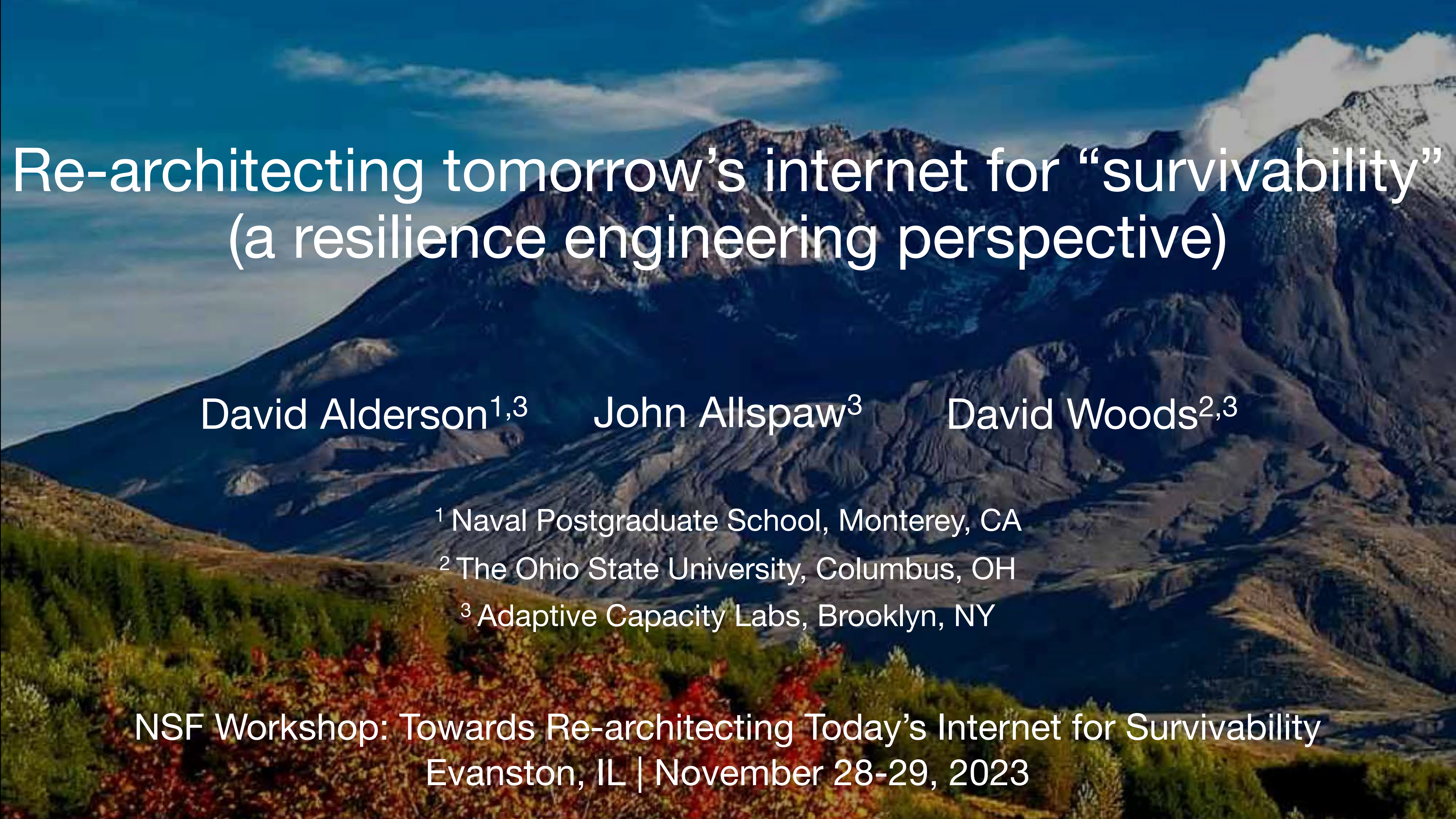


Re-architecting tomorrow’s internet for “survivability” (a resilience engineering perspective)

David Alderson[1,3] John Allspaw[3] David Woods[2,3]

[1] Naval Postgraduate School, Monterey, CA

[2] The Ohio State University, Columbus, OH

[3] Adaptive Capacity Labs, Brooklyn, NY

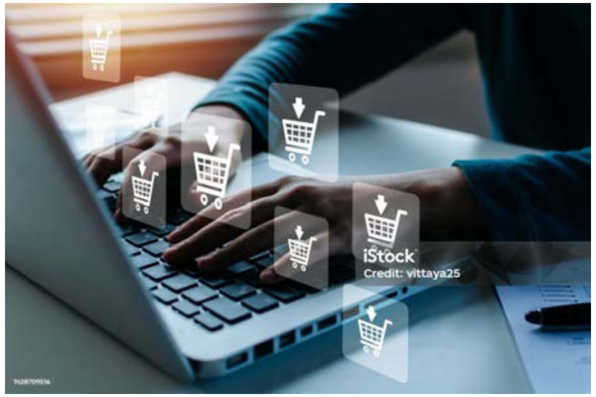
NSF Workshop: Towards Re-architecting Today’s Internet for Survivability
Evanston, IL | November 28-29, 2023

AND NOW FOR SOMETHING COMPLETELY DIFFERENT

> *Over the past decades, the Internet has undergone a major change from being primarily a research-oriented network for academics to becoming a cyber-physical infrastructure "critical" for modern society in general and the global economy in particular.*

Internet function is more than routing!

