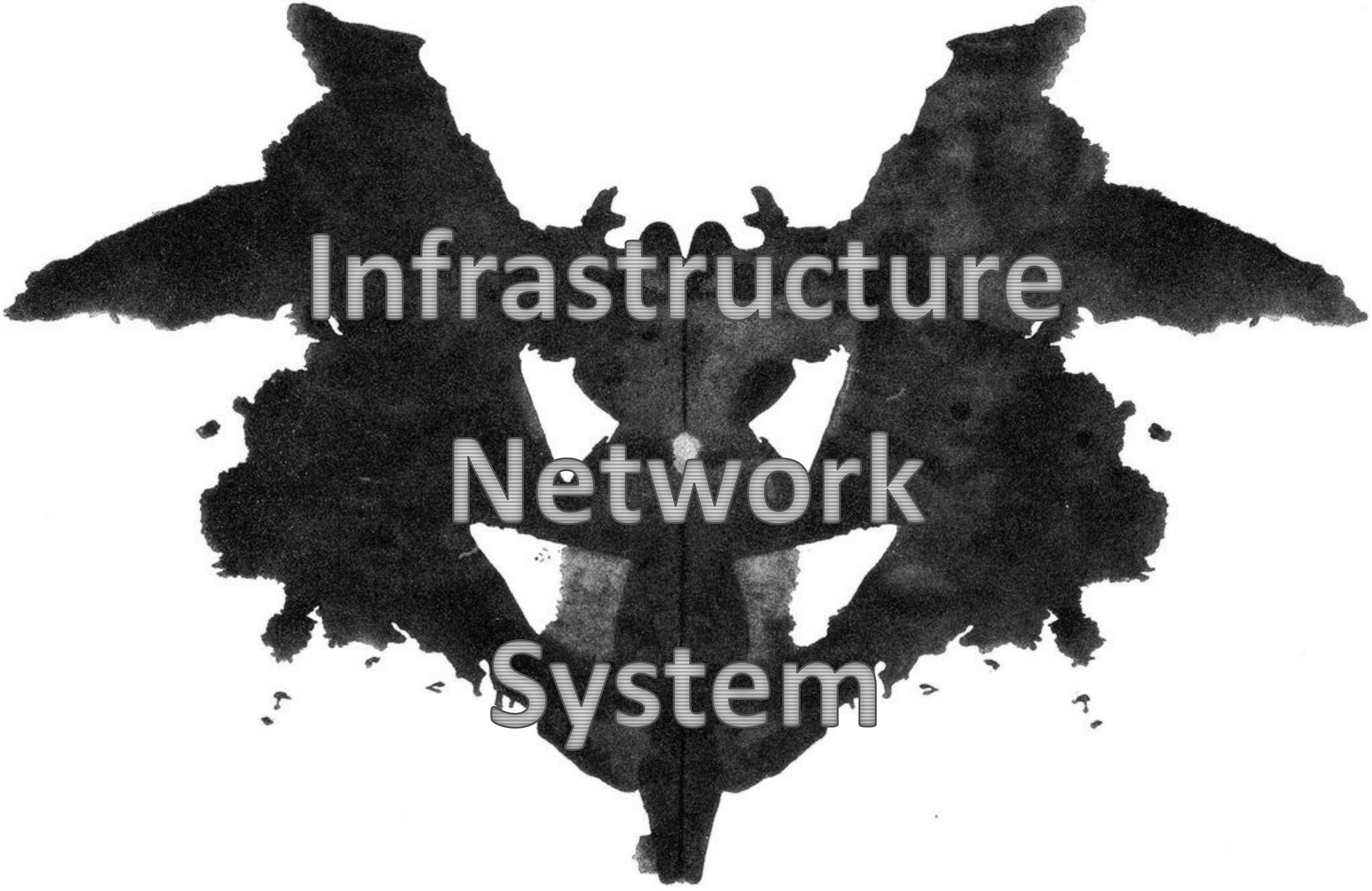
Rethinking Vulnerability and Resilience for Critical Infrastructure

Dr. David L. Alderson
Executive Director | Center for Infrastructure Defense
Professor | Operations Research
Naval Postgraduate School (NPS) | Monterey, CA USA

MORS Global Critical Infrastructure Workshop

Garmisch, Germany – 22 October 2024


Infrastructure
Network
System

Any single perspective
simultaneously ***reveals*** and ***obscures***

We must be able to ***shift perspectives***
if we are to avoid blind spots

Operations Research has enabled the development of an “optimized world”

Image Source: European Commission Newsletter, “Critical Infrastructure Resilience: News, Updates and Events,” https://publications.jrc.ec.europa.eu/repository/handle/JRC135769

Operations Research has enabled the development of an “optimized world”

“Optimized” == “Efficient”

Faster, Better, Cheaper

no waste, no slack ⟷ brittle, fragile

increasing complexity

nonlinear behavior

large scale

hidden dependencies

accidents

extreme weather

surprise events

failures

attacks

unintended consequences

cascading failures

system collapse

mission failure

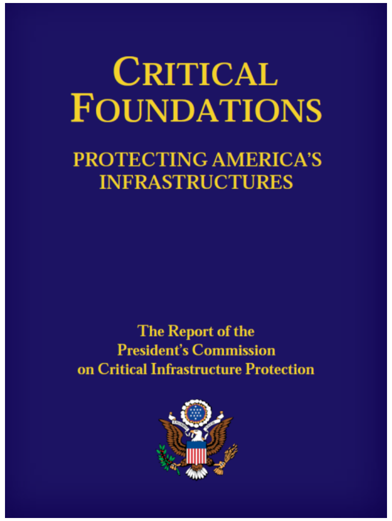
Image Source: European Commission Newsletter, “Critical Infrastructure Resilience: News, Updates and Events,” https://publications.jrc.ec.europa.eu/repository/handle/JRC135769

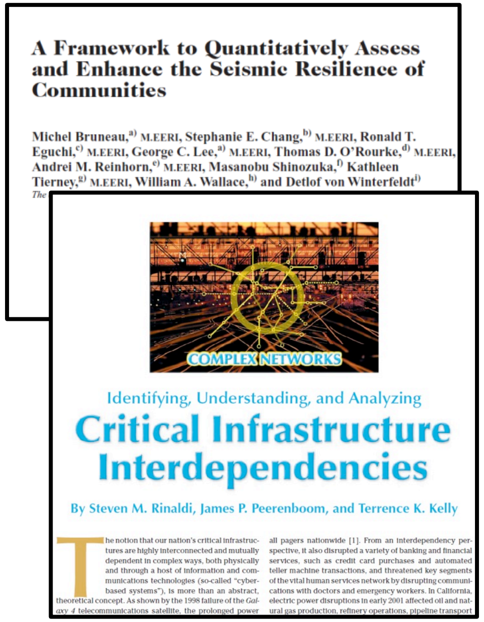
Act I: The US Infrastructure Resilience Renaissance

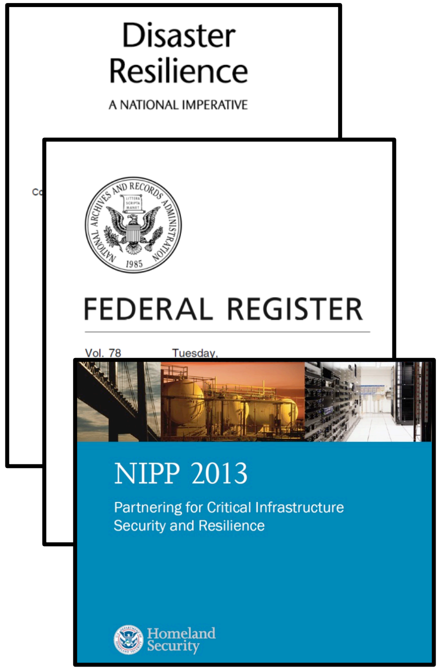
Act II:

1997 → **2001 – 2005** → **2009 – 2010** → **2012 – 2013** → **2013 – 2023**

Drivers | **Theories** | **Frameworks** | **Policies** | **Modeling + Simulation**







Conferences
Journals
National Funding
Centers of Excellence

Universities
National Laboratories
FFRDCs
Defense Contractors

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

Act II:

2013 – 2023

Modeling
+
Simulation

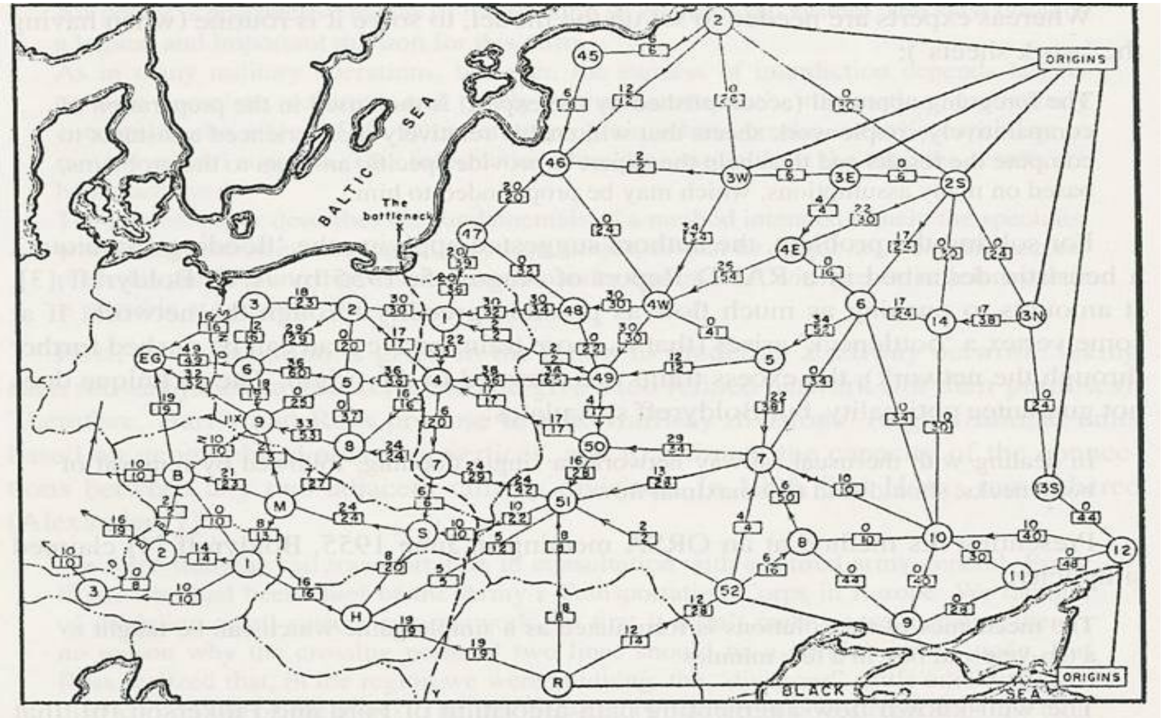
Conferences
Journals
National Funding
Centers of Excellence

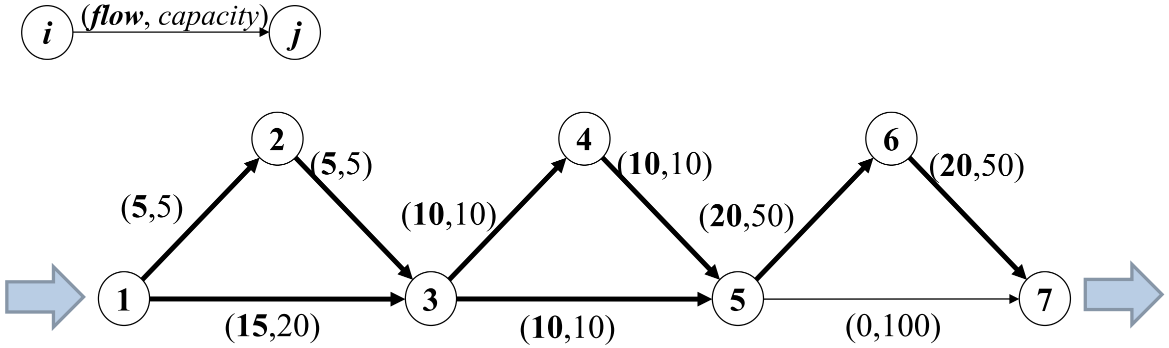
Universities
National Laboratories
FFRDCs
Defense Contractors

