How Complex Systems Fail

Adam Johnson - me@adamj.eu

18th March 2015

Introduction

Me

- Developer/DevOps/DBA/Sysadmin at YPlan

Introduction

Tonight's Paper

- "How Complex Systems Fail" by Richard I. Cook

Introduction

Tonight's Paper

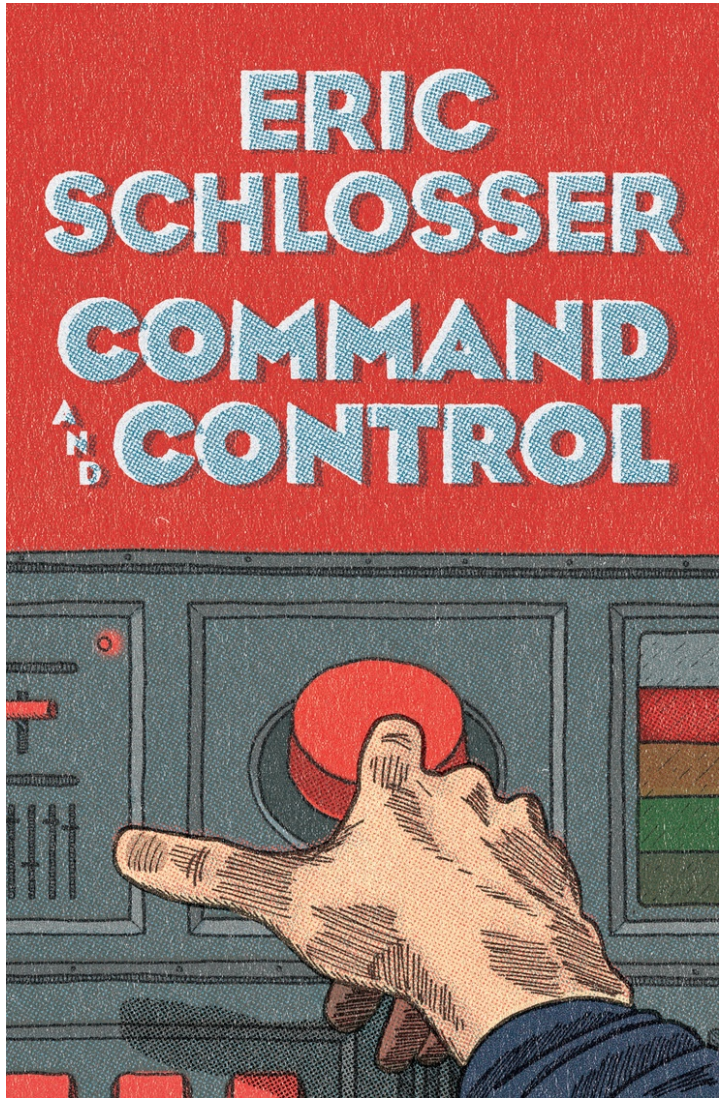
Introduction

This Talk

1. The Paper
2. Computer Systems
3. Nuclear Weapons

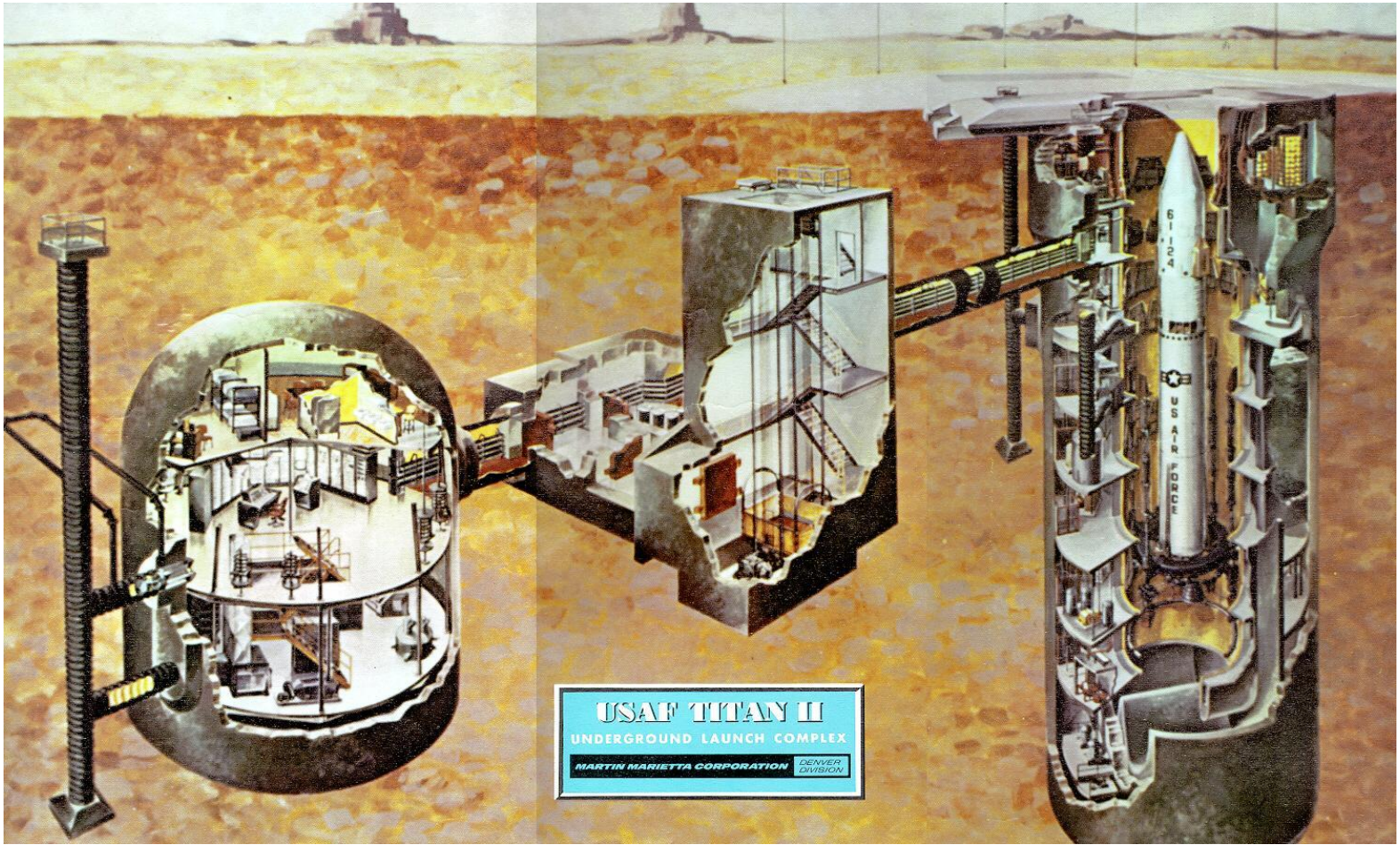
Introduction

Command and Control



Introduction

Launch Complex 374-7, Little Rock Air Base, Arkansas



Introduction

Launch Complex 374-7, Little Rock Air Base, Arkansas

1. Complex Systems are Intrinsically Hazardous Systems

- Part of the definition

1. Complex Systems are Intrinsically Hazardous Systems

Complex vs. Complicated

The Zen of Python states:

- Simple is better than complex.
- Complex is better than complicated.

1. Complex systems are intrinsically hazardous systems.

Complex vs. Complicated

- Complexity is intrinsic.
- Complication is extrinsic.

2. Complex systems are heavily and successfully defended against failure.

- Multiple layers
- *Successful* = survivorship bias?

4/5/6. Complex systems run on the edge of failure

"Catastrophe is always just around the corner"

