

Dynamic Non-Events



Adrian Cockcroft
VP Cloud Architecture Strategy, AWS
[@adrianco](#)



“Work in complex systems is bounded by three types of constraints. Economic, workload and safety.”

- Jens Rasmussen

**How did we all non-eventfully
manage to get to this talk?**

(Survivor bias accounts for those that didn't...)

thwest



st.com

First US airline casualty since 2009

Why is flying so safe?

My Visit to the North Pole



My Visit to the North Pole

The screenshot shows a flight tracking interface. At the top, it displays the flight number EK275 and the route from Milan to San Francisco. The main section is titled "Today's Flight" and contains a table of flight details. To the right of the table is a map showing the flight path. At the bottom, there is a Windows taskbar with various application icons and a media player window.

Flight Number	EK275
Route to San Francisco	
Aircraft Type	A380-800
Aircraft ID	A54-OM
Speed	561 mph
Altitude	37,964 ft
Outside Temp	-51° C
Distance Travelled	4606 mi
Time to Destination	8h 27m
Distance to Destination	3666 mi
Time at Destination	05:35
Estimated Time of Arrival	12:02

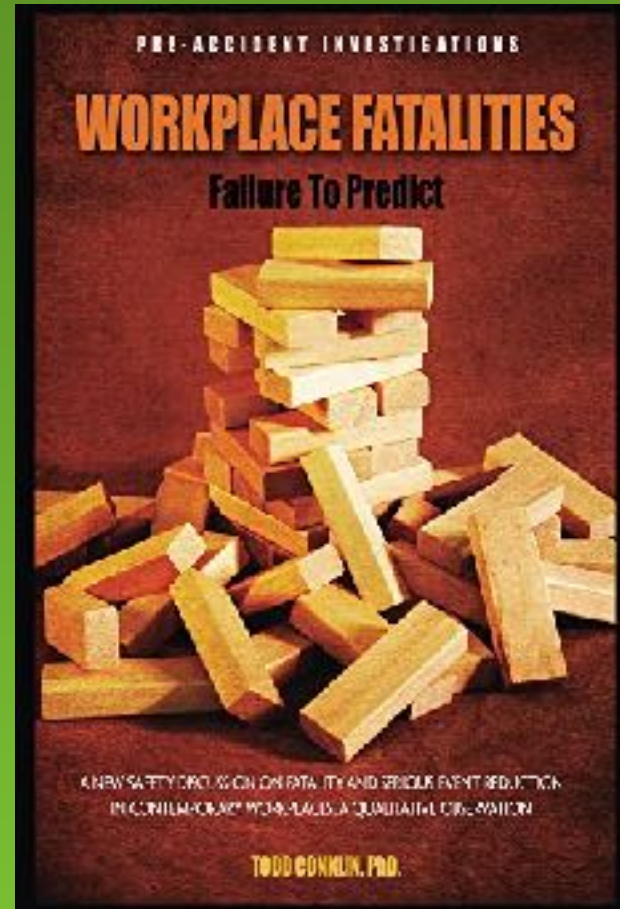
My Visit to the North Pole



Workplace Fatalities

Todd Conklin

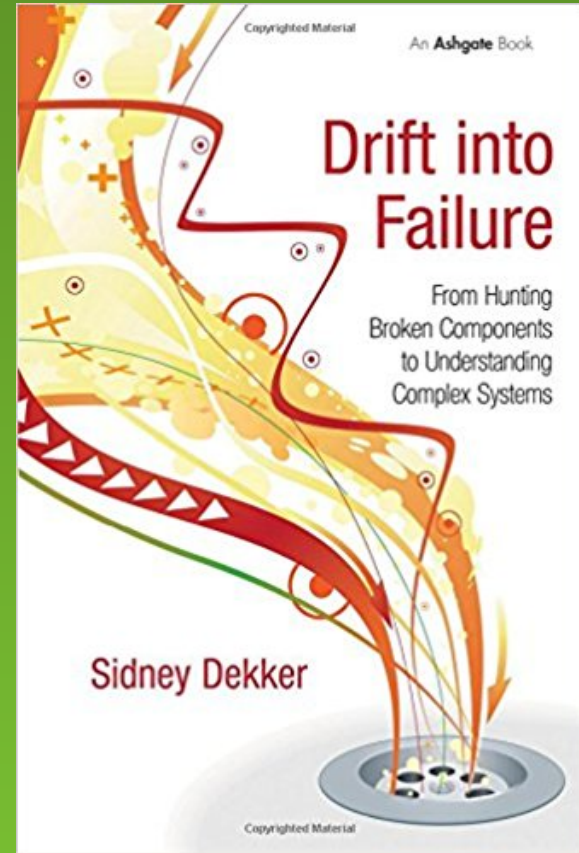
Airlines with the fewest incidents have the highest passenger mortality risk
(Barnett & Wang, 2000)



Drift into Failure

Sidney Dekker

Chapter 2





DC-9, MD-80, MD-90, 717



January 31st, 2000



Alaska Airlines 261



Mexico to Seattle



“Horizontal stabilizer appears to be jammed...”



