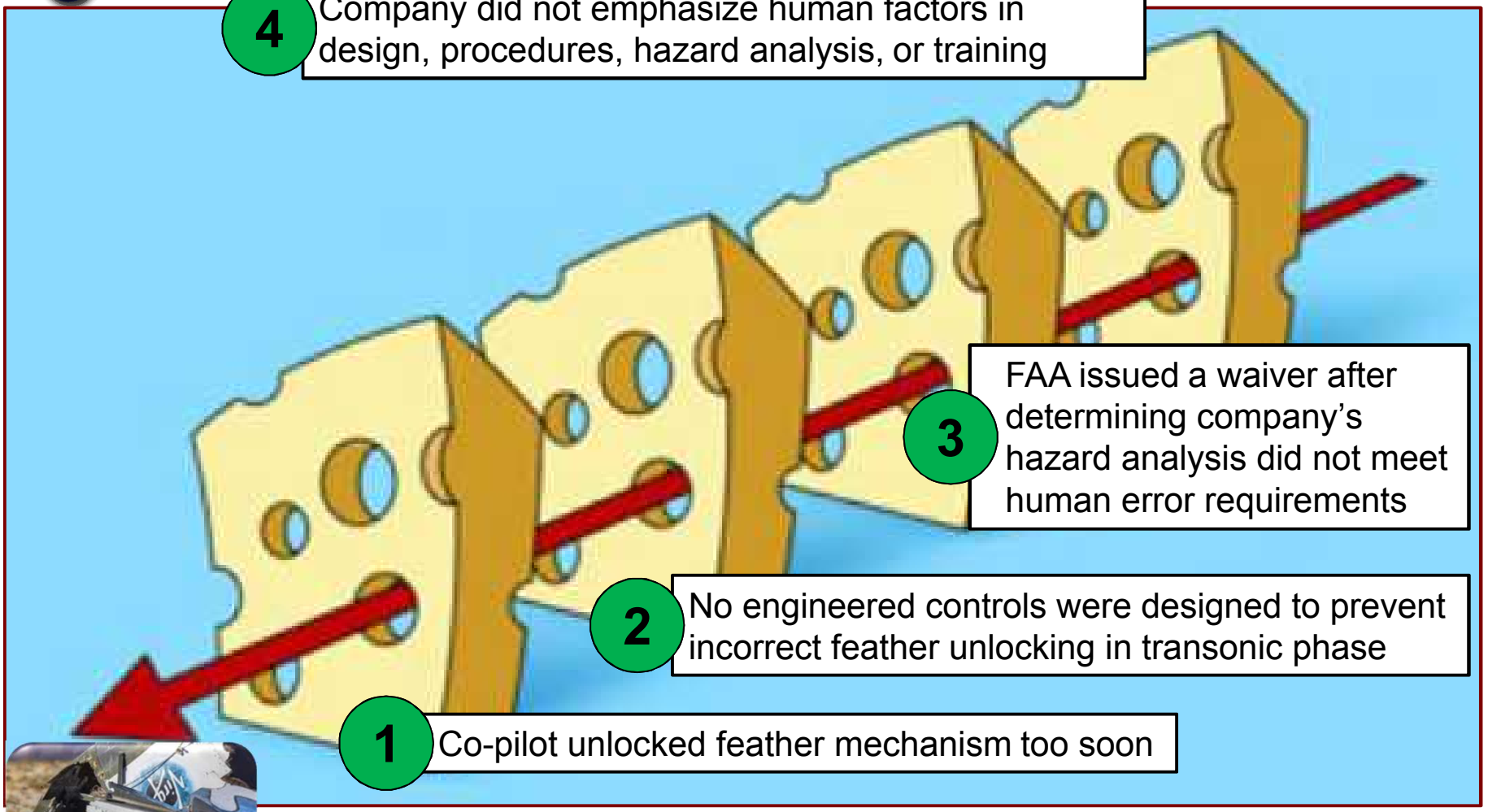
- High-altitude system manufactured by Butler Parachute Systems to slow descent after emergency egress at altitude
  - Oxygen bottle activated by pulling downward on a handle at upper right front parachute harness strap with a force of 37 lbs.
  - User guide originally indicated handle should be pulled with one hand
  - Wording was revised to state both hands should be used
  - Crew either did not receive this update or did not understand it
- Pilot repeatedly attempted unsuccessfully to activate oxygen with his left hand
  - NTSB testing indicated activation force was closer to 55 lbs.
  - Scaled did not have formal hands-on parachute system training
  - There was no specific checklist for preflight examination of parachute