- all the value-added layers above routing
- an ecosystem of ***critical digital services***



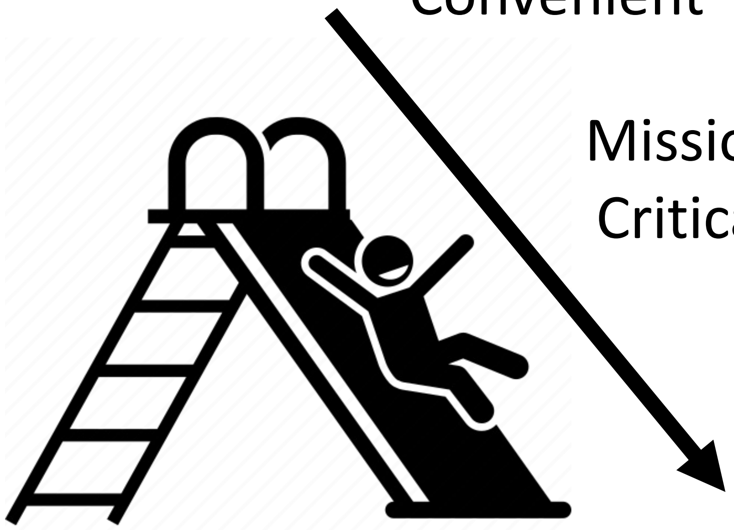
Both transactions + controls!

All the software that enables critical digital services!

"Internet Survivability" in the presence of incidents is MUCH MORE THAN continued routing!

> *This transformation of the Internet into a critical infrastructure has occurred largely by happenstance, rather than by design, and under the assumption that the current architecture that has ensured its robustness in the past would be sufficient to provide the robustness now expected from it.*

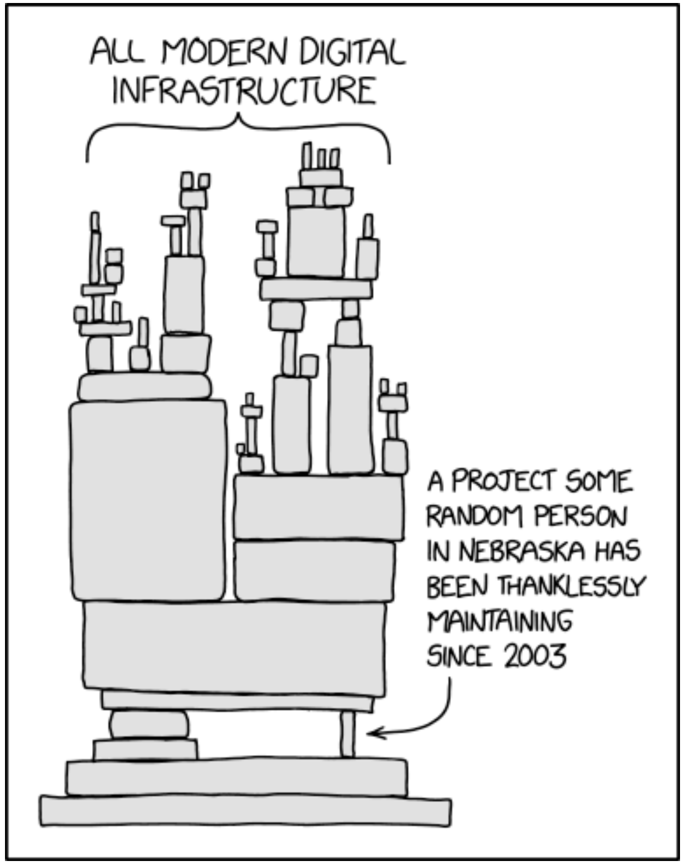
- This transformation is not happenstance, but representative of **patterns in adaptive behavior** found in biology, cognitive systems, economics, engineering, social systems, etc.
- The **“slide-to-criticality”** is not rare, but really the norm



Convenient

Mission Critical

Safety Critical


ALL MODERN DIGITAL INFRASTRUCTURE
A PROJECT SOME RANDOM PERSON IN NEBRASKA HAS BEEN THANKLESSLY MAINTAINING SINCE 2003

> *This transformation of the Internet into a critical infrastructure has occurred largely by happenstance, rather than by design, and under the assumption that the current architecture that has ensured its robustness in the past would be sufficient to provide the robustness now expected from it.*

- This transformation is not happenstance, but representative of **patterns in adaptive behavior** found in biology, cognitive systems, economics, engineering, social systems, etc.

- The **“slide-to-criticality”** is not rare, but really the norm

- **Change is continuous!**
    - Services
    - Dependencies
    - Threats

Impact how saturation, conflict and cascade are presented

- **Real world** provides continuing stream of incidents...
    - **An empirical opportunity** for learning about dealing with complexity
    - Context for **developing theory to understand how resilient systems survive**
    - A platform for **engineering new architectures with adaptive capacity**

> *We argue that this evolved architecture of today's Internet cannot live up to this new role humanity has assigned it or withstand the types of threats that it now faces.*

- **Growing system complexity**—stimulated by new technologies and opportunities
- **New conflicts & threats**—others 'hijack' capabilities for their own purposes
- **Changing environment**—scale of external events, e.g., climate-driven extremes,
- **Changes Tempos of Activity and larger shifts in tempo**