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

Russian Rail Network circa 1955



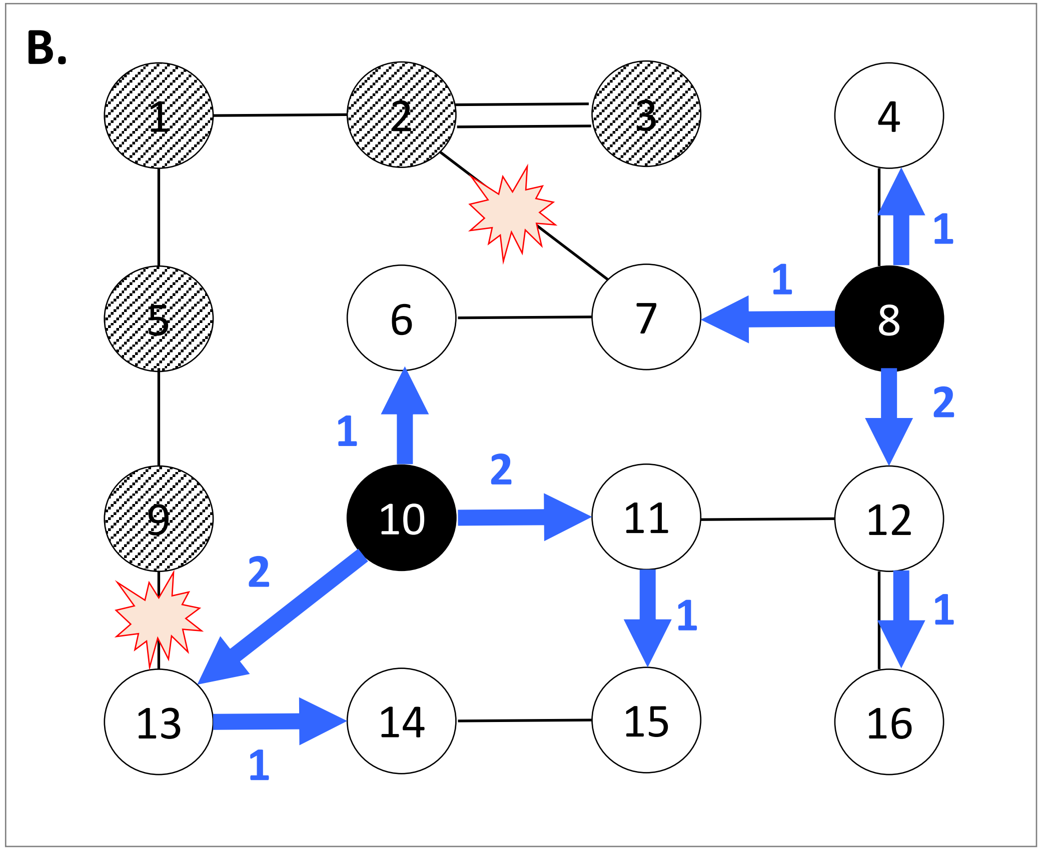


Alderson, D., Brown, G., Carlyle, M., and Cox, L. A., 2013, "Sometimes There is No "Most-Vital" Arc: Assessing and Improving the Operational Resilience of Systems," Military Operations Research, 18(1), pp. 21-37.

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

Attacker - Defender Models



$$\min_{\mathbf{y}\in Y(\hat{\mathbf{x}})} f(\hat{\mathbf{x}},\mathbf{y})$$

$$\max_{\mathbf{x}\in X} \min_{\mathbf{y}\in Y(\mathbf{x})} f(\mathbf{x},\mathbf{y})$$

Alderson, D.L., Brown, G., and Carlyle, W.M., 2015, "Operational Models of Infrastructure Resilience," Risk Analysis 35(4): 562-586

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify ***vulnerabilities***
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

An Issue…

Many **separate notions of vulnerability**…

… each with their own set of assumptions and tools…

… that often yield **different conclusions** about the same system!

The Premise

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify ***vulnerabilities***
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build ***resilience***…
- …and assure the mission!

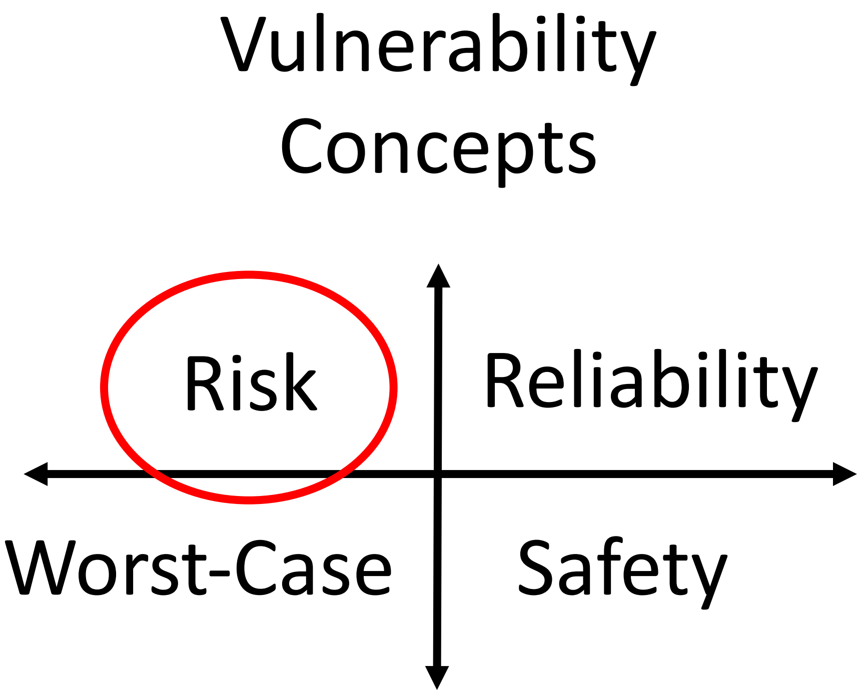
An Issue…

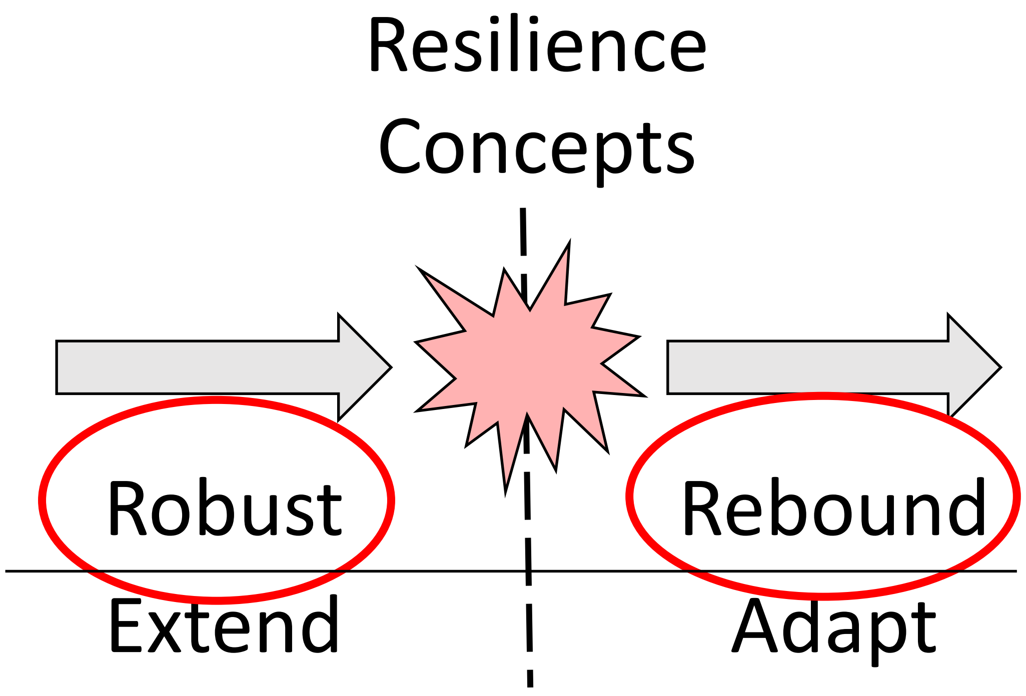
Many **separate notions of resilience**…

… each with their own set of assumptions and tools…

… that often yield **different recommendations** for the same system!

Distinct perspectives on mission assurance



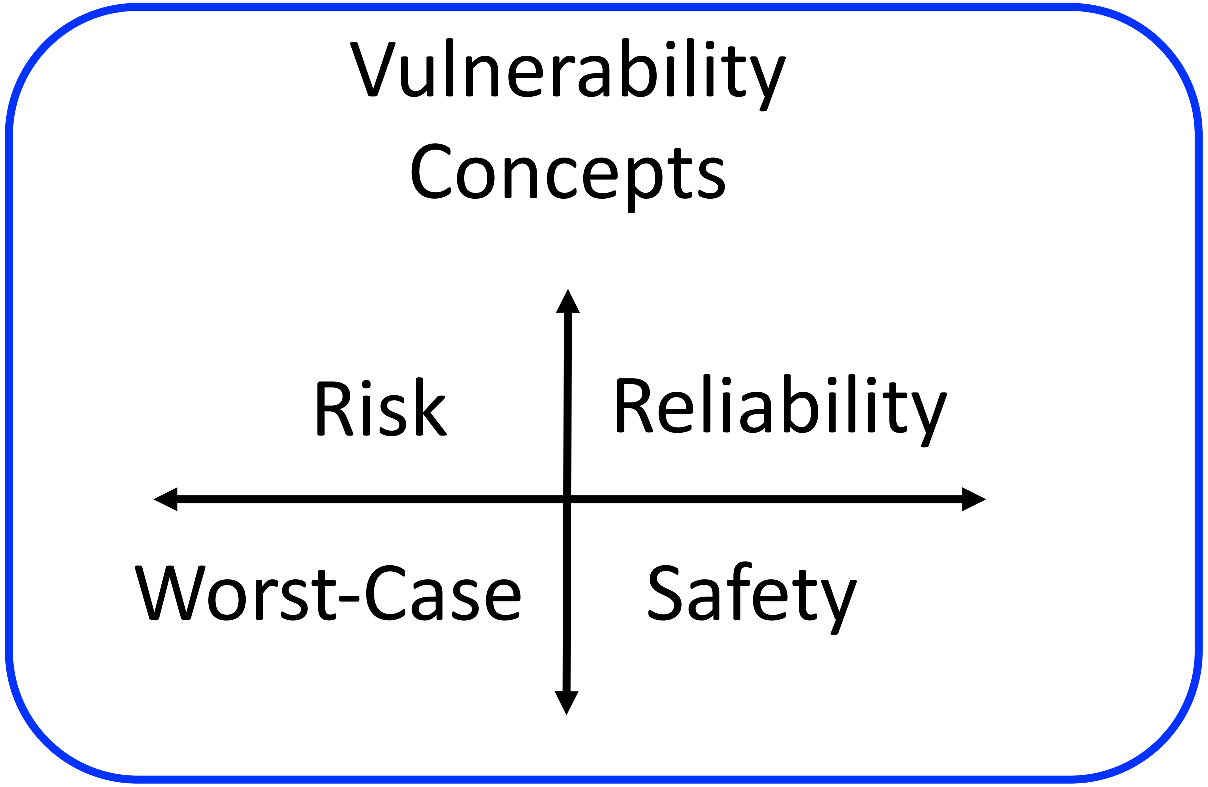


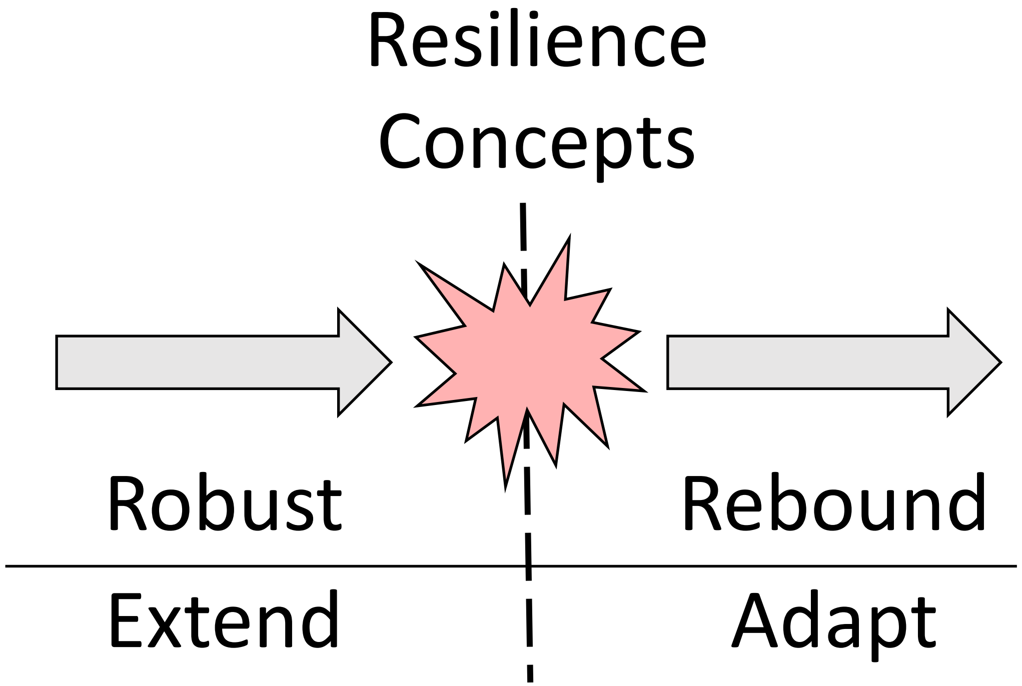
Commonly the sole focus of vulnerability analysis
Incomplete at best
Leaves blind spots in terms of vulnerability

Commonly the sole focus of resilience analysis
Incomplete at best
Leaves blind spots in terms of resilience

This reframing is joint work with Dan Eisenberg, NPS.

