COSC345 Software Engineering

How Complex Systems Fail

Richard A. O'Keefe

July 11, 2017

References

- "General System Theory", Ludwig von Bertalanffy, 1968.
- "Systems Theory" article at Wikipedia.
- "How Complex Systems Fail", Richard I. Cook, Cognitive Technology Laboratory, University of Chicago, 2000. Read it!
- "How Complex Web Systems Fail", Mathias Lafeldt, Blog "Production Ready", 26 Jul 2016. Read both parts and Cook's response.

What's a *System*?

A system is an entity with interrelated and interdependent parts; it is defined by its boundaries and it is more than the sum of its parts (subsystem). Change in one part of the system affects other parts and the whole system, with predictable patterns of behaviour. Positive growth and adaptation of a system depend upon how well the system is adjusted with its environment, and systems often exist to accomplish a common purpose. (Wikipedia.)

What's a *Complex* System?

If your mental model of the system *has* to be an approximation because of the number or variety of the parts or their connections, it's complex. cat(1) is not complex. Firefox is.

How Complex Systems Fail 1–3

1. **Complex systems are intrinsically hazardous systems.**
   We cannot prevent this. We must *expect* hazards, try to defend and recover.
2. **Complex systems are heavily and successfully defended against.**
   If they (and we) survive. . . Technical means like redundancy and checking; people keeping an eye on this; policies, procedures, rules.
3. **Catastrophe requires multiple failures — single point failures are not enough.**
   Isolated bugs? OK. *Combinations* defeat us.

How Complex Systems Fail 4–6

4. **Complex systems contain changing mixtures of failures latent within them.**
   We *can't* [afford to] fix all flaws. We think remaining ones are minor but are often wrong.
5. **Complex systems run in degraded mode.**
   That is, all complex systems are broken all the time.
6. **Catastrophe is always just around the corner.**
   What if lots of wind turbines are shut down or destroyed by hackers?

How Complex Systems Fail 7–9

7. **Post-accident attribution to a 'root cause' is fundamentally wrong.**
   That is, complex systems fail by *lots* of things going wrong, there is no such thing as *the* cause. We want there to be, and blaming a human is always politically convenient.
8. **Hindsight biases post-accident assessments of human performance.**
   We know *now*, so *they* should have known it *then*. This is spectacularly unrealistic.
9. **Human operators have dual rôles: as producers and as defenders against failure.**
   Before: focus on production! After: why didn't you defend?

How Complex Systems Fail 10–12

10 **All practitioner actions are gambles.**
Practitioner = user/operator. Unlucky gambles get noticed, lucky ones not.

11 **Actions at the sharp end resolve all ambiguity.**
Policies may be vague, but users must do one thing.

12 **Human practitioners are the adaptable element of complex systems.**
Why might driverless cars be a stupid idea?

How Complex Systems Fail 13–15

13 **Human expertise in complex systems is constantly changing.**
Beware loss of institutional knowledge.

14 **Change introduces new forms of failure.**
New features may stress old code (bugs).

15 **Views of 'cause' limit the effectiveness of defences against future events.**
Preparing for the last war...

How Complex Systems Fail 16–18

16 **Safety is a characteristic of systems and not of their components.**
"Rope thinking" *vs* "chain thinking".

17 **People continuously create safety.**
Complex systems work because people nudge them right.

18 **Failure-free operations require experience with failure.**
We'll see this applied on Friday.

Friday

- The topic is Exception handling.
- Inspired by a paper about distributed software failures.
- We shall see that the results in that paper follow from these principles.

Systemantics

There is a very funny book "Systemantics: How Systems Work and Especially How They Fail" by John Gall, Quadrangle, 1977. While funny, it is also painfully true. See the Wikipedia page on Systemantics for a summary and references, and https://www.laetusinpraesens.org/docs/systfail.php for another. This material will *not* be covered in the lecture, but some overlaps with the previous material will be pointed out.

Systemantics Axioms I

- Systems in general work poorly or not at all.
- New systems generate new problems.
- Systems operate by redistributing energy into different forms and into accumulations of different sizes.
- Systems tend to grow, and as they grow, they encroach.
- Complex systems exhibit unpredictable behaviour.
- Complex systems tend to oppose their own proper function.

Systemantics Axioms II

- People in systems do not do what the system says they are doing.
- The system does not do what the system says it is doing.
- A function performed by a larger system is not operationally identical to the function of the same name performed by a smaller system.
- The real world is whatever is reported to the system.
- Systems attract systems people.
- The bigger the system, the narrower and more specialised the interface with individuals.

Systemantics Axioms III

- A complex system cannot be 'made' to work; it either works or it doesn't.
- A simple system may or may not work.
- If a system is working, leave it alone.
- **A complex system that works is invariably found to have evolved from a simple system that works.**
- A complex system designed from scratch never works and cannot be patched up to make it work; you have to start over, beginning with a working simple system.

Systemantics Axioms IV

- In complex systems, malfunction and even total nonfunction may not be detectable for long periods, if ever.
- Large complex systems are beyond human capacity to evaluate.
- A system that performs a certain way will continue to operate in that way regardless of the need or of changed conditions.
- Systems develop goals of their own the instant they come into being.
- Intra-system goals come first.

Systemantics Axioms V

- **Complex systems usually operate in failure mode.**
- A complex system can fail in an infinite number of ways.
- The mode of failure of a complex system cannot ordinarily be predicted.
- The crucial variables are discovered by accident.
- The larger the system, the greater the possibility of unexpected failure.
- 'Success' or 'function' in any system may be failure in the larger or smaller systems to which it is connected

Systemantics Axioms VI

- When a fail-safe system fails, it fails by failing to fail safe.
- Complex systems tend to produce complex responses (not solutions) to problems.
- Great advances are not produced by systems designed to produce great advances.
- Systems aligned with human motivational vectors will sometimes work; systems opposing such vectors work poorly or not at all.
- **Loose systems last longer and work better.**