“We’re going to LAX”



Disengage autopilot



**Aircraft nose pitched down,
dived from 31,000 to 23,000ft**



**Pulled out of dive, pulling hard
to hold it level.**



**Reduced speed, flaps deployed
17,000ft, over the ocean.**



Thumps heard,
then a loud noise



**Nose pitched down,
25° per second**



Rolling, pointing straight down



Inverted



Pilot tried to roll back upright



Both engines stalled



No recovery possible

Hit the ocean, destroyed

**Two pilots, three cabin crew
83 passengers died**

What went wrong?

**2,300 similar aircraft delivered
95 million flight hours**

**This problem had never been
seen before**

95 million non-eventful hours

What went right?

In a dynamic real-world stressed environment, what causes non-events?

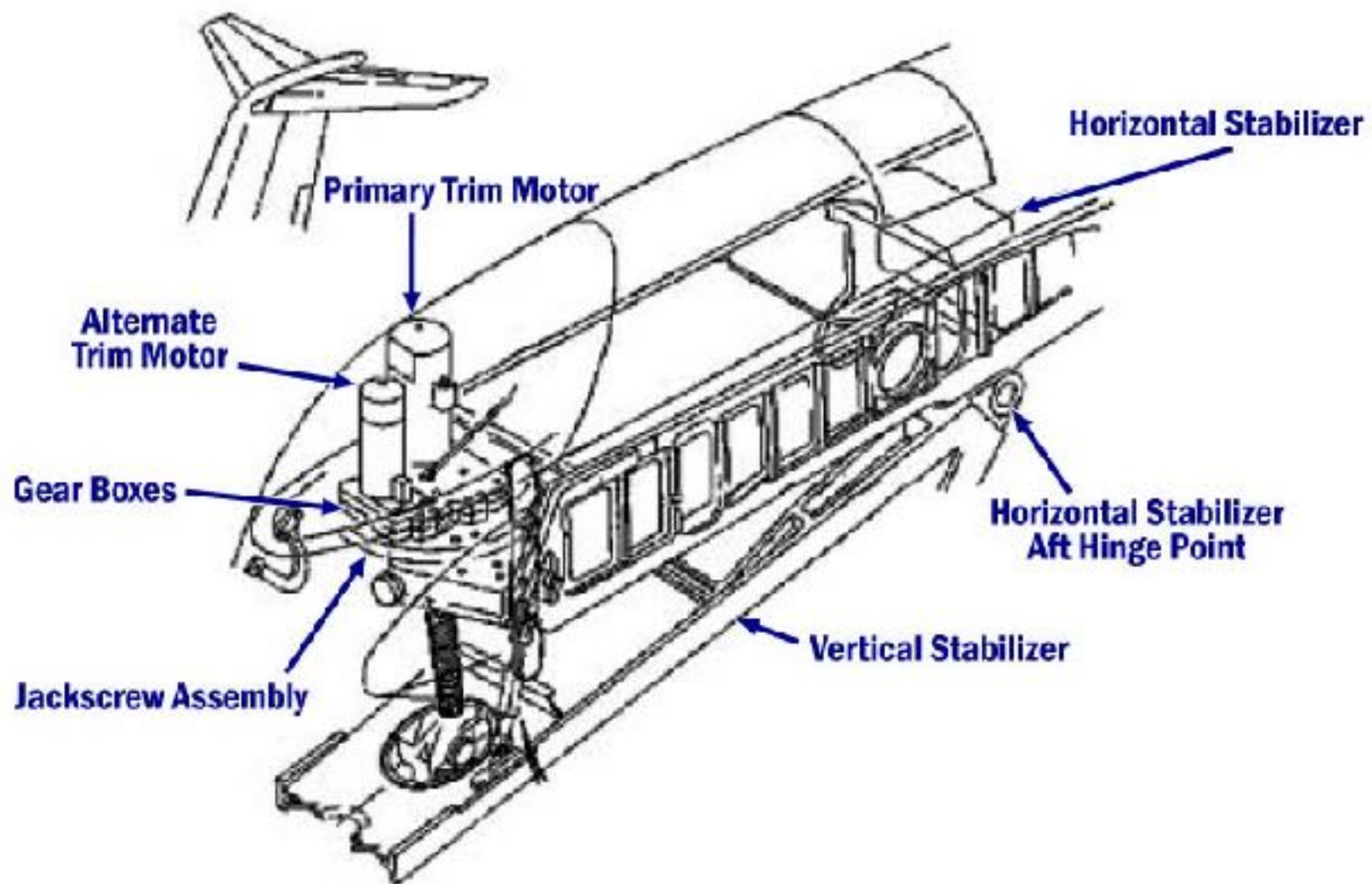
Redundancy

Safety Margins

Inspections and Maintenance

**MD-80 Tailplane has
one jack-screw to
adjust its angle**





**Maintenance, inspection
and lubrication are the
compensating controls**



**The jack screw stripped
its thread and the whole
tailplane jammed with
the leading edge up**



**At first launch of DC-9 in 1965
recommendation to lubricate every
300-350 flight hours**

**Committees, reports, analysis
supported economic push to
longer intervals**

Lubrication Interval

1965 every 350 flight hrs ~2 weeks

1985 Air industry deregulation

1985 every 700 flight hrs

1987 every 1000 flight hrs

1988 every 1250 flight hrs

1991 every 1600 flight hrs

1996 every 8 months ~2550 flight hrs

**Parts recovered from flight 261
showed no signs of lubrication in the
last ~5000 flight hrs.**

Maintenance inspection check

Inspection Interval

1965 30,000 flight hrs design life

1967 problems found, 3600 hrs

1985 air industry deregulation

1985 inspection every 5000 flight hrs