- There are always latent failures

3/7/8. The Root Cause Fallacy

Post-accident attribution to a 'root cause' is fundamentally wrong.

- Turtles all the way down to the CEO
- Hindsight bias

3/7/8. The Root Cause Fallacy

"Hindsight bias remains the primary obstacle to accident investigation, especially when expert human performance is involved."

9/10. Human operators are producers of and defenders against failure who gamble

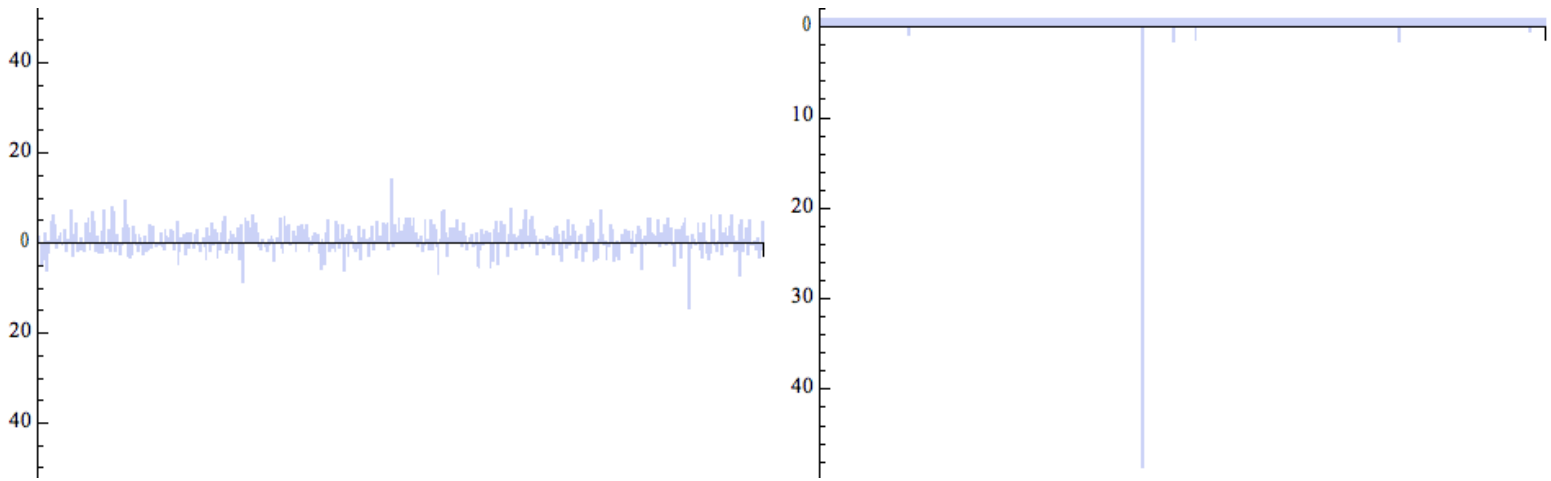
- Unexpected Repercussions
- “Try It”

12/13/17. Human operators are the adaptable, but constantly changing, element

- Celebrate the humanity

14. Change introduces new forms of failure.

- Reducing variability leads to “black swans”



14. Change introduces new forms of failure.

Iatrogenics Harm caused by the healer

16. Safety is a characteristic of systems and not of their components.

- Take the holistic view

16. Safety is a characteristic of systems and not of their components.

The Root Cause Fallacy again.

Conclusion

- Complex systems are hazardous, and run on the edge of failure
- Beware the root cause fallacy
- Value the human element
- Try really hard to not do iatrogenic harm

Thank you

- me@adamj.eu