Distinct perspectives on mission assurance





This reframing is joint work with Dan Eisenberg, NPS.

Reframing Vulnerability Analysis

Likelihood

- ***Probable***

  We have a sense of how likely (frequent) an event will happen.

  Tools: probability, statistics.

- ***Possible***

  The event could conceivably happen, but the idea seems strange, absurd, or unbelievable.

  Tools: game theory

Challenge

- ***External***

  Vulnerabilities arise from external threats that impact operations

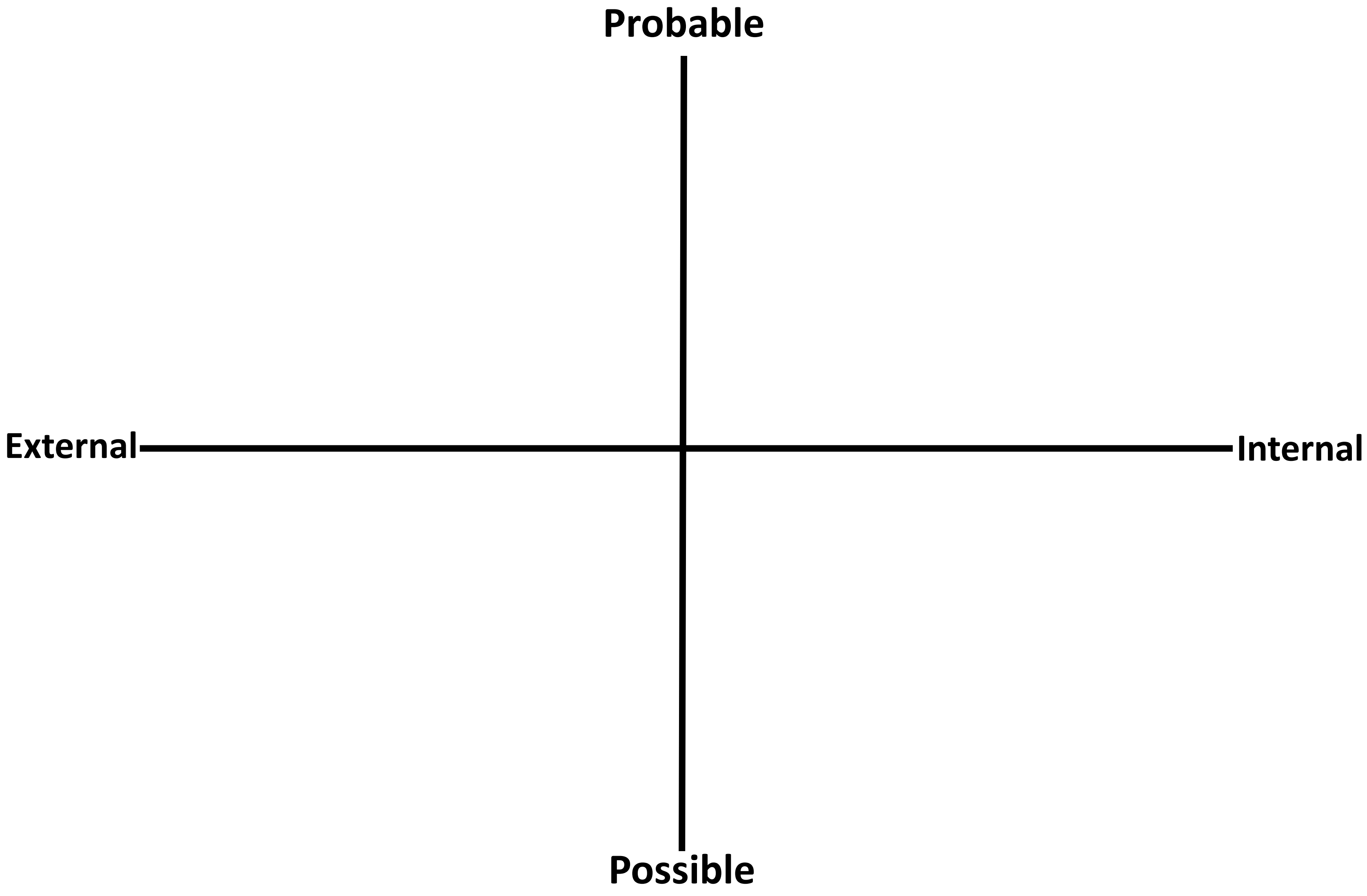
  Tools: threat modeling

- ***Internal***

  Vulnerabilities arise from system design and operational decisions

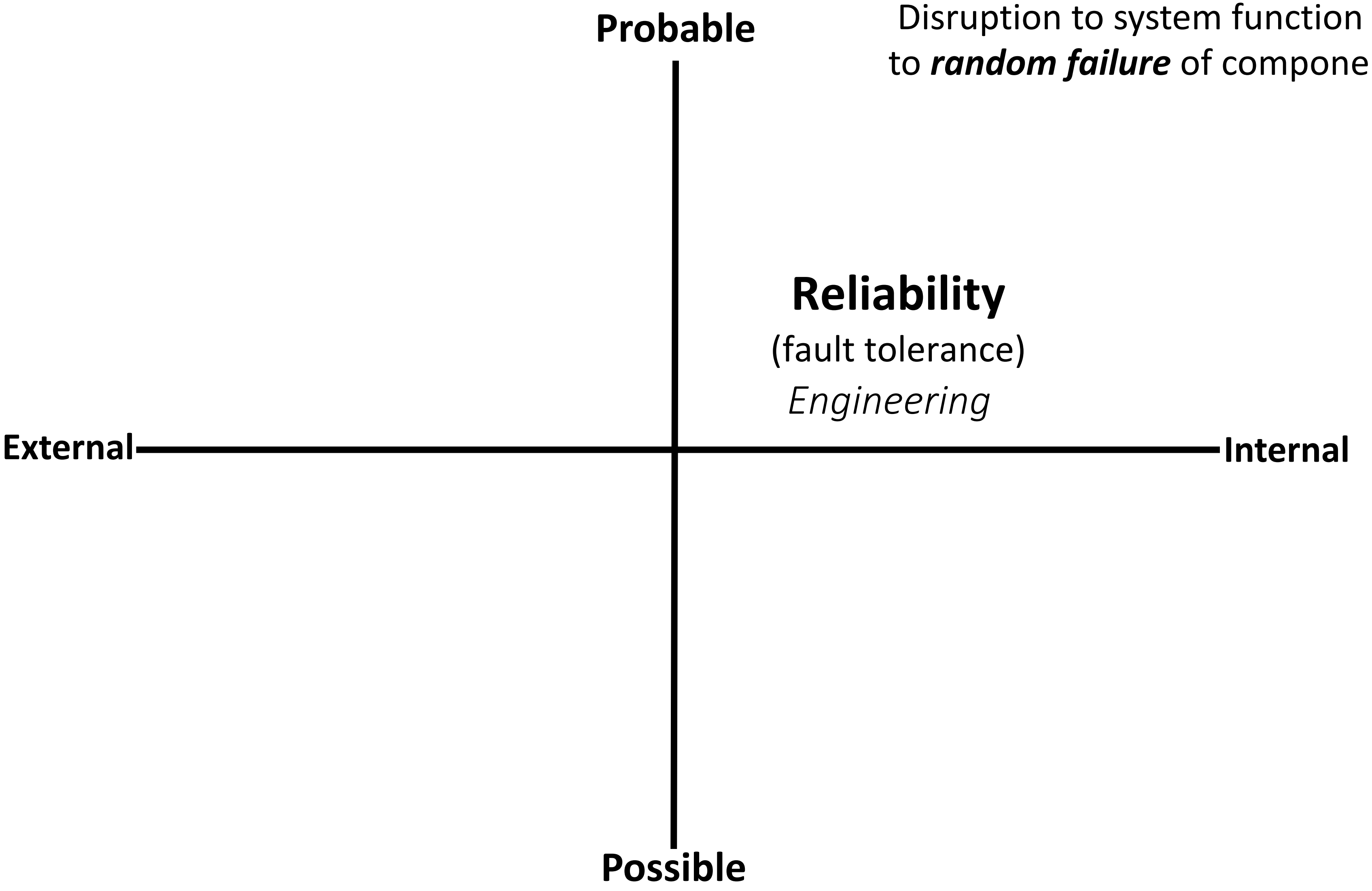
  Tools: systems engineering

Reframing Vulnerability Analysis



Reframing Vulnerability Analysis

Disruption to system function due to ***random failure*** of component(s)



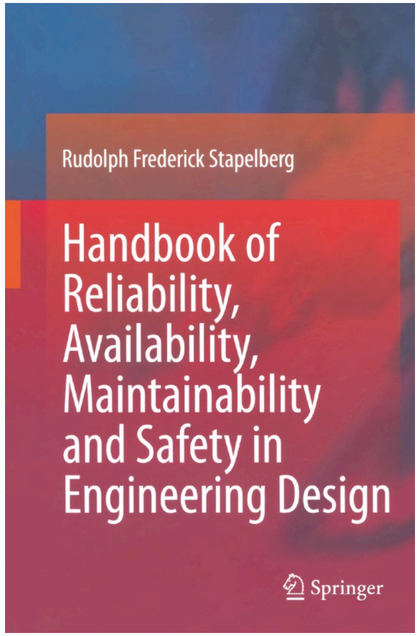
Reliability Engineering

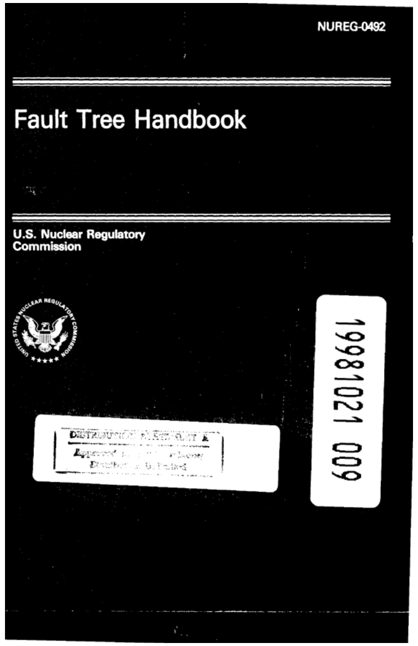
Key Topics:

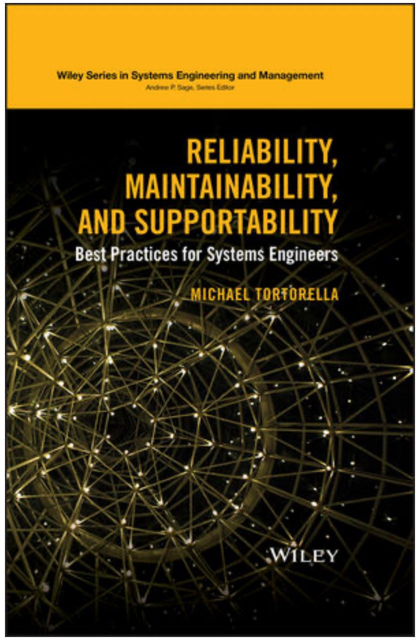
Reliability focuses on CI ***Quality*** and ***Failures***

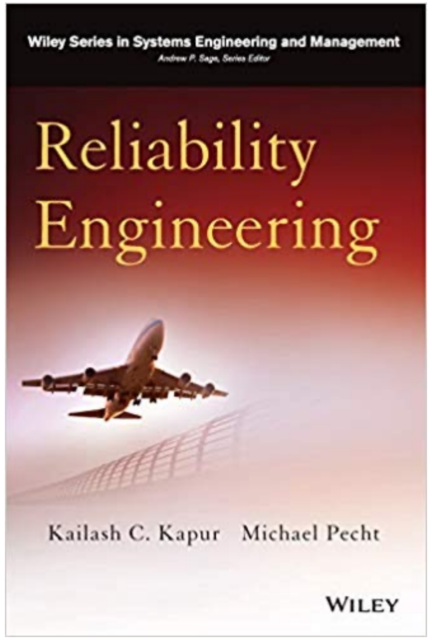
- What models / data fit within the reliability world?

