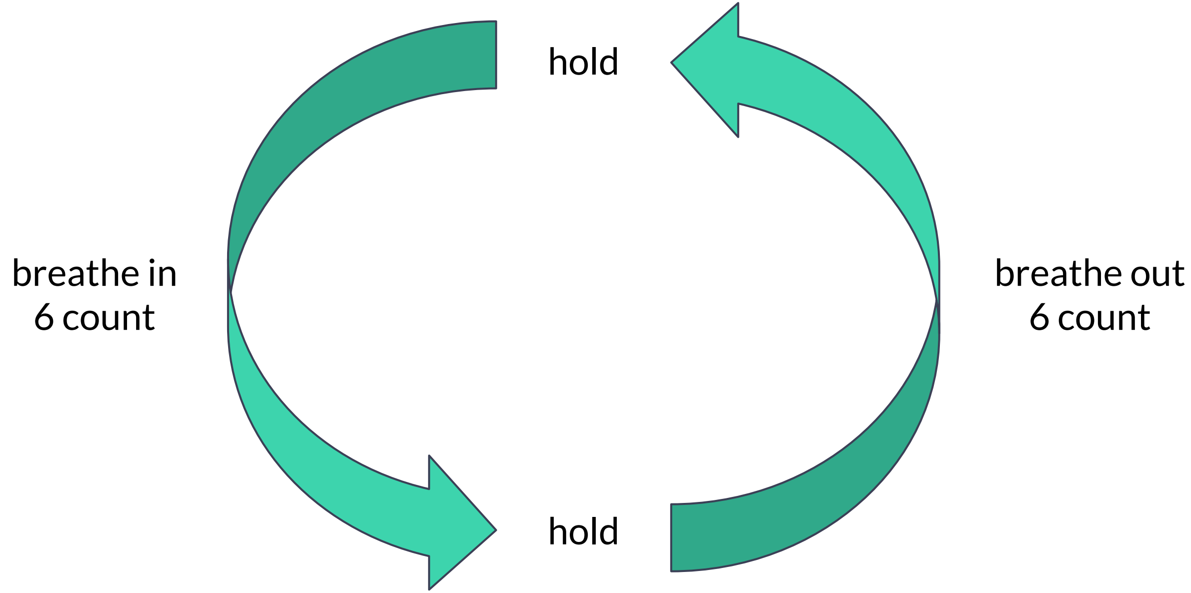
SKILup℠ DAYS

by: DevOps INSTITUTE

The Future of Devops is Resilience Engineering

Amy Tobey
Staff SRE
Blameless
@MissAmyTobey
amy@blameless.com

Prāṇāyāma


hold

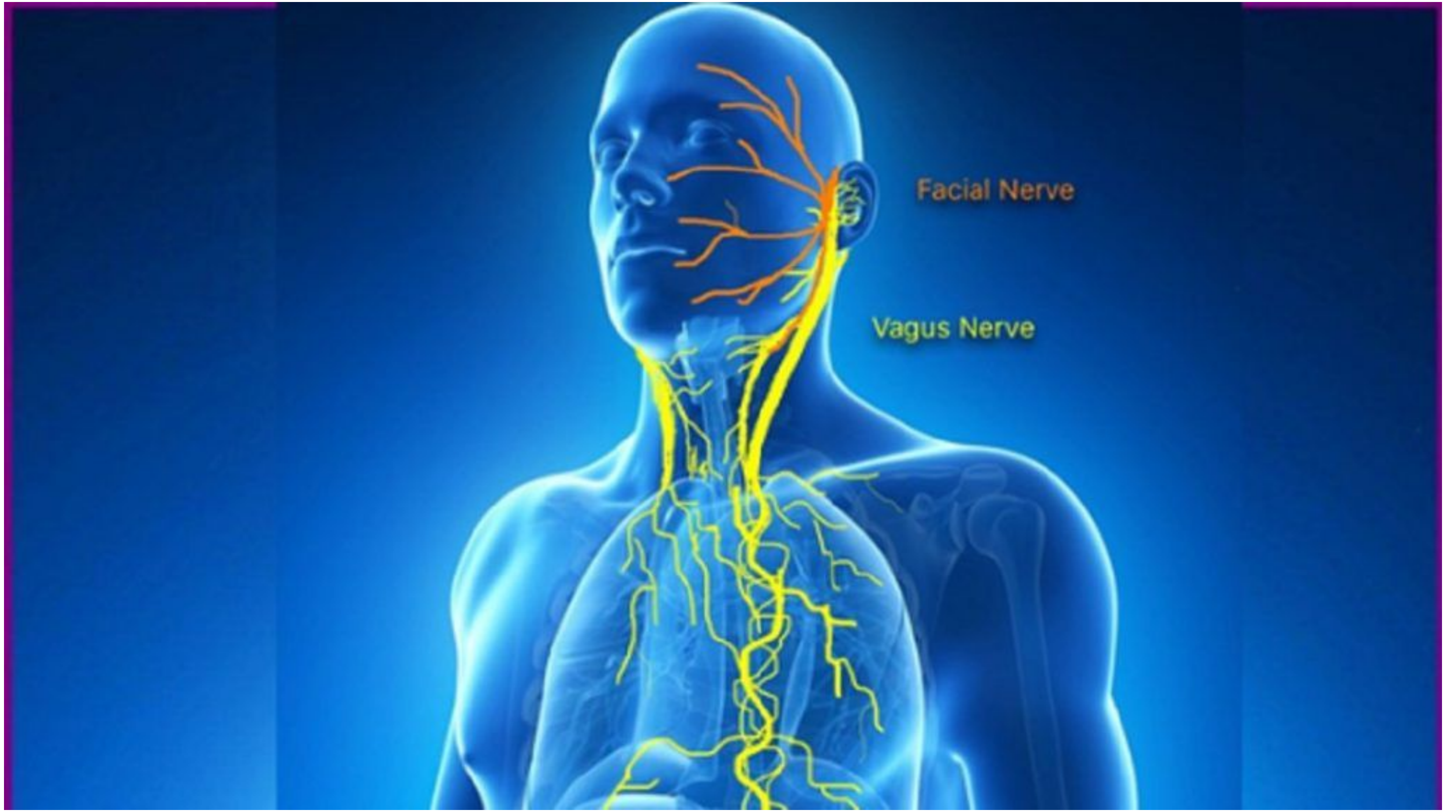
