EMPATHY, COMPLEXITY AND THE BOTTOM-LINE: THE DESTRUCTION OF TRUST AND ENGINEERING EXCELLENCE AT AN AMERICAN ICON

GREGORY TRAVIS

OVERVIEW

- In 1963 Boeing fielded a new airplane, the 737. Marketing had indicated a need for a small airliner particularly suited to operations at modestly-developed airports
  - This drove a requirement that the airplane sit very close to the ground
- Sales were sluggish until the mid-1970s at which point they took off
- In the early 1990s, Airbus fielded a direct competitor – the "fly by wire" A320
- Functionally both aircraft are nearly identical. These machines are commodities where competitive advantages of one over the other revolve around rebates and fuel efficiency
- Fuel efficiency is a function of engine size (larger engines are more efficient)
  - The 737's low stance on the ground makes it extremely difficult to fit large engines under the wing
  - Being competitive with the A320 *requires* that there be found a way to fit ever-larger engines under the wing
- In mid-2010s the tension between the above two points precipitated a collapse of competence at Boeing, resulting in the deaths of 346 people in two separate accidents
  - The chain of events that made those accidents inevitable were set in motion decades before the crashes themselves

ARCHITECTURE

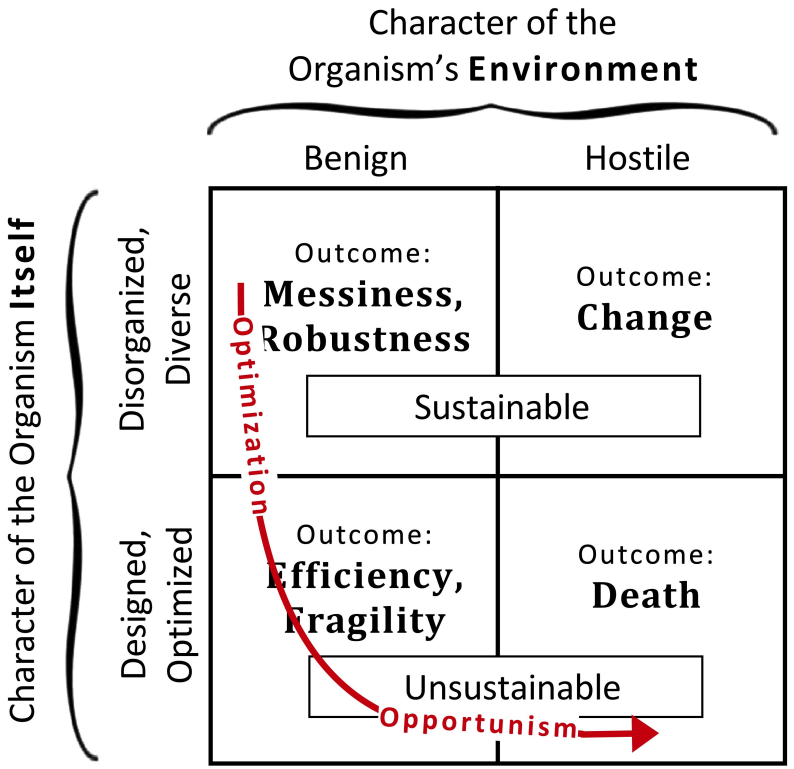
- Architecture is not engineering. It is an expression of shared values and culture
  - *"Any organization that designs a system (defined broadly) will produce a design whose structure is a copy of the organization's communication structure." (Conway's Law)*
- At the core of those shared values are the antagonistic concepts of *efficiency* vs. *resiliency*
  - Aircraft engineering practitioners must architect systems that are both highly efficient and highly resilient. This is extraordinarily difficult to do well: *Simplify, then add lightness*
- A key factor in successfully resilient architectures is corporate management via a sense of shared mission. Shared risk, shared reward. This is called empathy
  - Empathy is expensive and inefficient. It is the process by which value is created
- A key factor in successfully efficient architecture is corporate management via dictation. Bifurcated risk and reward
  - Efficiency is the process by which value is extracted
- All companies contain elements of both resiliency and efficiency. However, the natural evolution of a company typically follows a path of favoring resiliency early (building value) and then (particularly as the company's products become commodities) shifting in favor of efficiency (extracting value)
  - There are some industries where that "natural evolution" is utterly corrosive to the company