- How to take a reliability-based view of resilience for energy infrastructure



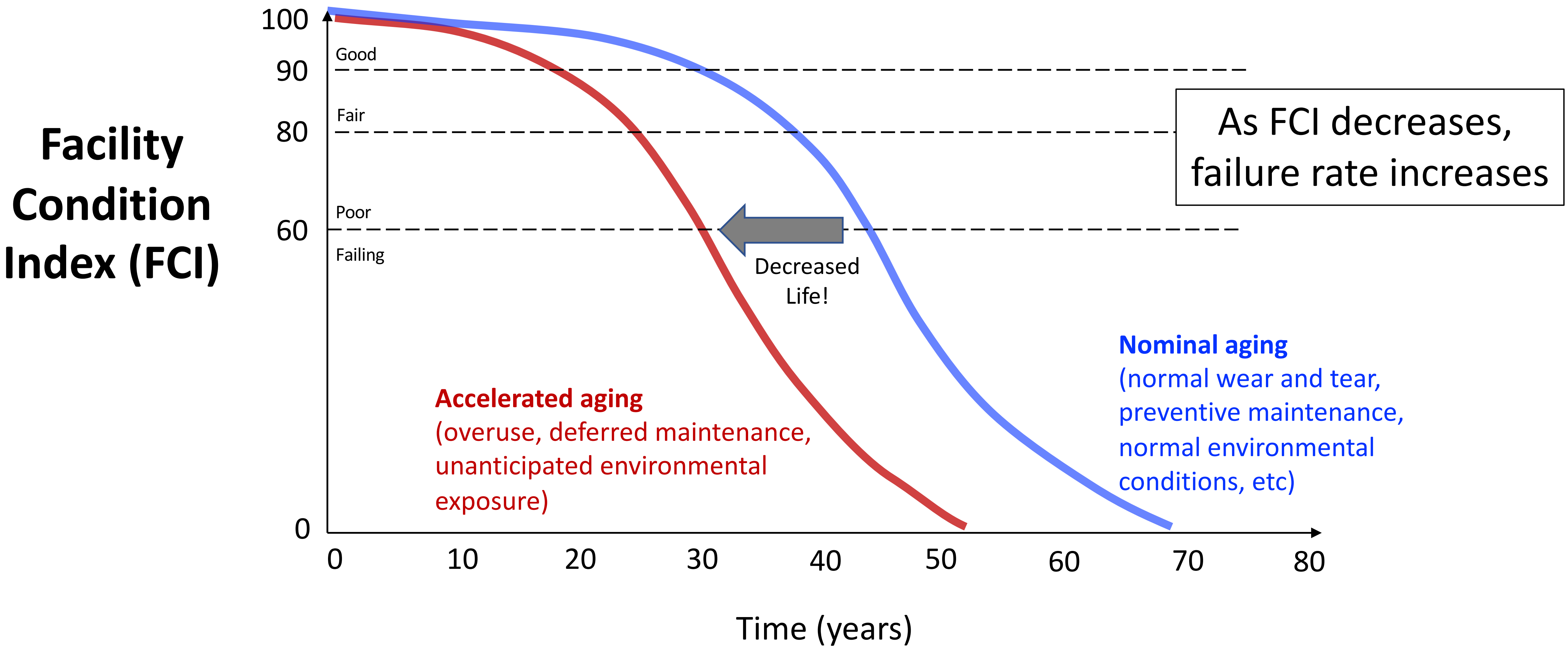






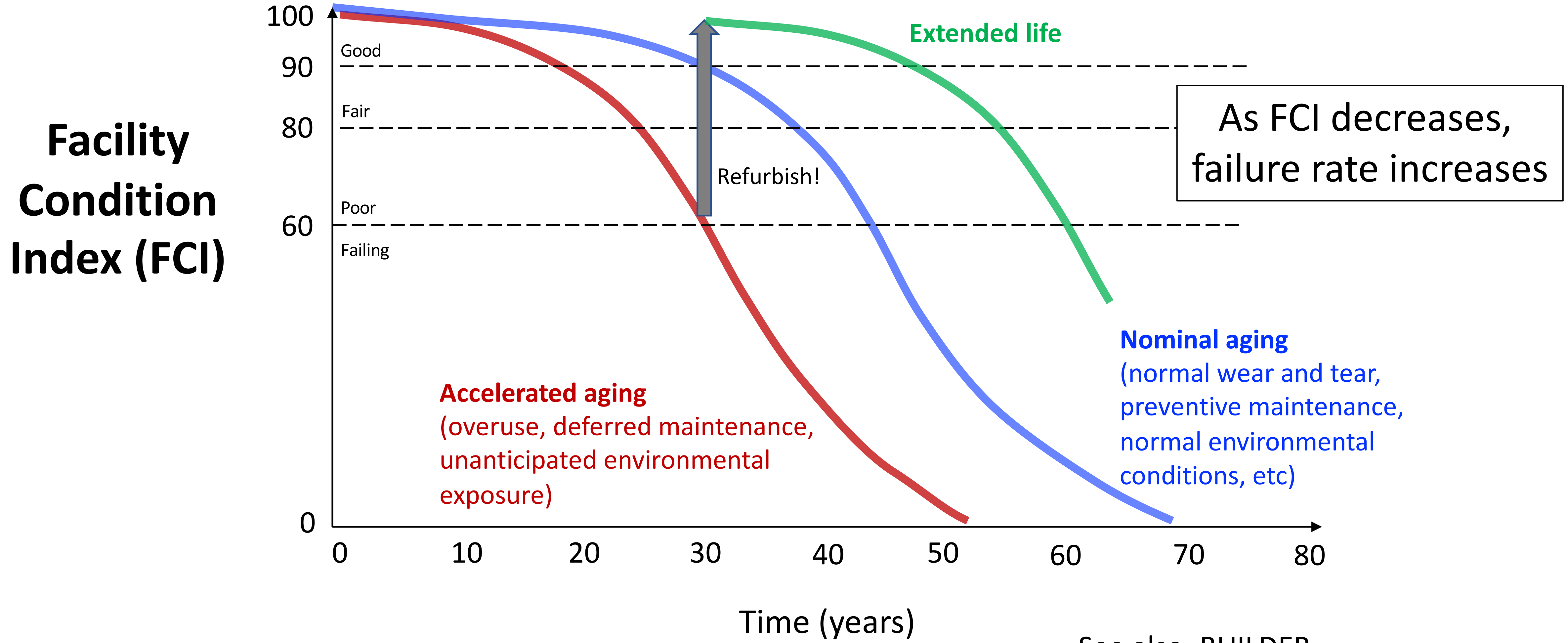
Reliability

Reliability decreases as the facility or component ages



Reliability

Reliability decreases as the facility or component ages



Adapted from: Renosto, A, 2019. *Optimizing Marine Corps Installation Readiness*. MS Thesis, Naval Postgraduate School, Monterey CA.

See also: BUILDER,
Sustainment Management System
https://www.sms.erdc.dren.mil/

Reliability

What do we mean when we say, "It works 99% of the time" ?

Reliability is a <u>population statistic</u>

- Of *a particular system or design*
- Based on *past experience*:
    - In the past, over significant periods of time
    - Over many units, deployments, implementations, etc.
- Based on a *model*:
    - Given a model of how the system works, the potential ways things can fail, and how the system will respond, we generate a population of data via experiments that simulate how the system will behave in the real world

What happens when the operating environment changes?

What if the future is not like the past?

What happens when the system changes?

What if our model becomes stale?

In many cases, reliability is a weak indicator of future system performance.

Pitfalls of Reliability Analysis

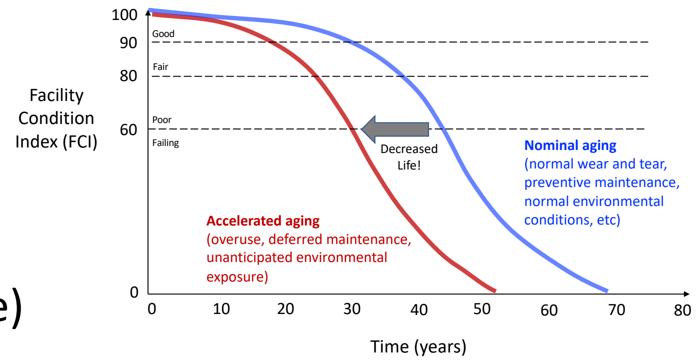
- Condition Curves Don’t Match Reality
  - New assets can fail like old ones
  - Systems experience non-linear degradation
  - “Like new” is not the same as new

- Relying Too Much on Reliability
  - We become dependent on reliable systems making their failure more and more catastrophic

Reframing Vulnerability Analysis

Probable

Disruption to system function due to ***random failure*** of component(s)



Reliability

(fault tolerance)

Engineering

External **Internal**

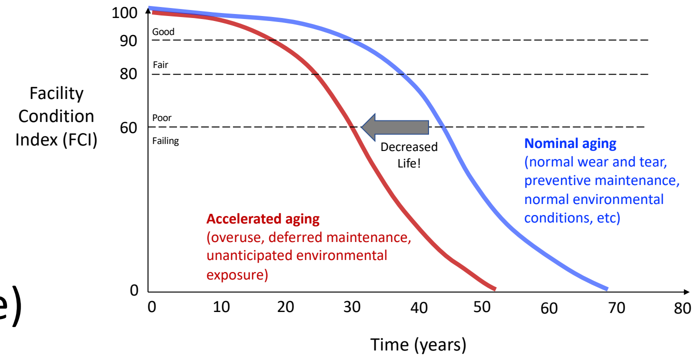
Possible

Reframing Vulnerability Analysis

High impact disruption
(in magnitude and/or frequency)

Probable

Disruption to system function due to ***random failure*** of component(s)



Risk
(expected case)
Insurance

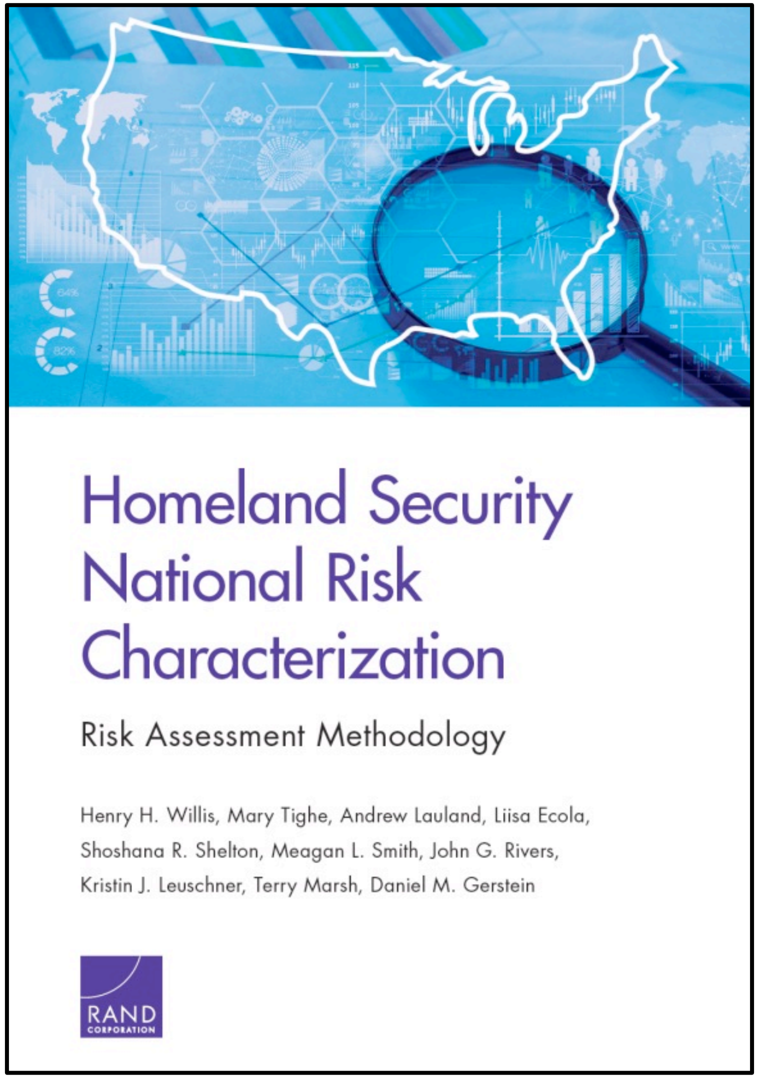
Reliability
(fault tolerance)
Engineering