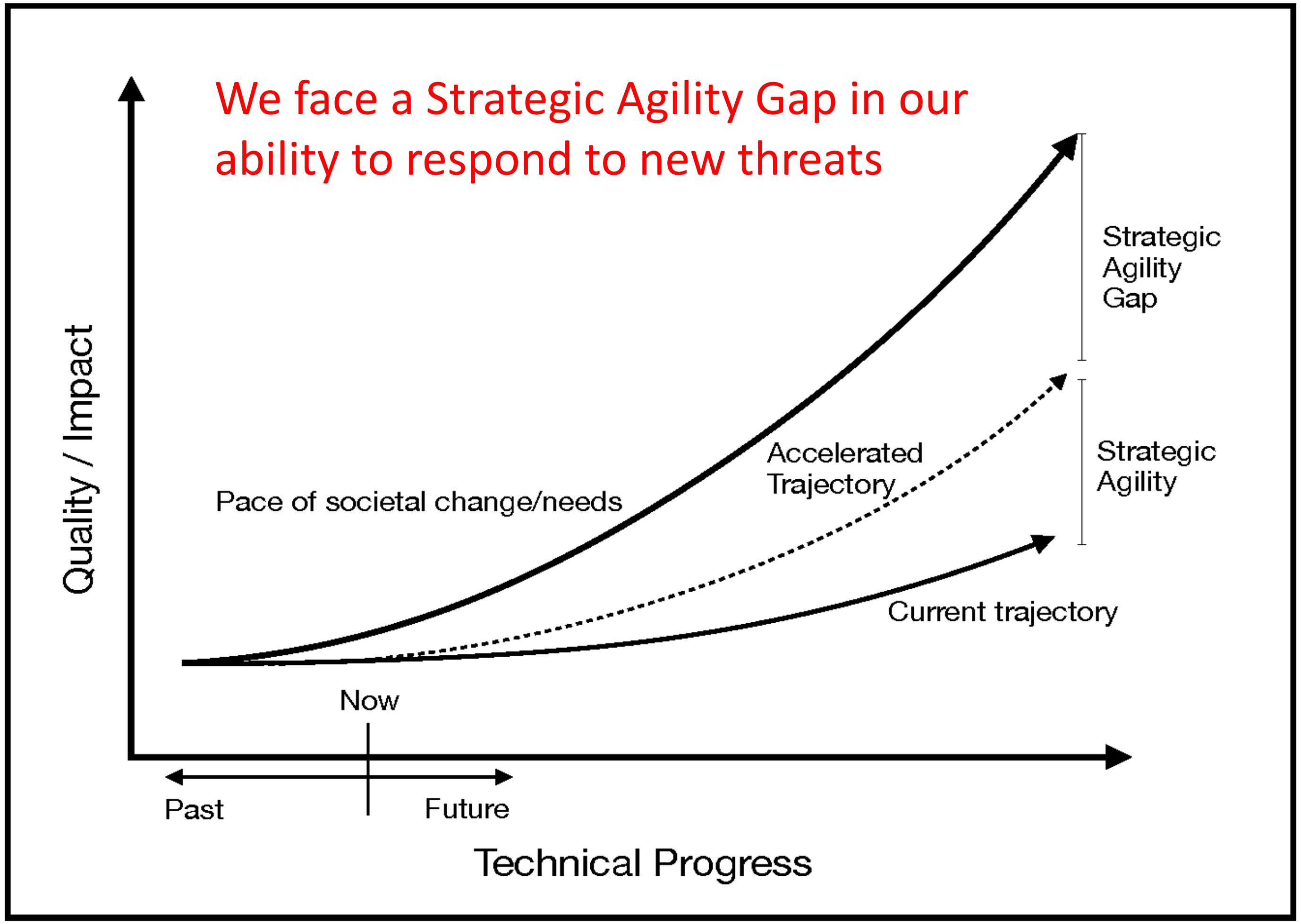
Growth → Complexification

> *We argue that this evolved architecture of today’s Internet cannot live up to this new role humanity has assigned it or withstand the types of threats that it now faces.*

- **Growing system complexity**
- **New conflicts & threats**
- **Changing environment**

Can we learn how to offset changing risks before failures occur as growth continues?

Can we build capabilities to be poised to adapt to keep pace with and stay ahead of the trajectory of growing complexity and the penalties that arise as a result?



References:
Woods D.D., Alderson D.L. (2022). "Progress Toward Resilient Infrastructures: Are we falling behind the pace of events and changing threats?," Journal of Critical Infrastructure Policy, 2(2):5-18. doi: 10.18278/jcip.2.2.2
Woods, D.D. (2020). “The Strategic Agility Gap: How Organizations are Slow and Stale to Adapt in a Turbulent World.” In Journé, B., Laroche, H., Bieder, C. and Gilbert, C. (Eds.), Human and Organizational Factors: Practices and Strategies for a Changing World. Springer Open & the Foundation for Industrial Safety Culture, Springer Briefs in Safety Management, Toulouse France, pp. 95-104 https://doi.org/10.1007/978-3-030-25639-5

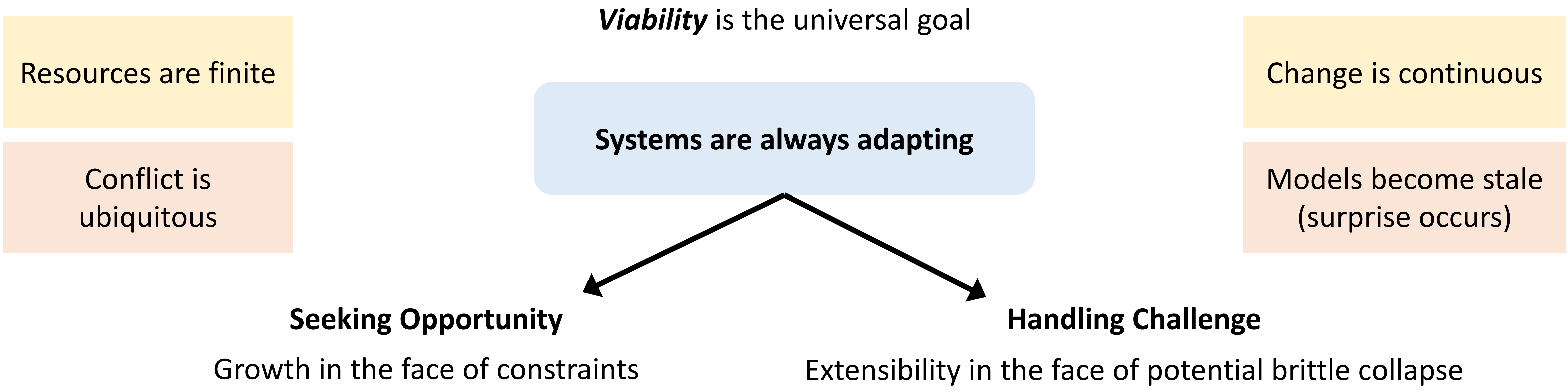
Our Agenda

Today

- Framing Concepts
  - ☑ The Internet is much more than routing!
  - ❑ Challenges for Internet Survivability
  - ❑ How people are currently dealing with it
  - ❑ The Resilience Engineering perspective
- Living Examples
  - ❑ 100% Tracing - Lorin Hochstein
  - ❑ SNAFU - Zoran Perkov
- Plans for tomorrow