1988 inspection every 26 months

1996 inspection every 30 months

1996 30 months ~9,550 flight hrs

Inspection tolerance

**At the last inspection in 1997
wear was at limit**

**Re-tested a few shifts later, just
under limit**

No maintenance action

“Maintenance often performed at night, in the basket of a lift truck, even in the rain, through two tiny access panels with hardly room for a human hand.”

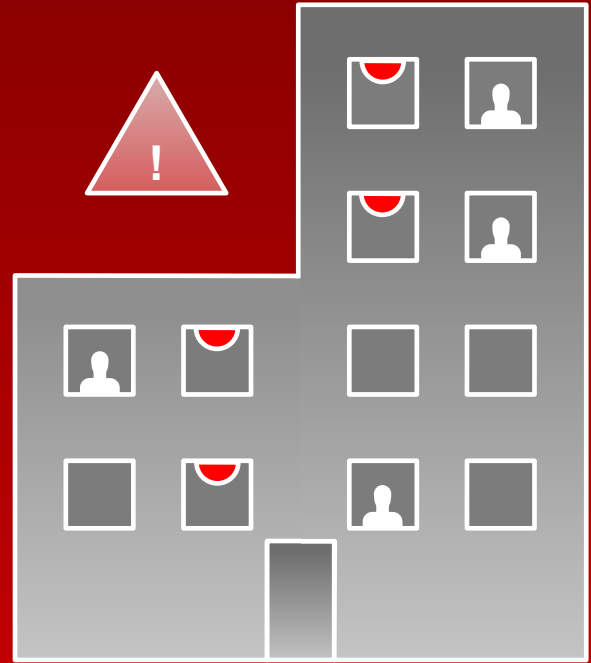
“Using a wear measurement tool that was not calibrated to manufacturer guidelines.”

**With a reporting and learning culture,
humans use intuition and judgement, see
things, fix things, perhaps report things
that might be wrong**

Humans cause the non-events that keep things safely working most of the time

People Training

A fire drill is a boring routine where we make everyone take the stairs and assemble in the parking lot



People Training

Fire drills save lives in the event of a real fire, because people are trained how to react



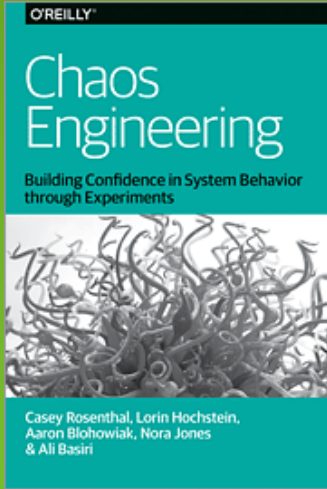
Who runs the “fire drill” for I.T.?

People

Application

Switching

Infrastructure



Chaos
Engineering
Team

People

Application

Switching

Infrastructure

Safety is a dynamic non-event

**To make systems safe, we need to
instrument and study the non-events**

Look for near-misses and outliers

**Beware of drift, from economic and
workload pressure, into unsafe territory**

Forgot to renew domain name...

SaaS vendor

Didn't update security certificate and it expired...

Entertainment site

Datacenter flooded in hurricane Sandy...

Finance company, Jersey City

Whoops!

YOU, tomorrow

Dynamic Non-Events



Adrian Cockcroft
VP Cloud Architecture Strategy, AWS
[@adrianco](#)

Next in this room:
Russ Miles 10:15-11:00
Adrian Cockcroft 11:15-12:00