External

Internal

Possible

Lots of Existing Frameworks
for Physical and Cybersecurity Infrastructure Risk



Homeland Security National Risk Characterization

Risk Assessment Methodology

Henry H. Willis, Mary Tighe, Andrew Lauland, Liisa Ecola, Shoshana R. Shelton, Meagan L. Smith, John G. Rivers, Kristin J. Leuschner, Terry Marsh, Daniel M. Gerstein

RAND CORPORATION

Framework for Improving
Critical Infrastructure Cybersecurity

Version 1.1

National Institute of Standards and Technology

April 16, 2018

Traditional approaches to vulnerabilities: *reliability* and *risk*

Based on estimates of event

- Likelihoods
- Consequences

OPNAVINST 3500.39D
29 Mar 2018

Risk Assessment Matrix

SEVERITY – Effect of Hazard		PROBABILITY – Frequency of Occurrence Over Time: A Frequent (Continuously experienced)	B Likely (Will occur frequently)	C Occasional (Will occur several times)	D Seldom (Unlikely; can be expected to occur)	E Unlikely (Improbable; but possible to occur)
Catastrophic (Death, Loss of Asset, Mission Capability or Unit Readiness)	I	EH 1	EH 1	H 2	H 2	M 3
Critical (Severe Injury or Damage, Significantly Degraded Mission Capability or Unit Readiness)	II	EH 1	H 2	H 2	M 3	L 4
Moderate (Minor Injury or Damage, Degraded Mission Capability or Unit Readiness)	III	H 2	M 3	M 3	L 4	L 4
Negligible (Minimal Injury or Damage, Little or No Impact to Mission Readiness or Unit Readiness)	IV	M 3	L 4	L 4	L 4	L 4

Risk Assessment Levels

EH=Extremely High 1 H=High 2 M=Medium 3 L=Low 4

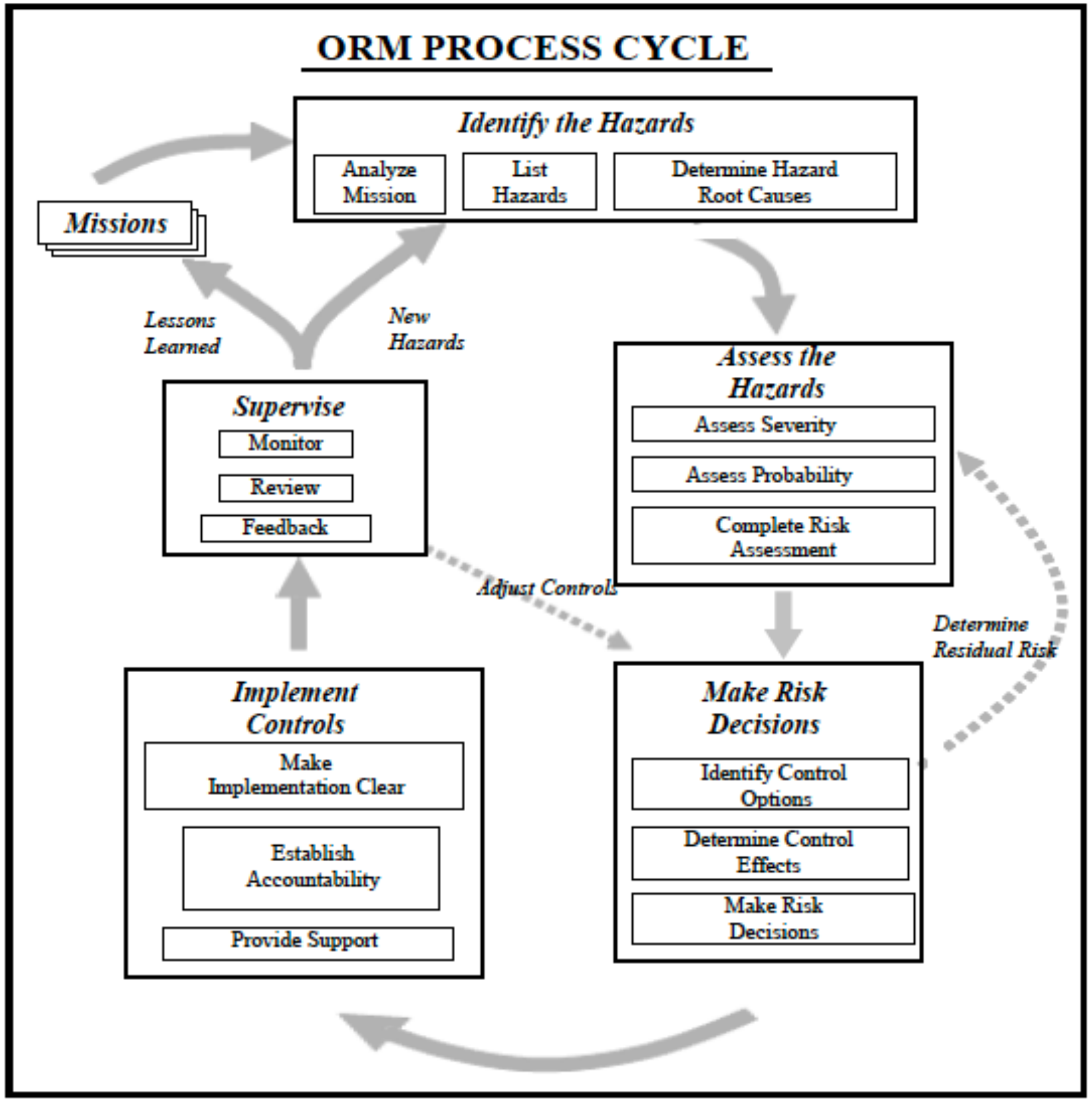
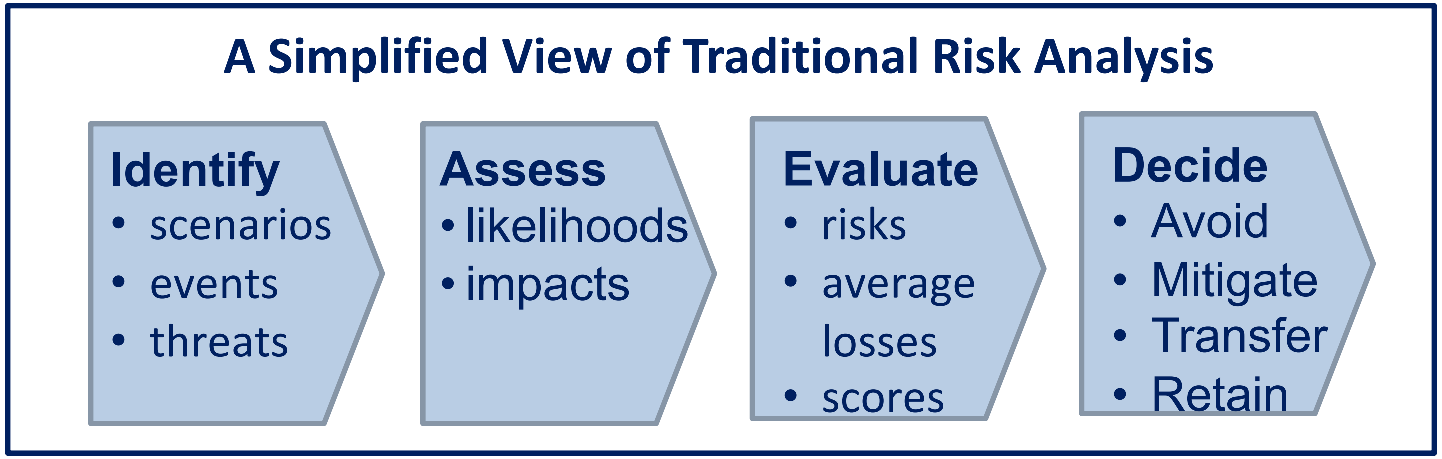


Figure 1-2: The Five-Step ORM Process

Traditional approaches to vulnerabilities: *reliability* and *risk*

Based on estimates of event

- Likelihoods
- Consequences



CISA Strategic Risk Management Process

CISA = Cybersecurity and Infrastructure Security Agency
https://www.dhs.gov/cisa

Traditional approaches to vulnerabilities: *reliability* and *risk*

Based on estimates of event

- Likelihoods
- Consequences

A Simplified View of Traditional Risk Analysis

Identify
- scenarios
- events
- threats

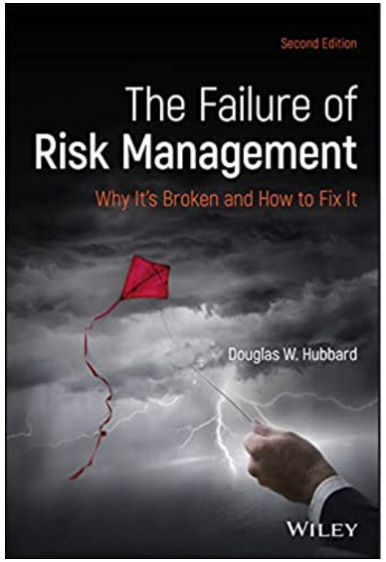
Assess
- likelihoods
- impacts

Evaluate
- risks
- average losses
- scores

Decide
- Avoid
- Mitigate
- Transfer
- Retain

LOTS of known problems with commonly used tools…

- Risk matrices
- Risk scores



by Douglas Hubbard

CISA Strategic Risk Management Process

CISA = Cybersecurity and Infrastructure Security Agency
https://www.dhs.gov/cisa

Traditional approaches to vulnerabilities: *reliability* and *risk*

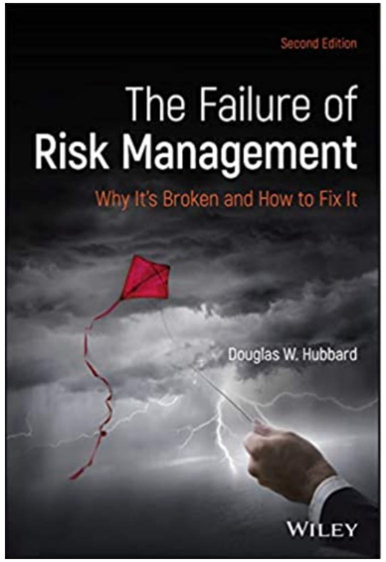
Rely primarily on <u>*past*</u> events.

Based on estimates of event

- Likelihoods
- Consequences

<u>LOTS</u> of known problems with commonly used tools…

- Risk matrices
- Risk scores



by Douglas Hubbard

A Simplified View of Traditional Risk Analysis

Identify
- scenarios
- events
- threats

Assess
- likelihoods
- impacts

Evaluate
- risks
- average losses
- scores

Decide
- Avoid
- Mitigate
- Transfer
- Retain

- You cannot predefine all threats!
- You will be surprised!

How do we deal with events outside of past experience?

How bad could things be?