Tomorrow

- Depends a lot on today…



Viability is the universal goal

Resources are finite

Conflict is ubiquitous

Systems are always adapting

Change is continuous

Models become stale (surprise occurs)

Seeking Opportunity

Growth in the face of constraints

Handling Challenge

Extensibility in the face of potential brittle collapse

Tangled Layered Networks (TLNs)
arise naturally

“Law of Stretched Systems”
any improvement will be exploited to achieve a new intensity and tempo of activity

Managing Tradeoffs
is fundamental

Robust Yet Fragile (RYF)

“Law of Fluency”
hides the effort required to maintain viability

Risk of saturation
must be monitored and regulated

Synchronization is necessary
among networks of adaptive units

Constraints on maneuver
Shapes the form of adaptative capacities needed

Reference: Woods, D. D. (2018). The Theory of Graceful Extensibility: Basic rules that govern adaptive systems. *Environment Systems and Decisions*, 38(4), 433-457.

Work as imagined (WAI)

- System is built and operated as designed
- Components of the system (humans, algorithms, devices) behave as specified
- Exceptions/Anomalies are relatively few & usually well anticipated.

Work as done (WAD)

- “adaptations tailored to contingencies and context are always going on”
- “The adaptations that make the system function also hide the systems weaknesses.”
- “Management often can’t see the gaps so it seems that the system is functioning as designed.”
- Anomalies and surprises are continuous.

How we imagine incidents happen

- Problems of compliance
- Need to find the root cause
- Can be categorized in a taxonomy, measured, and usefully described with statistics
- Humans are often the problem

How incidents actually happen

- Things are always messy
- Root cause analysis is a fallacy that hides the real problems lurking in system complexity
- Taxonomies often hide rather than reveal; statistics like availability and MTTF are not useful
- Human error as a red herring – (some) people in some roles fill the gaps so that systems work

Reference:
Hollnagel, Woods & Leveson (2006). Resilience Engineering.   Woods et al., Behind Human Error (1994/ 2nd edition 2010). Cook et al. (2009). Minding the Gaps.
Quotes from Woods et al. (2021). Patterns in How People Think and Work: Importance of Patterns Discovery for Understanding Complex Adaptive Systems..

Notions of resilience have become noisy

Four ways that *resilience* is used.

easier to understand ↓ more generality

$\mathbb{R}_1$	***rebound***	return to previous levels of performance
$\mathbb{R}_2$	***robustness***	copes successfully from well-modeled challenges
$\mathbb{R}_3$	***graceful extensibility***	stretches to meet challenges at the boundaries
$\mathbb{R}_4$	***sustained adaptability***	sustains the ability to adapt over cycles of change

modified from Woods DD. Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety* 141 (2015) 5-9.

A Pattern:

- "Computer technology capabilities advance in an organization.

- Stakeholders take advantage of this capability to introduce new services that perform new functions to gain value.

- But these same people know very little about how the service is supplied, what sorts of demands it will not be able to process efficiently, how it is interdependent on other services."

Pattern, continued:

- “When the service was built it was imagined that it would be used in a certain way, even though the service as provided permitted much wider range of uses.

- Developers wrote code that exploited the new service in ways that generated new forms of failure that were unexpected by the authors and for which no defenses existed.

- These uses brought the system to its knees.”

Pattern, continued:

- “After gaining experience with these forms of failure it became clear that the developers who were using the service to run their jobs lacked a deep appreciation of what they were asking the service to do.

- They had no real opportunity to anticipate this, however, because the service was arcane, hidden, and the contextual assumptions about how it would be used were left unstated.”

Rise of High Frequency Trading / Emergence of IEX as a 'Neutral' Exchange

To begin, Requires reference to previous adaptive cycles, to chart ongoing process of adaptation with unseen/ mis-seen reverberations:

- Some people seeking advantage begin to recognize and act to expand opportunities.
- Increased *scale* of operations: finer and multiple time scales; scale of transactions; more variability, more players; and cross-scale interactions matter.
- *Complexity Penalties* increase that produce new forms of gaps, anomalies, conflicts, and surprises.
- New roles arise at multiple layers.
- Partial, incomplete models fragmented over roles. Understanding the changes afoot lags the changes; old models persist long after they no longer apply.
- New goal conflicts arise – value for some comes at costs for others.
- *Anomaly recognition*: Many anomalous behaviors appear which fall outside previous models/experience.
- *Discounting* of anomalies that conflict with past models.

Poised to Adapt

Responding to surprise requires preparatory investments that provide the *potential for future adaptive action.* Model surprise is ubiquitous.