breathe in
6 count

breathe out
6 count

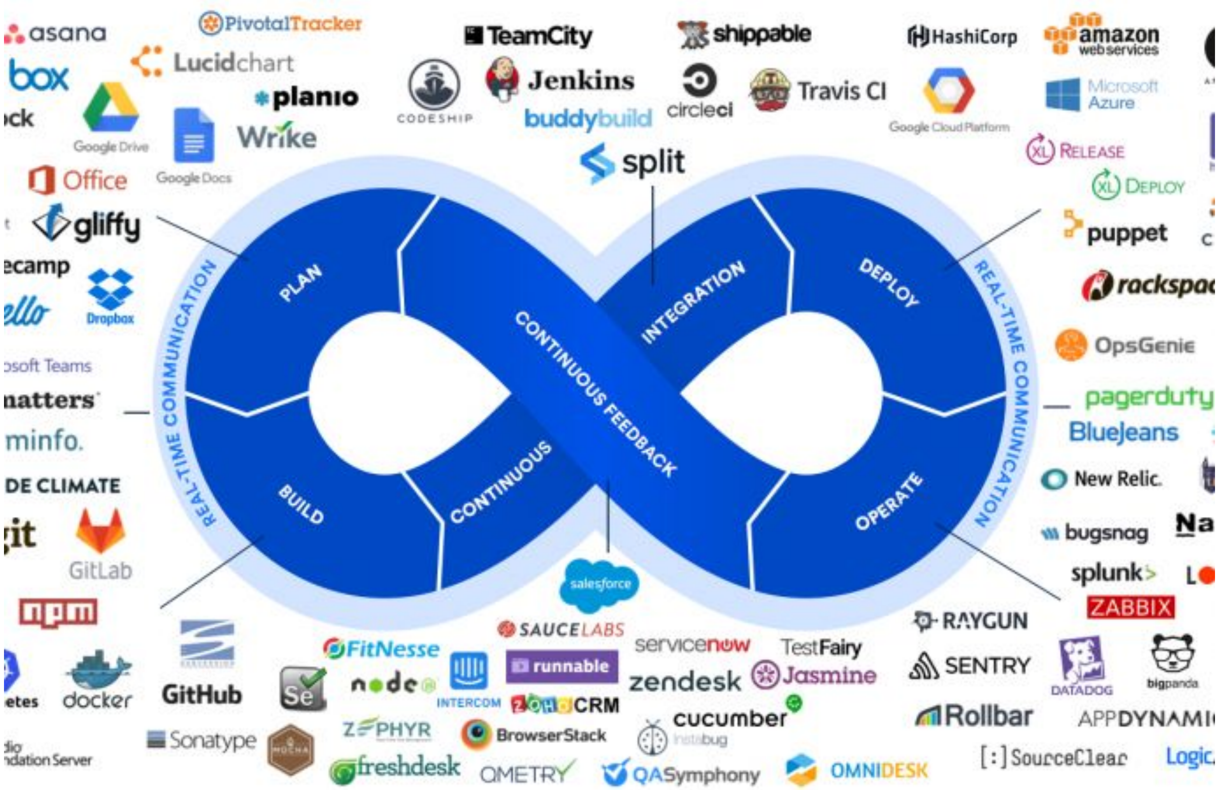
hold

Prāṇāyāma

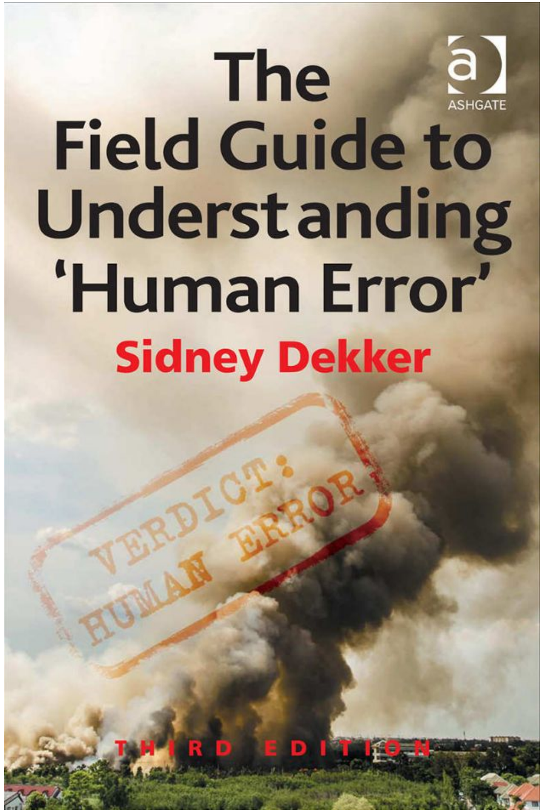
Polyvagal Theory

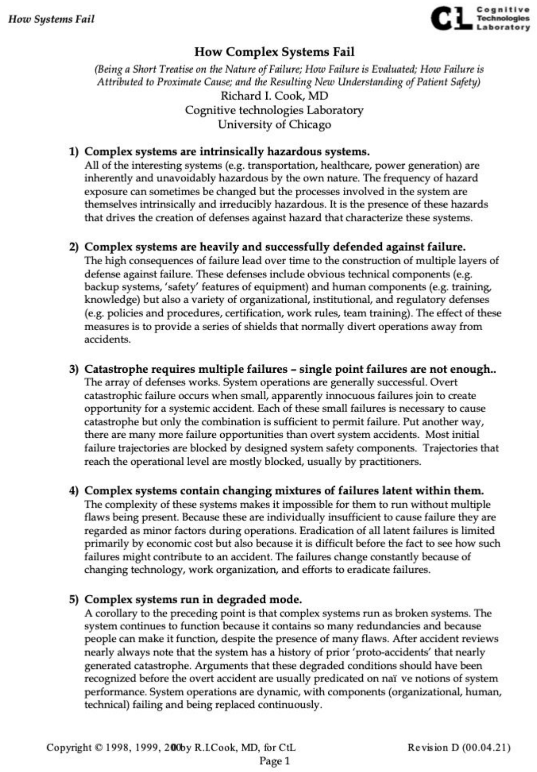


Ancient Practice



Science





How Systems Fail

Cognitive Technologies Laboratory

How Complex Systems Fail

(Being a Short Treatise on the Nature of Failure; How Failure is Evaluated; How Failure is Attributed to Proximate Cause; and the Resulting New Understanding of Patient Safety)