*It is unrealistic to expect pilots to reliably use all features of an emergency system for the first time while involved in a life-threatening situation.* ***~NTSB Report***

# You Can't Make This Stuff Up

- No current guidance specifically for commercial space operators in any of the following areas
  - Obtain human factors expertise
  - Consider human error in hazard analyses
  - Mitigate single-point failures
  - Ensure flight crew is aware of catastrophic hazards that might result from a single human error
- Lessons learned database for commercial space transportation is incomplete—only three entries, all from Aug 10
- Pilot Operating Handbook did not have any warnings, cautions, or limitations specifying risk of unlocking feather before 1.4 Mach

# Reason's Swiss Cheese Model




# Resolutions

*After the accident, Virgin Galactic undertook a comprehensive internal and external program review of SpaceShipTwo design and operations.*

- Developed electromagnetic inhibit device to prevent pilot from inadvertently unlocking/locking feather in critical phases
- Added warning to checklist and pilot operating handbook about consequences of premature feather unlocking
- Implementing challenge/response protocol for safety-critical aircrew actions, including feather lock handle movement
- Conducting comprehensive internal safety review to identify and eliminate catastrophic single-point human performance actions
- No mention of “wait to unlock” or “OK to unlock” indicators

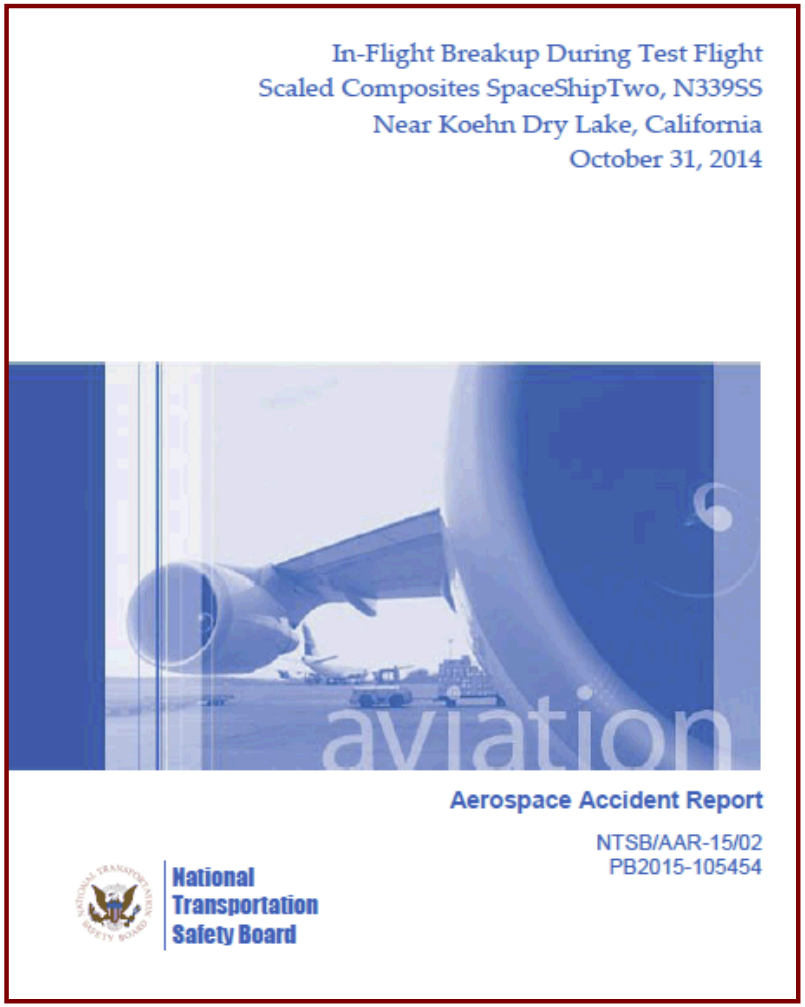
# Conclusions

- One person lost his life and another was seriously injured because their company did not think about human factors
- "Human error" could have been avoided by designing the system to prevent incorrect pilot actions
- Lessons learned from other very similar safety-critical systems were not applied to SpaceShipTwo
- Checks and balances meant to be provided through the experimental permit application process failed
- Human factors is serious business
  - More than just applying common sense
  - More than just asking operators what they want

*How does the NSE compare to Scaled Composites?*

# References

http://www.ntsb.gov/investigations/AccidentReports/Reports/AAR1502.pdf


In-Flight Breakup During Test Flight
Scaled Composites SpaceShipTwo, N339SS
Near Koehn Dry Lake, California
October 31, 2014

aviation

Aerospace Accident Report

NTSB/AAR-15/02
PB2015-105454

National Transportation Safety Board