Empirical Laws in Adaptive Cycles

Patterns from studies of people *adapt to cope with complexity*

Discoveries

Fundamentals that explain the phenomena – *Graceful Extensibility*

Capabilities

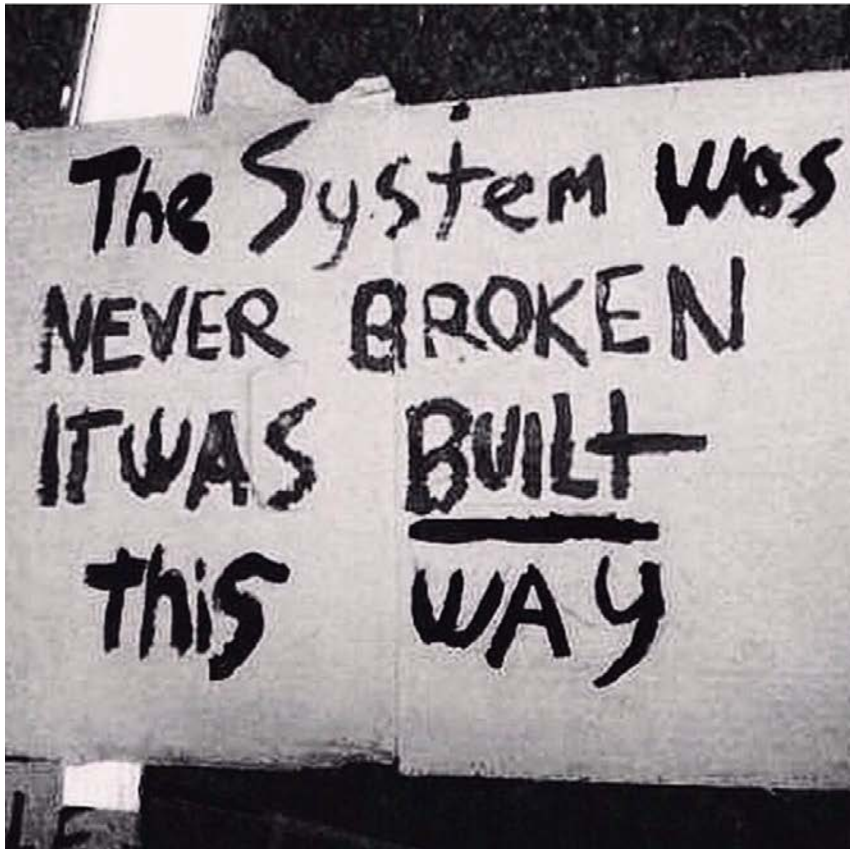
Different paths for pragmatic action – New Architectures

Outmaneuver complexity penalties

Operating in Seas of Complexity

places where surprise is tangible

Systems are Messy
(some) people provide necessary extensibility to overcome brittle systems



Finite Resources / Change

Pressures

SNAFU is normal

Poised to Adapt

05

SNAFU CATCHERS

SNAFU is the natural state of systems

SNAFU CATCHERS

Consortium for Resilient Internet-Facing Business IT

THE OHIO STATE UNIVERSITY

Industry and Research partnership

Studying how critical digital services cope with complexity

KeyBank

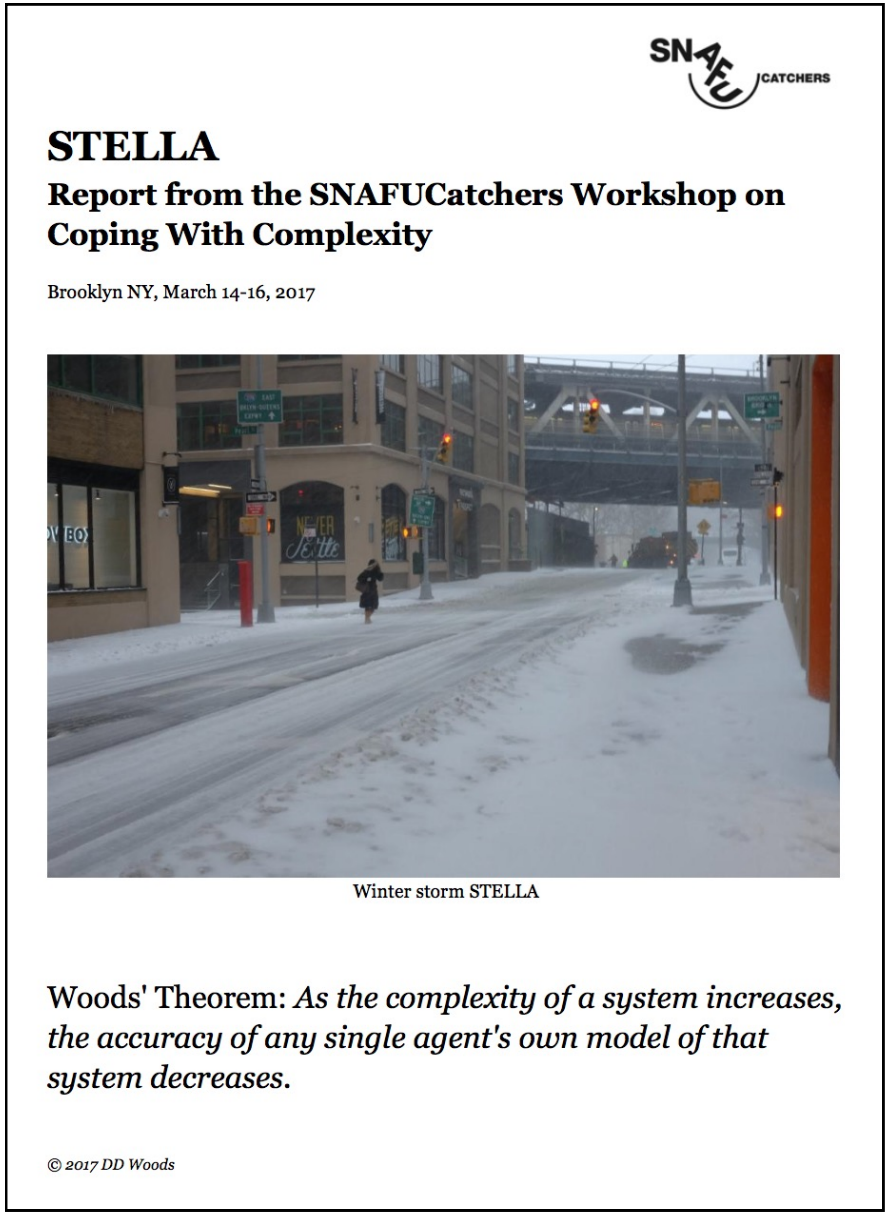
New Relic.