Pitfalls of Risk Analysis

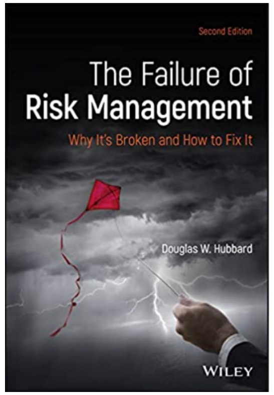
- Threats must be identified in advance
  - No way to define all threats
  - Data on defined threats might be insufficient

- Simple risk scores and models
  - Risk matrices create mathematical inaccuracies
  - Simple risk metrics do not work in most cases

Hubbard:
Acting with confidence based on poor risk analysis
can be more dangerous than doing nothing at all!!!

Reframing Vulnerability Analysis

High impact disruption
(in magnitude and/or frequency)



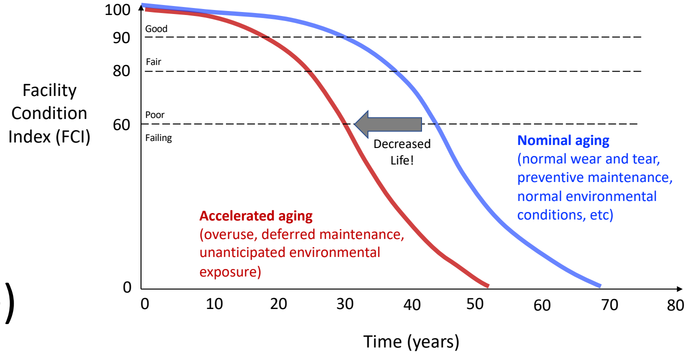
Hubbard

RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Probable

Disruption to system function due to ***random failure*** of component(s)



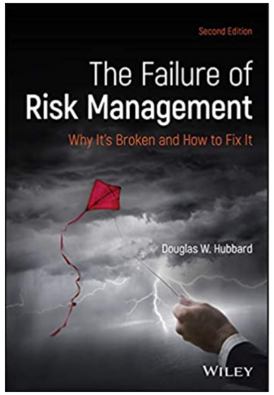
Risk
(expected case)
Insurance

Reliability
(fault tolerance)
Engineering

External — **Internal**

Possible

Reframing Vulnerability Analysis



Hubbard

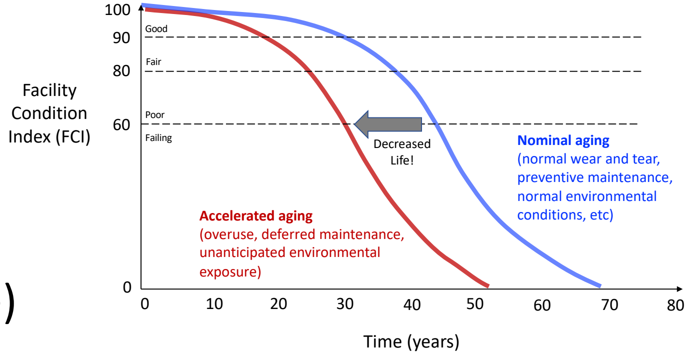
High impact disruption
(in magnitude and/or frequency)

RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Probable

Disruption to system function due
to ***random failure*** of component(s)



Risk
(expected case)
Insurance

Reliability
(fault tolerance)
Engineering

External **Internal**

Worst Case
(game theory)
Military

Worst-case disruption
(as defined by system objective)

Possible

Assessing and improving infrastructure vulnerability

1. *Build an "operator model" of infrastructure function*

$$\min_{\mathbf{y}\in Y} f(\mathbf{y})$$

e.g., electric power, traffic congestion
(validated, industry-standard model)

2. *What-if scenario analysis: loss of sets of components*

$$\max_{\mathbf{x}\in X} \min_{\mathbf{y}\in Y(\mathbf{x},\mathbf{w})} f(\mathbf{y})$$

X = set of admissible disruptions
"attacker" selects worst-case

3. *Assess improvements from potential investments*

$$\min_{\mathbf{w}\in W} \max_{\mathbf{x}\in X(\mathbf{w})} \min_{\mathbf{y}\in Y(\mathbf{x},\mathbf{w})} f(\mathbf{y})$$

mitigates worst-case

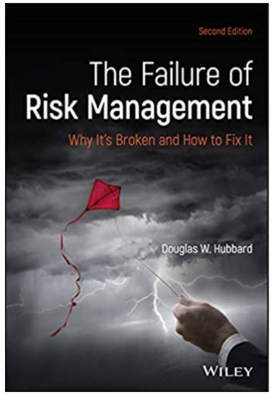
Reference: Alderson, D.L., G.G. Brown, W.M. Carlyle. 2014. "Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems." A. Newman, J. Leung, eds., *Tutorials in Operations Research: Bridging Data and Decision*. Institute for Operations Research and Management Science, Hanover, MD, 180-215.

Pitfalls of Worst-Case Analysis

- Defining your objective
  - Assumes we have an established measure of system “cost”
  - Often how infrastructure operator measures “cost” is insufficient for analysis

- Ignores failures less than worst-case
  - Called “adversarial” to emphasize that an enemy would choose to cause worst-case disruption
  - Failures can happen for *any reason*

Reframing Vulnerability Analysis



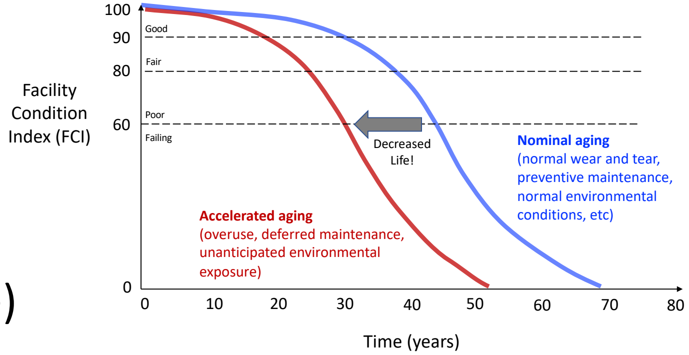
Hubbard

High impact disruption
(in magnitude and/or frequency)

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Probable

Disruption to system function due to ***random failure*** of component(s)



Risk
(expected case)
Insurance

Reliability
(fault tolerance)
Engineering

External — **Internal**

Worst Case
(game theory)
Military

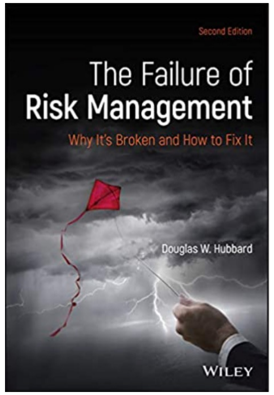
Build models to assess the capability of a system to deliver service under different scenarios

- **Attacker Models**: We identify worst-case disruptions
- **Defender Models**: We identify optimal investments to mitigate disruptions

Worst-case disruption
(as defined by system objective)

Possible

Reframing Vulnerability Analysis



Hubbard

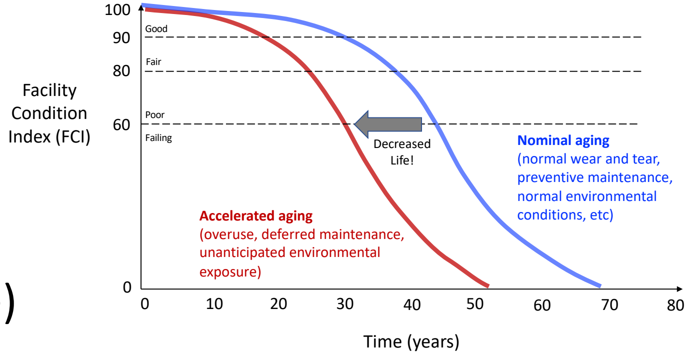
RISK ASSESSMENT MATRIX

PROBABILITY \ SEVERITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

High impact disruption
(in magnitude and/or frequency)

Probable

Disruption to system function due to ***random failure*** of component(s)



Risk
(expected case)
Insurance

Reliability
(fault tolerance)
Engineering

External — **Internal**

Worst Case
(game theory)
Military

Safety
(dealing with surprise)
Human Factors

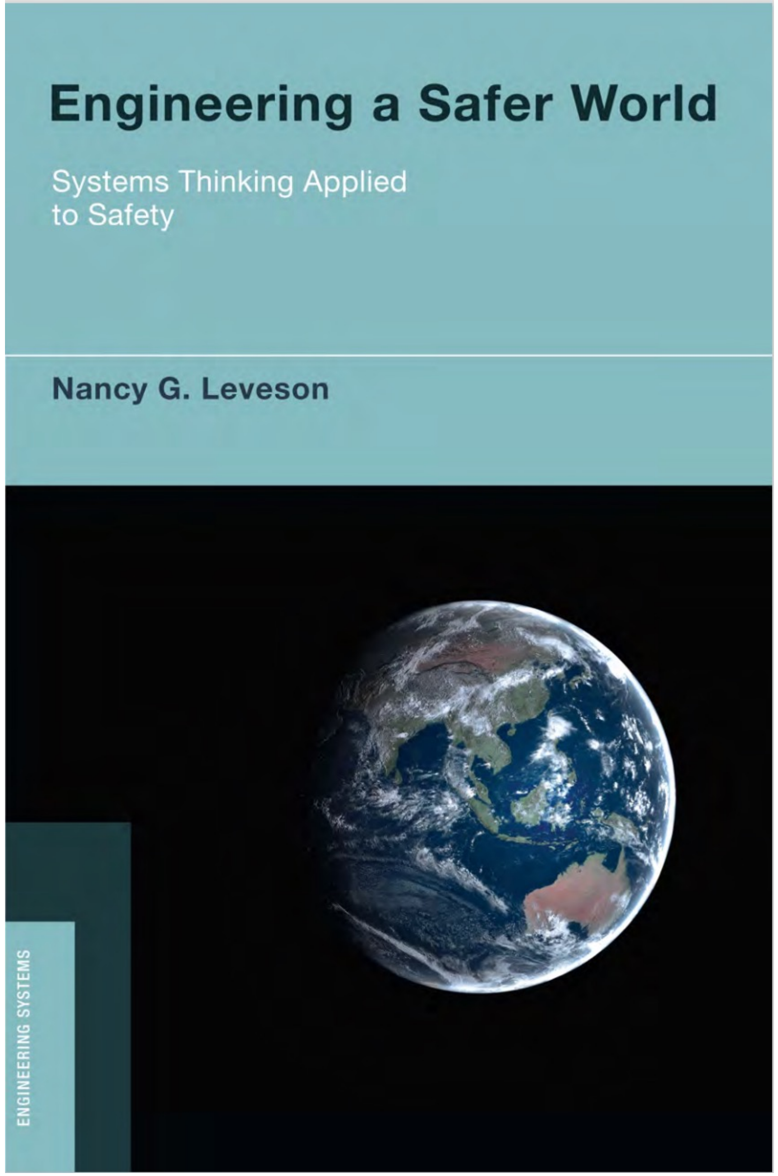
Build models to assess the capability of a system to deliver service under different scenarios
- **Attacker Models**: We identify worst-case disruptions
- **Defender Models**: We identify optimal investments to mitigate disruptions

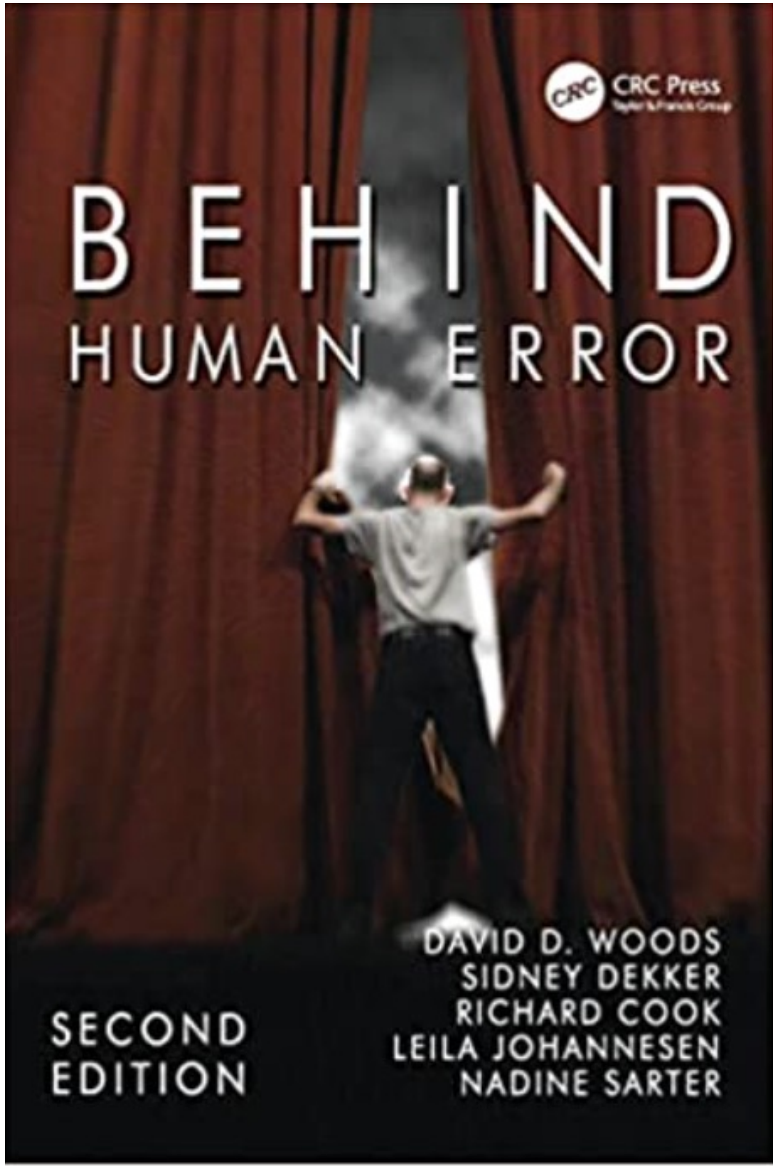
Worst-case disruption
(as defined by system objective)