COMPLICATED VS. COMPLEX

- A complicated system merely consists of a great number of components, many of which may be identical (example, a brick wall). Complicated systems are easy to understand and inherently resilient (removing a single brick will not cause the entire wall to collapse). Complicated systems are homogenous
- Complex systems also consist of a great number of components, many of which are probably different. Complex systems rapidly become impossible to understand *or predict* and thus become subject to *Normal Failure*. Complex systems are heterogenous

THE 737 SAGA

- Designed in the late 1950s when jet transport was in its infancy
  - Conscious of the dangers of the unknown
  - Risk mitigation (resiliency) primarily through redundancy
  - Complicated, but not complex
- Re-designed continuously as the needs of the company evolved along with the company's transition from a resilient culture to an efficient culture
  - Risk mitigation is inefficient
  - Complex solutions evolve, replacing complicated solutions



Courtesy: Mel Conway

THE RESILIENT 737

- Safety achieved through redundancy
  - Two engines, not one
  - Two sets of flight instruments, not one
  - Two auto pilots, not one
    - None of the redundant systems relied on its twin in any way, nor were they connected to their twins
  - Two pilots
- Fault diagnosis and resolution a human responsibility
- Complex, but not complicated
  - Failure is *not an option*

THE EFFICIENT 737

- New, very large engines, fitted to an aged airframe via a large variety of bandaids/hacks
- Utilization of existing components in new and untried ways by an organization that had lost its ability to understand why those ways would very quickly lead to failure
- Complicated AND complex
  - Failure is *inevitable*