salesforce

IBM

iex

Etsy



SNAFU CATCHERS

STELLA

Report from the SNAFUCatchers Workshop on Coping With Complexity

Brooklyn NY, March 14-16, 2017

Winter storm STELLA

Woods' Theorem: *As the complexity of a system increases, the accuracy of any single agent's own model of that system decreases.*

http://stella.report

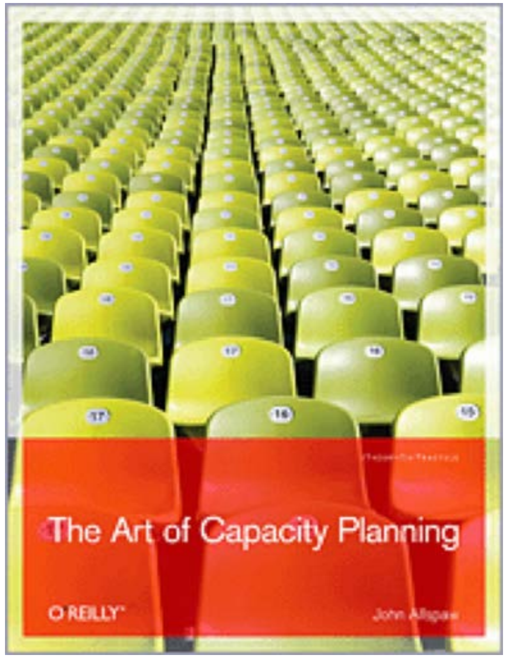
Industry - Academia Consortium

- **Postmortems as re-calibration**
- **Blameless v. sanctionless after action actions**
- **Controlling the costs of coordination**
- **Visualizations during anomaly management**
- **Strange Loops**
- **Dark Debt**

multi-party interdependencies

flickr

Etsy

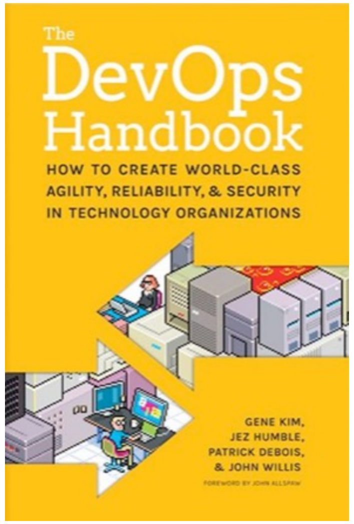


LUND UNIVERSITY

DevOps as Paradigm Shift

circa 2008-2010…

- realization that software cannot be built “correctly” — it must be *operated*
- no crisp boundary between ‘application developer’ and ‘systems engineer’ roles



https://tech-talks.code-maven.com/ten-plus-deploys-per-day.html

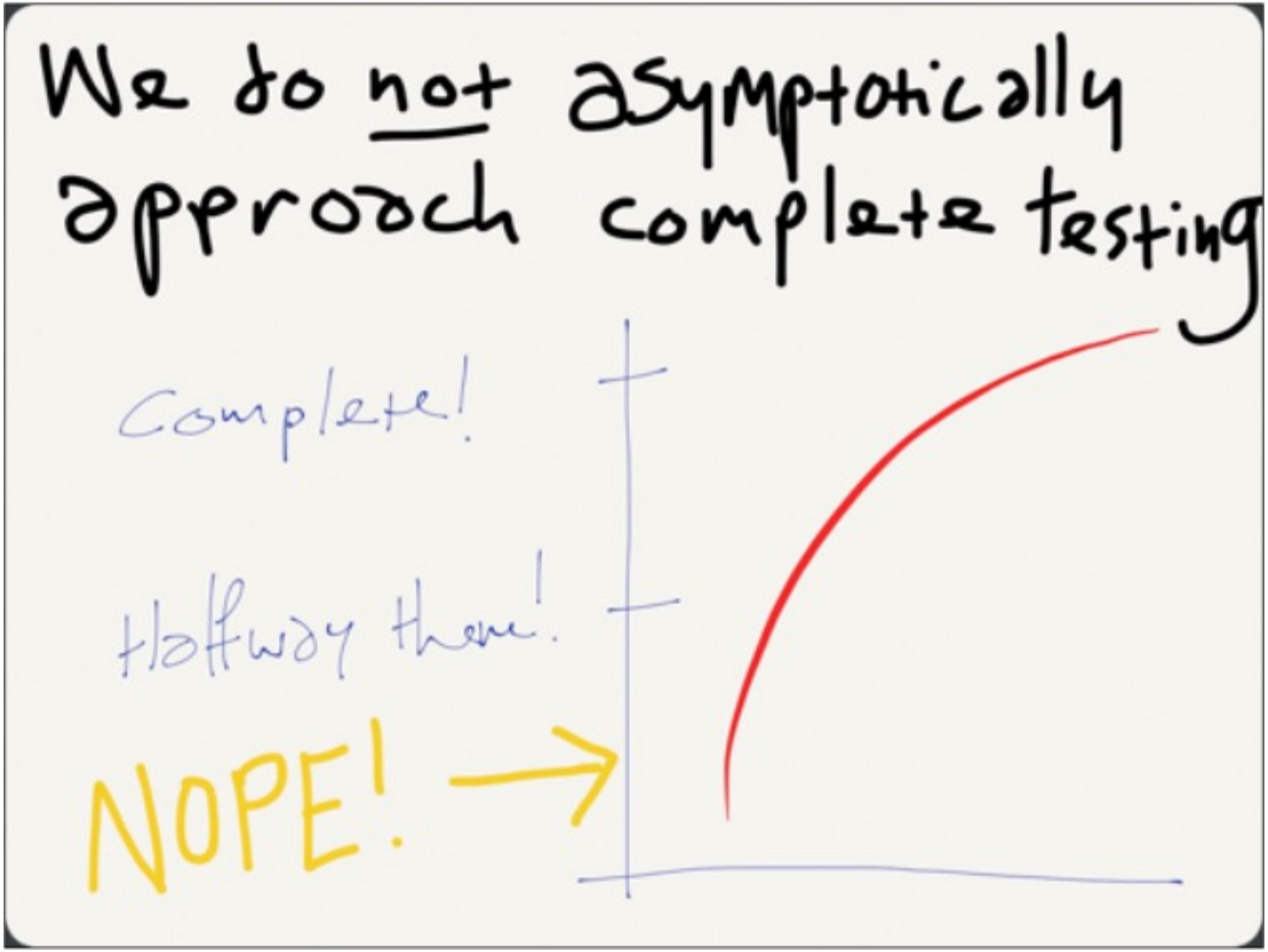
Continuous Deployment/Delivery

An acknowledgment that how software behaves in the *real world* cannot be predicted or anticipated comprehensively.