Richard I. Cook, MD
Cognitive technologies Laboratory
University of Chicago

1) **Complex systems are intrinsically hazardous systems.**
All of the interesting systems (e.g. transportation, healthcare, power generation) are inherently and unavoidably hazardous by the own nature. The frequency of hazard exposure can sometimes be changed but the processes involved in the system are themselves intrinsically and irreducibly hazardous. It is the presence of these hazards that drives the creation of defenses against hazard that characterize these systems.

2) **Complex systems are heavily and successfully defended against failure.**
The high consequences of failure lead over time to the construction of multiple layers of defense against failure. These defenses include obvious technical components (e.g. backup systems, 'safety' features of equipment) and human components (e.g. training, knowledge) but also a variety of organizational, institutional, and regulatory defenses (e.g. policies and procedures, certification, work rules, team training). The effect of these measures is to provide a series of shields that normally divert operations away from accidents.

3) **Catastrophe requires multiple failures – single point failures are not enough..**
The array of defenses works. System operations are generally successful. Overt catastrophic failure occurs when small, apparently innocuous failures join to create opportunity for a systemic accident. Each of these small failures is necessary to cause catastrophe but only the combination is sufficient to permit failure. Put another way, there are many more failure opportunities than overt system accidents. Most initial failure trajectories are blocked by designed system safety components. Trajectories that reach the operational level are mostly blocked, usually by practitioners.

4) **Complex systems contain changing mixtures of failures latent within them.**
The complexity of these systems makes it impossible for them to run without multiple flaws being present. Because these are individually insufficient to cause failure they are regarded as minor factors during operations. Eradication of all latent failures is limited primarily by economic cost but also because it is difficult before the fact to see how such failures might contribute to an accident. The failures change constantly because of changing technology, work organization, and efforts to eradicate failures.

5) **Complex systems run in degraded mode.**
A corollary to the preceding point is that complex systems run as broken systems. The system continues to function because it contains so many redundancies and because people can make it function, despite the presence of many flaws. After accident reviews nearly always note that the system has a history of prior 'proto-accidents' that nearly generated catastrophe. Arguments that these degraded conditions should have been recognized before the overt accident are usually predicated on naï ve notions of system performance. System operations are dynamic, with components (organizational, human, technical) failing and being replaced continuously.