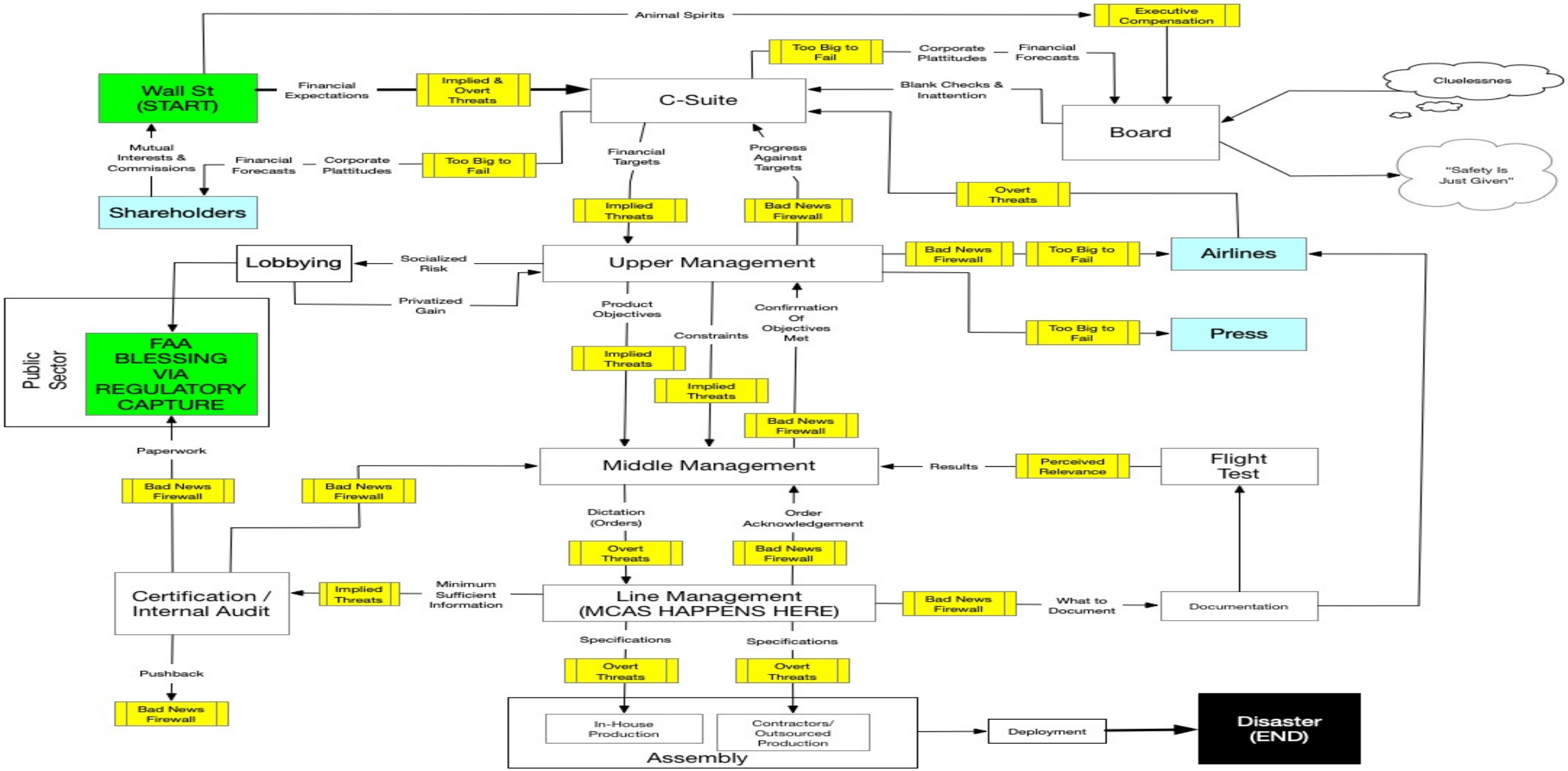
MCAS

- Late in 737 MAX development, it appears that the airframe had an unacceptable tendency to pitch up at high angles of attack
- The new Rockwell Collins Digital autopilot offered a quick and dirty (efficient) solution that could be implemented in software
- The solution relied on using a single angle of attack sensor to trigger a rapid reconfiguration of the horizontal stabilizer "nose down"
  - Angle of attack sensors are notoriously prone to failure
  - The software did absolutely no validation of its inputs
  - The system reacted so quickly that there was no chance a human could intervene
  - Everything about MCAS indicates that it was developed in a state of near-panic
  - No objective observer could have concluded that the system was remotely safe

HOW WAS THAT REMOTELY POSSIBLE AT A COMPANY LIKE BOEING?

- Communication at the company had become entirely ”top down”
  - There was no feedback mechanism from the factory floor(s) to upper management
    - Bad news firewalls were everywhere
  - Upper management was judged and rewarded on only a single criteria: The stock price
    - The Board of Directors was ineffective and unable to govern the company in the company’s long term interests
  - Engineering and design was decoupled from manufacturing, particularly the software aspects
    - No “lunch table chatter”

WELCOME TO THE MACHINE



QUESTIONS

- Why couldn't they just lengthen the landing gear?
- Why didn't anyone in the company see this coming?
- Has it been fixed? Is it safe now?
- I heard this was pilot error. Shouldn't a competent pilot have been able to control the airplane?
- What do you mean by "collapse of competence?"

MORE ON THE SUBJECT

- The Boeing 737 Max FAQ
- How the Boeing 737 Max Disaster Looks to a Software Developer
- Anatomy of a Disaster: Why Boeing should never build another airplane, again
- Ship the airplane: The cultural, organizational and technical reasons why Boeing cannot recover
- The Boeing 737 Max Saga
- Software is killing us