Continuous Deployment/Delivery

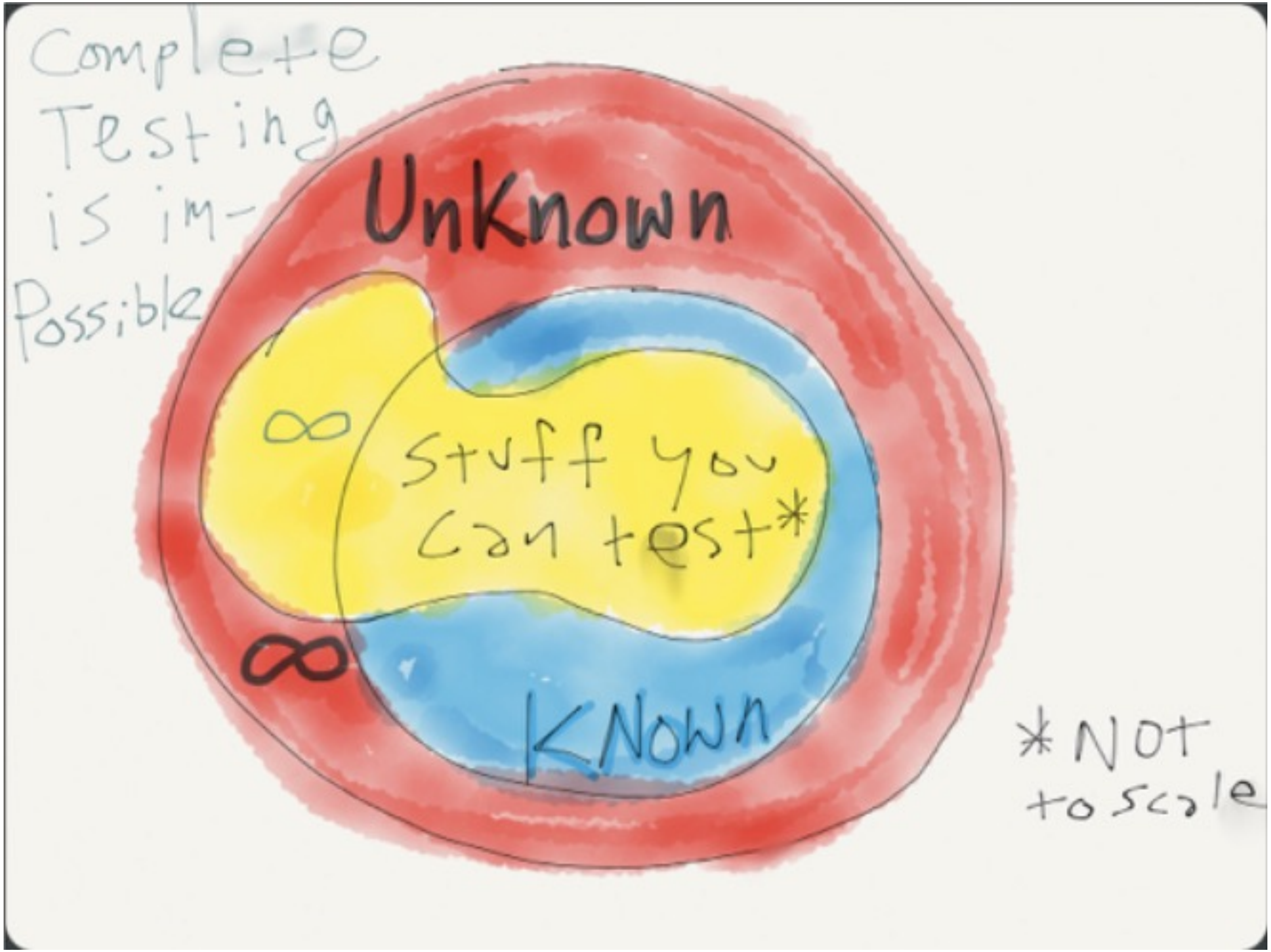
Fueled by a collection of hedging strategies

- ‘small’ changes made frequently >> ‘large’ changes made rarely
- feature flags, config flags
- % rollouts
- allow/block lists
- staff-only
- application and system-level telemetry



We do not asymptotically approach complete testing

"The Invisible Art Of Software Testing" - Noah Sussman, talk presented at AST, 2014



"The Invisible Art Of Software Testing" - Noah Sussman, talk presented at AST, 2014

if we *try* to be comprehensive in test,
you’ll be too slow and unable to keep pace

testing is ***necessary***, but ***insufficient***

No software survives first contact with production.

Preventative designs have real and consequential limits — surprises are *guaranteed!*