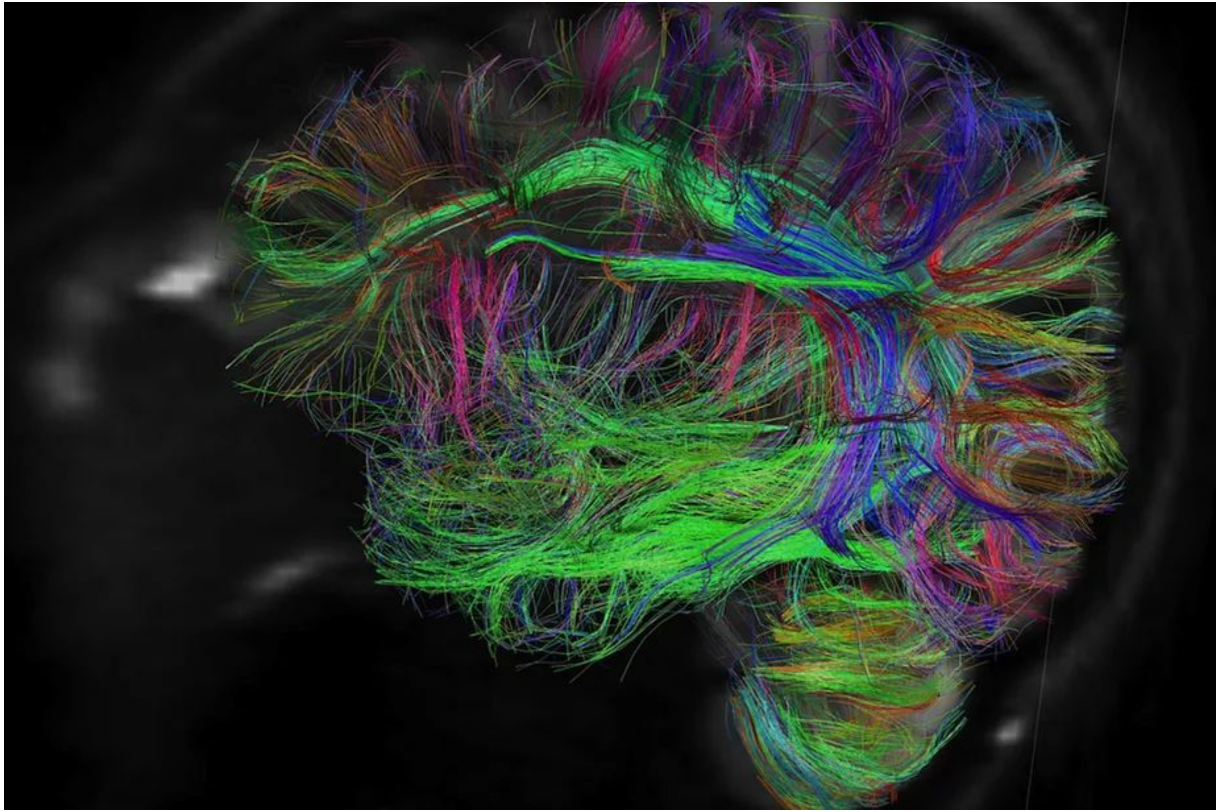
Revision D (00.04.21)
Page 1

It's Gonna Be the Future Soon

socio-technical systems

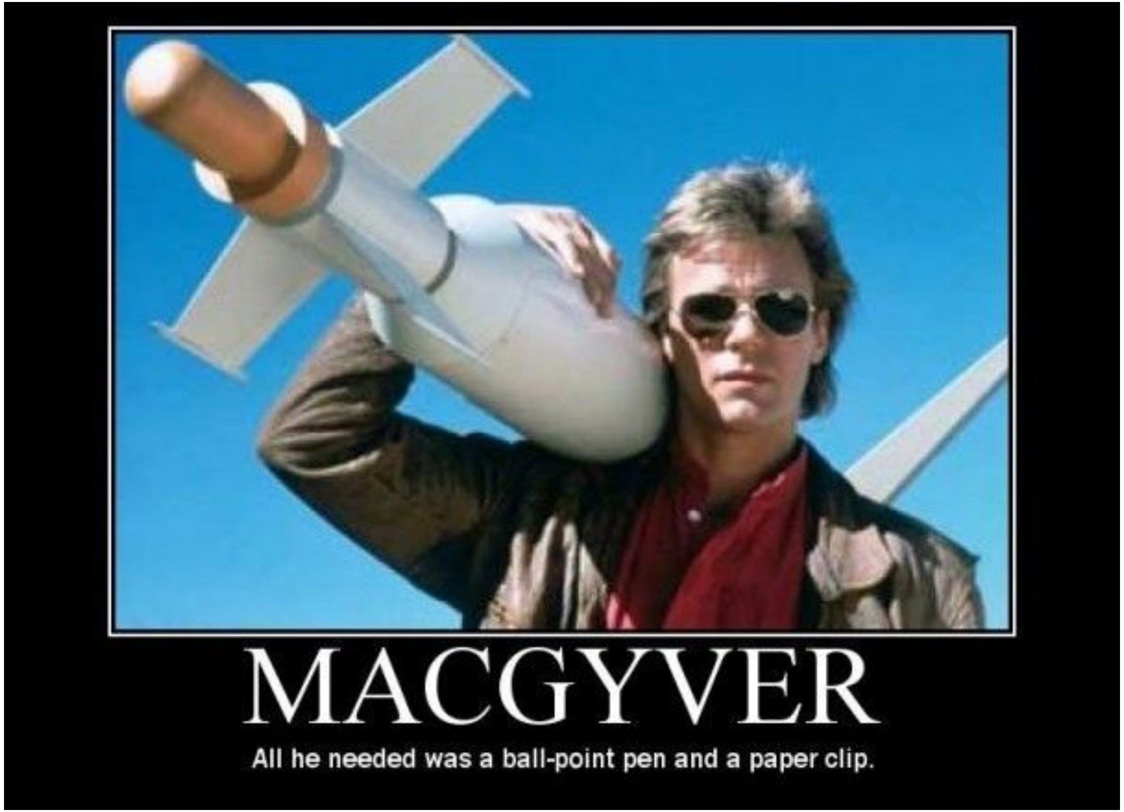
common ground

cognitive capacity



joint-cognitive systems