Possible

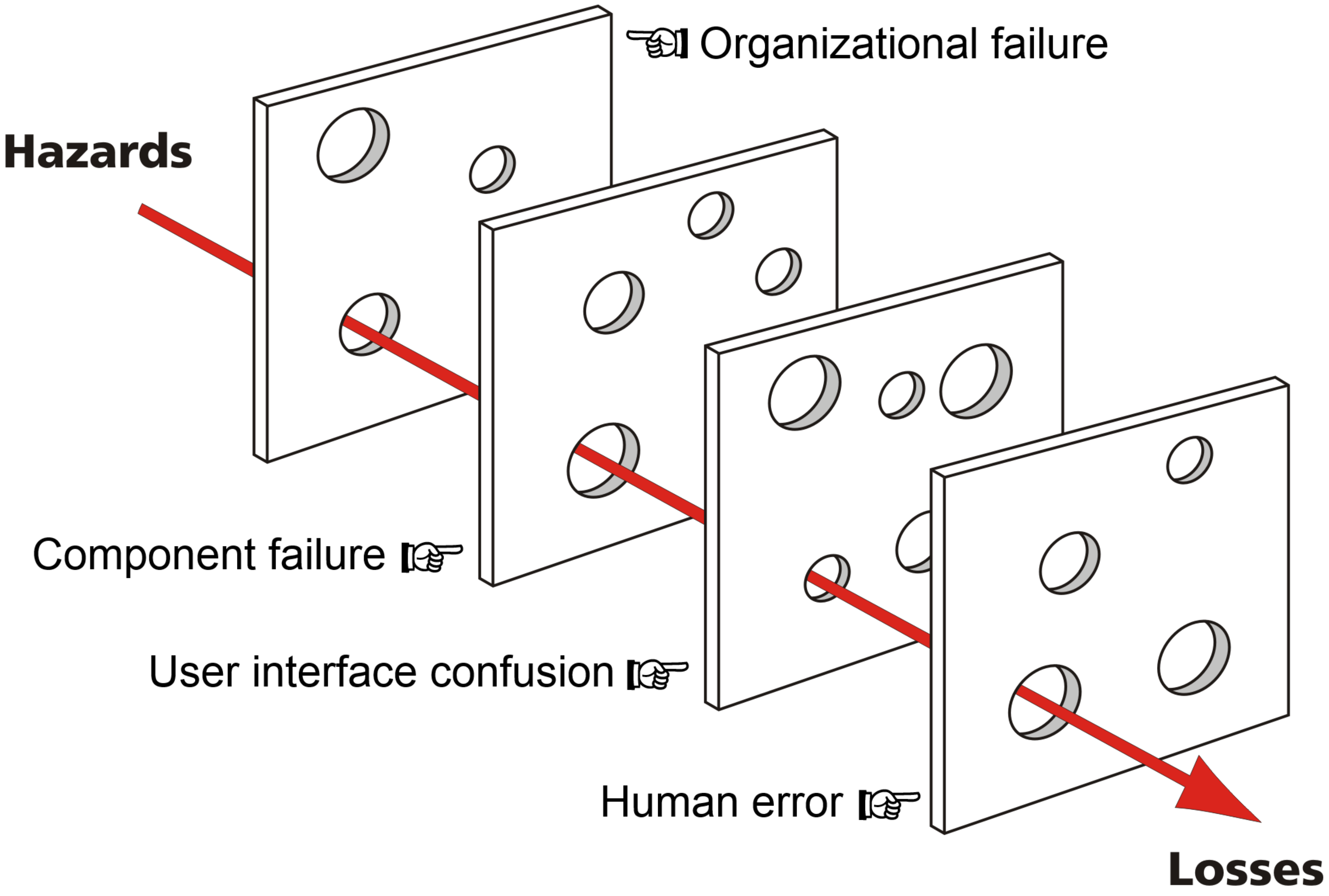
System works as designed but causes ***unintentional harm*** to people, assets, or environment

Safety Science





Misconception About How Failures Work…



Things Often Fail When (or Because) They Work as Designed

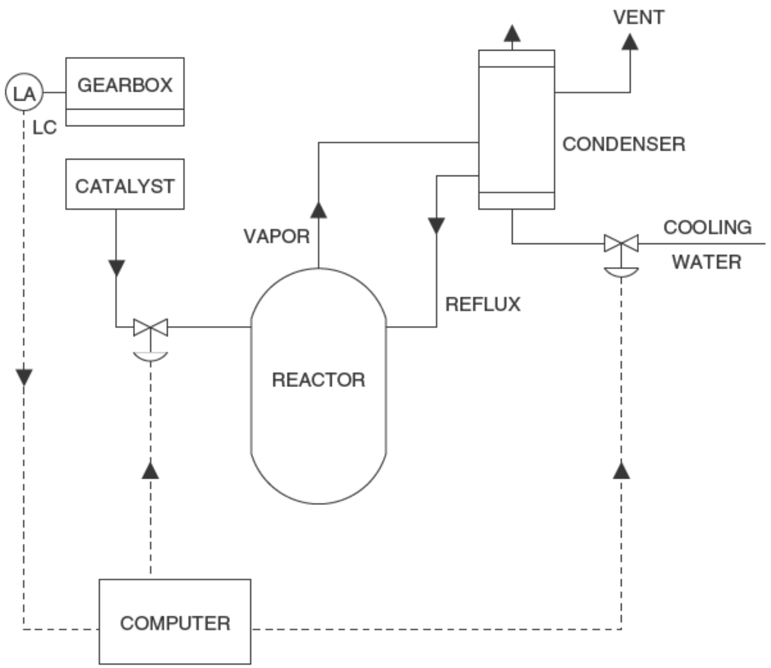
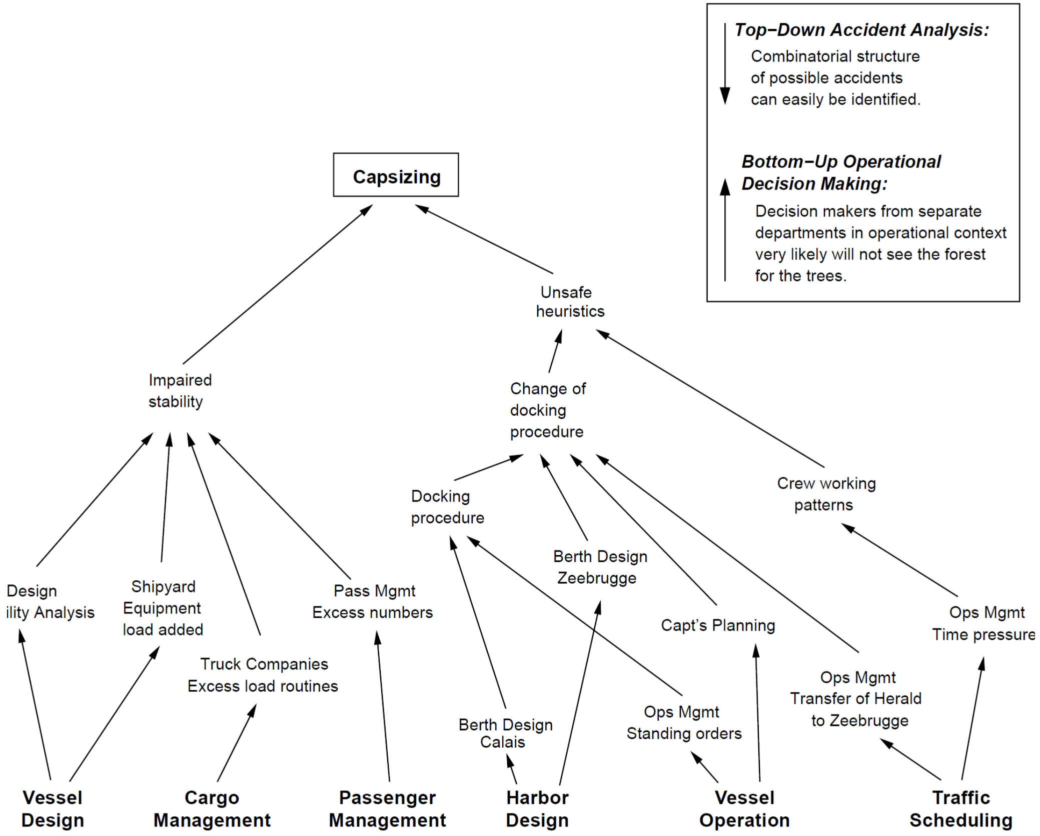


Figure 2.1
A chemical reactor design (adapted from Kletz [103, p. 6]).



Environmental disaster because system worked as designed

Boat capsized even though everyone did their job to the best of their ability

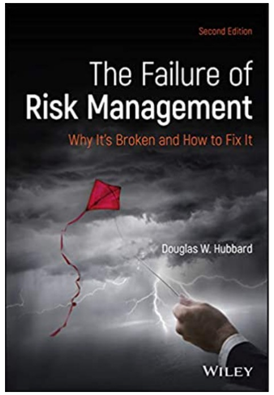
Leveson, Nancy G. *Engineering a safer world: Systems thinking applied to safety*. The MIT Press, 2016.

Pitfalls of Safety Analysis

- There is No Simple “Root Cause”
  - Systems experience failures even when everything was working as intended
  - Difficult to provide simple recommendations

- Systems Incentivized to be Unsafe
  - Organizations designed to hide responsibility
  - Experience with failure makes one better at managing it in the future

Reframing Vulnerability Analysis



Hubbard

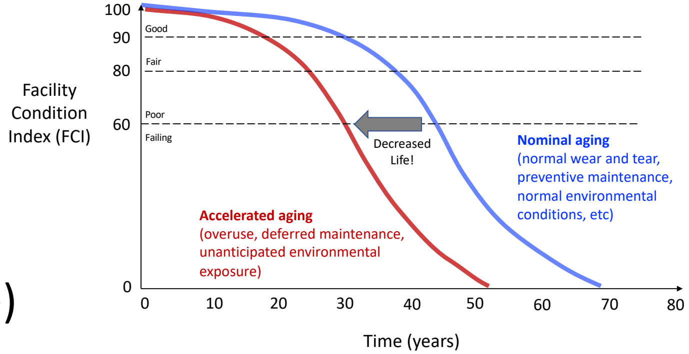
High impact disruption
(in magnitude and/or frequency)

RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Probable

Disruption to system function due to ***random failure*** of component(s)



Risk
(expected case)
Insurance

Reliability
(fault tolerance)
Engineering

External — **Internal**

Worst Case
(game theory)
Military

Safety
(dealing with surprise)
Human Factors

Build models to assess the capability of a system to deliver service under different scenarios

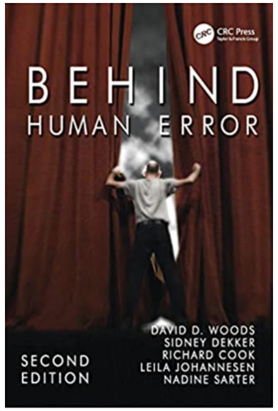
- **Attacker Models**: We identify worst-case disruptions
- **Defender Models**: We identify optimal investments to mitigate disruptions