Therefore: investments have to be made — *ahead of time* — to support people responsible for handling those surprises

adaptive capacity

A system's capacity to adapt to challenges ahead, when the exact challenge to be handled ***cannot*** **be specified completely in advance.**

unforeseen

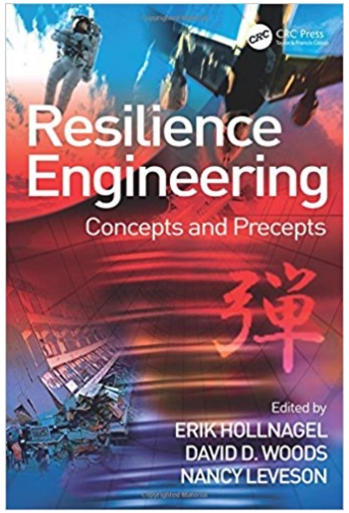
unanticipated

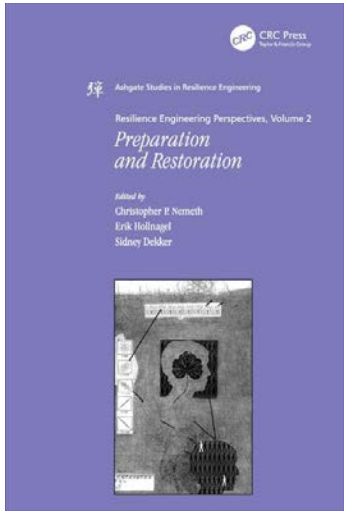
unexpected

fundamentally surprising

Resilience Engineering Is a *Field*

- Multidisciplinary, emerged from Cognitive Systems Engineering
- Early 2000s, largely in response to NASA events in 1999 and 2000
- 8 symposia over 13 years



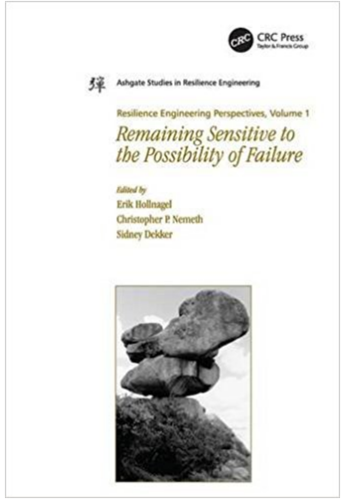

CRC Press

弾 Ashgate Studies in Resilience Engineering

Resilience Engineering Perspectives, Volume 2

Preparation and Restoration

Edited by
Christopher P. Nemeth
Erik Hollnagel
Sidney Dekker

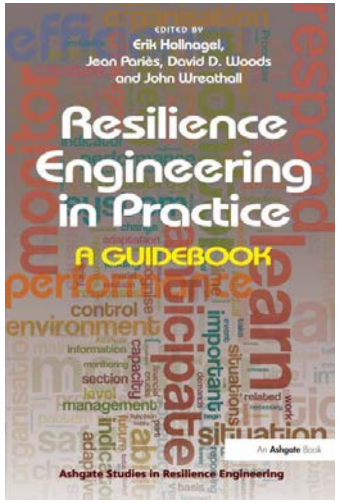

CRC Press

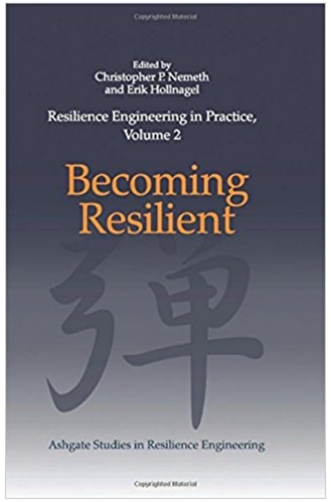
弾 Ashgate Studies in Resilience Engineering

Resilience Engineering Perspectives, Volume 1

Remaining Sensitive to the Possibility of Failure

Edited by
Erik Hollnagel
Christopher P. Nemeth
Sidney Dekker




Edited by
Christopher P. Nemeth
and Erik Hollnagel

Resilience Engineering in Practice, Volume 2

Becoming Resilient

弾

Ashgate Studies in Resilience Engineering

Resilience Engineering is a *Community*

is largely made up of practitioners and researchers from….

Human Factors & Ergonomics

Cognitive Systems Engineering

Complexity Science

Sociology

Cognitive Psychology

Operations Research

Engineering*

Safety Science

Ecology

Cybernetics

Biology

Control Systems

Resilience Engineering is a *Community*

working in domains such as…

Aviation/ATM

Construction

Mining

Space

Explosives

Surgery

Rail

Pediatrics

Anesthesia

Law Enforcement

Power Grid & Distribution

Maritime

Military Agencies

Firefighting

Intelligence Agencies

Software Engineering

Resilience Engineering is a *Community*

RESILIENCE ENGINEERING ASSOCIATION
the official home of Resilience Engineering

Learning From Incidents
Conference | 2023

https://www.resilience-engineering-association.org/

https://www.learningfromincidents.io/

Our Agenda

Today

- Framing Concepts
  - ☑ The Internet is much more than routing!
  - ☑ Challenges for Internet Survivability
  - ☑ How people are currently dealing with it
  - ☑ The Resilience Engineering perspective
- Living Examples
  - □ 100% Tracing - Lorin Hochstein
  - □ SNAFU - Zoran Perkov
- Plans for tomorrow

Tomorrow

- Depends a lot on today…

Our Agenda

Today

- Framing Concepts
  - ☑ The Internet is much more than routing!
  - ☑ Challenges for Internet Survivability
  - ☑ How people are currently dealing with it
  - ☑ The Resilience Engineering perspective
- Living Examples
  - ☑ 100% Tracing - Lorin Hochstein
  - ☑ SNAFU - Zoran Perkov
- Final Thoughts

Tomorrow

- Depends a lot on today…

resilience is:

- proactive activities aimed at **preparing to be unprepared**

  -- *without an ability to justify it economically!*

- sustaining the potential for future adaptive action when conditions change

- something that a system ***does***, not what it ***has***

“Lack of resilience is hidden until system failure.”

Resilience is always present.

It hides the anomalies and surprises that are continuous.

It is the only reason your system is working in the first place!

“First, any effort to re-architect the Internet for resilience and survivability requires a new understanding of the architectural principles on which it should be based.

what adaptive capabilities enable agents to handle challenges to

It requires a reassessment of ~~the possible scenarios that can threaten~~ the network’s basic functioning, as well as the threats that can arise due to the network’s constant evolution, be it for economic, political, or societal reasons."

Final Thoughts

We need a different type of architecture.

One that goes beyond traditional internet design.

The principles are different, but ubiquitous in the real world.

We cannot escape the traps if we don’t build adaptive capacity.

The End