adaptive capacity



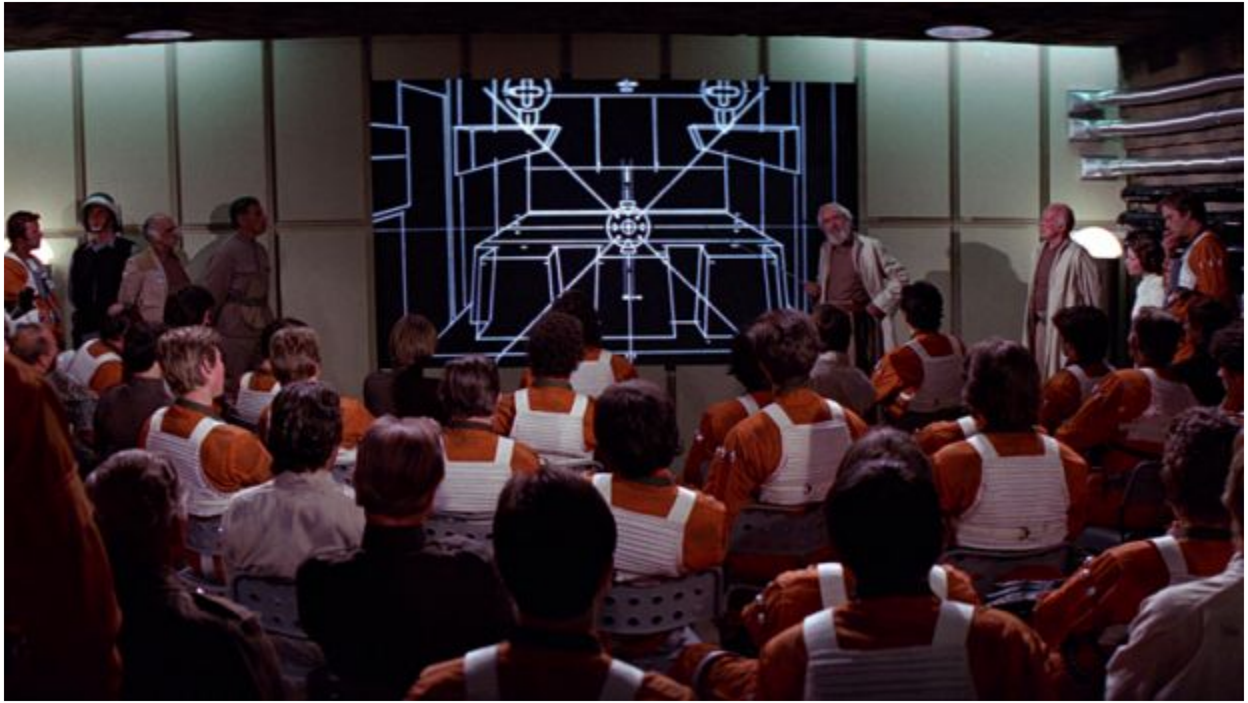
coordinated response

~~human error~~

~~root cause~~

~~learn from failure~~

Once More with Feeling



THANK YOU!

Meet me in the Network Chat Lounge for questions

SKILup DAYS