Worst-case disruption
(as defined by system objective)

Possible

System works as designed but causes ***unintentional harm*** to people, assets, or environment

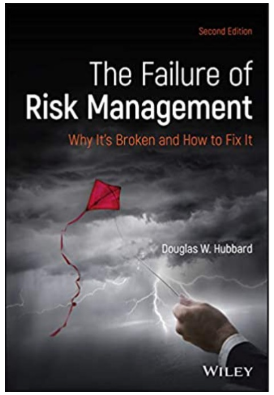
Woods et al



Reframing Vulnerability Analysis

Probable

High impact disruption
(in magnitude and/or frequency)

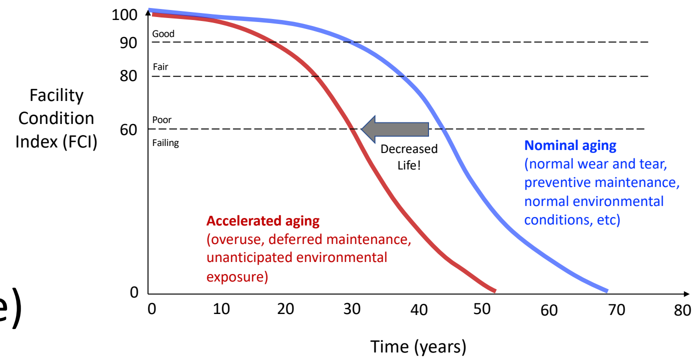


Hubbard

RISK ASSESSMENT MATRIX				
SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

Risk
(expected case)
Insurance

Disruption to system function due to ***random failure*** of component(s)



Reliability
(fault tolerance)
Engineering

External — **Internal**

- Risk and reliability **relate to traditional understandings of vulnerability**
- Use **probability & statistics** to guide decisions
- **Rely on historical data**
- **Potentially blind** to things we haven't seen before?

Reframing Vulnerability Analysis

- Worst-Case and Safety are **novel concepts** that are less commonly understood and applied
- Looking for things we haven't seen before
- **Possibility and potential actions** guide decisions

External — **Internal**

Build models to assess the capability of a system to deliver service under different scenarios
- **Attacker Models**: We identify worst-case disruptions
- **Defender Models**: We identify optimal investments to mitigate disruptions

Worst Case

(game theory)

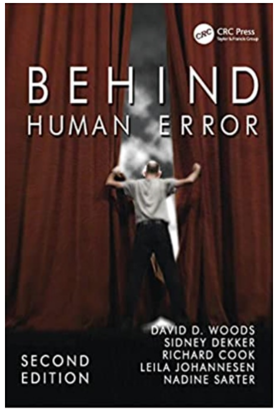
Military

Safety

(dealing with surprise)

Human Factors

Woods et al

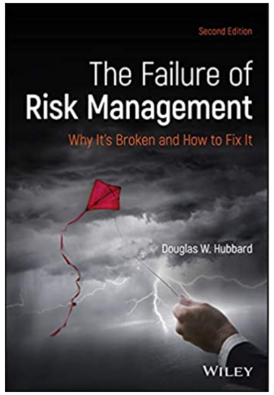


Worst-case disruption
(as defined by system objective)

Possible

System works as designed but causes ***unintentional harm*** to people, assets, or environment

Reframing Vulnerability Analysis



Hubbard

RISK ASSESSMENT MATRIX

SEVERITY / PROBABILITY	Catastrophic (1)	Critical (2)	Marginal (3)	Negligible (4)
Frequent (A)	High	High	Serious	Medium
Probable (B)	High	High	Serious	Medium
Occasional (C)	High	Serious	Medium	Low
Remote (D)	Serious	Medium	Medium	Low
Improbable (E)	Medium	Medium	Medium	Low
Eliminated (F)	Eliminated			

High impact disruption
(in magnitude and/or frequency)

Probable

Risk
(expected case)
Insurance

External

Worst Case
(game theory)
Military

(c

Possible

Worst-case disruption
(as defined by system objective)

Build models to assess the capability of a system to deliver service under different scenarios

- **Attacker Models**: We identify worst-case disruptions
- **Defender Models**: We identify optimal investments to mitigate disruptions

- Risk and worst-case are primarily focused on **external events** and their impacts
- Assume systems **work as intended**

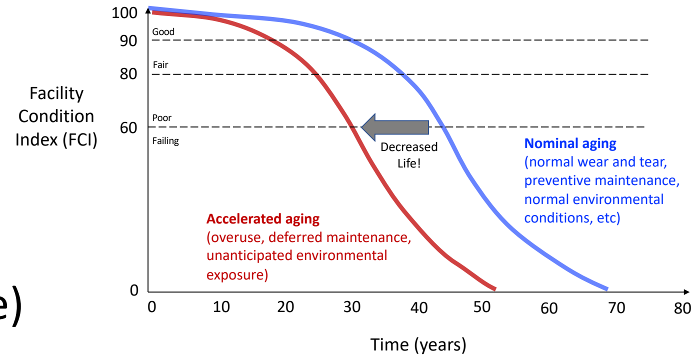
Reframing Vulnerability Analysis

- Reliability and Safety are primarily focused on **internal failures** and their impacts

- Assume that **systems have flaws**

Probable

Disruption to system function due to ***random failure*** of component(s)

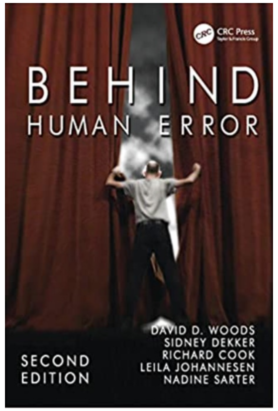


Reliability
(fault tolerance)
Engineering

Internal

Safety
(dealing with surprise)
Human Factors

Woods et al



Possible

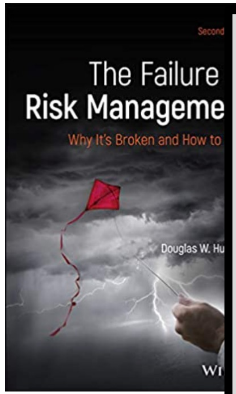
System works as designed but causes ***unintentional harm*** to people, assets, or environment

Reframing Vulnerability Analysis

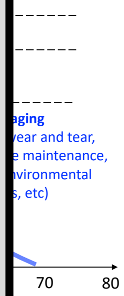
High impact disruption

Probable

Disruption to system function due



Hubbard



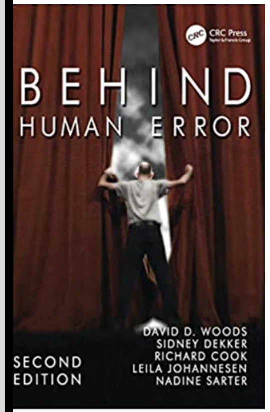
4 Vulnerability ***Perspectives***

- All perspectives relevant for vulnerability analysis
- Any single perspective simultaneously reveals and hides important features
- Each perspective can lead to different recommendations
- There is no "best" approach

Pitfalls in Analysis

- Each technique has known shortcomings
- Be aware of common pitfalls and misunderstandings

Build models
capability of
service unde
- **Attacker M**
  worst-case
- **Defender M**
  optimal inv
  mitigate dis

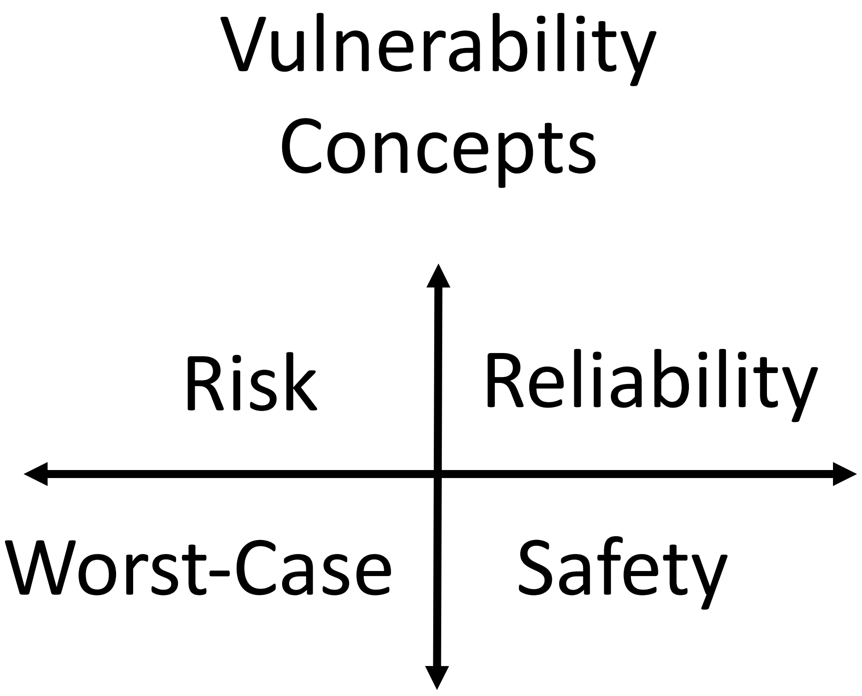


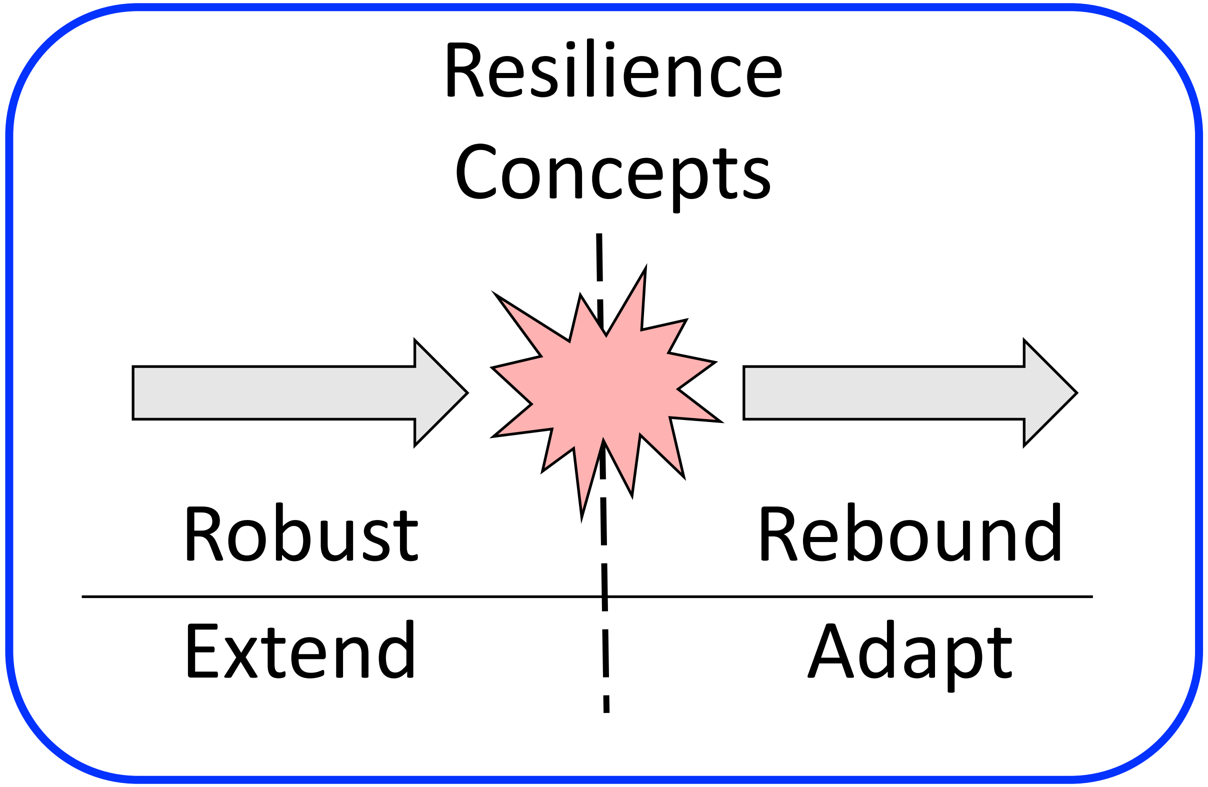
(as defined by system objective)

Possible

people, assets, or environment

Distinct perspectives on mission assurance



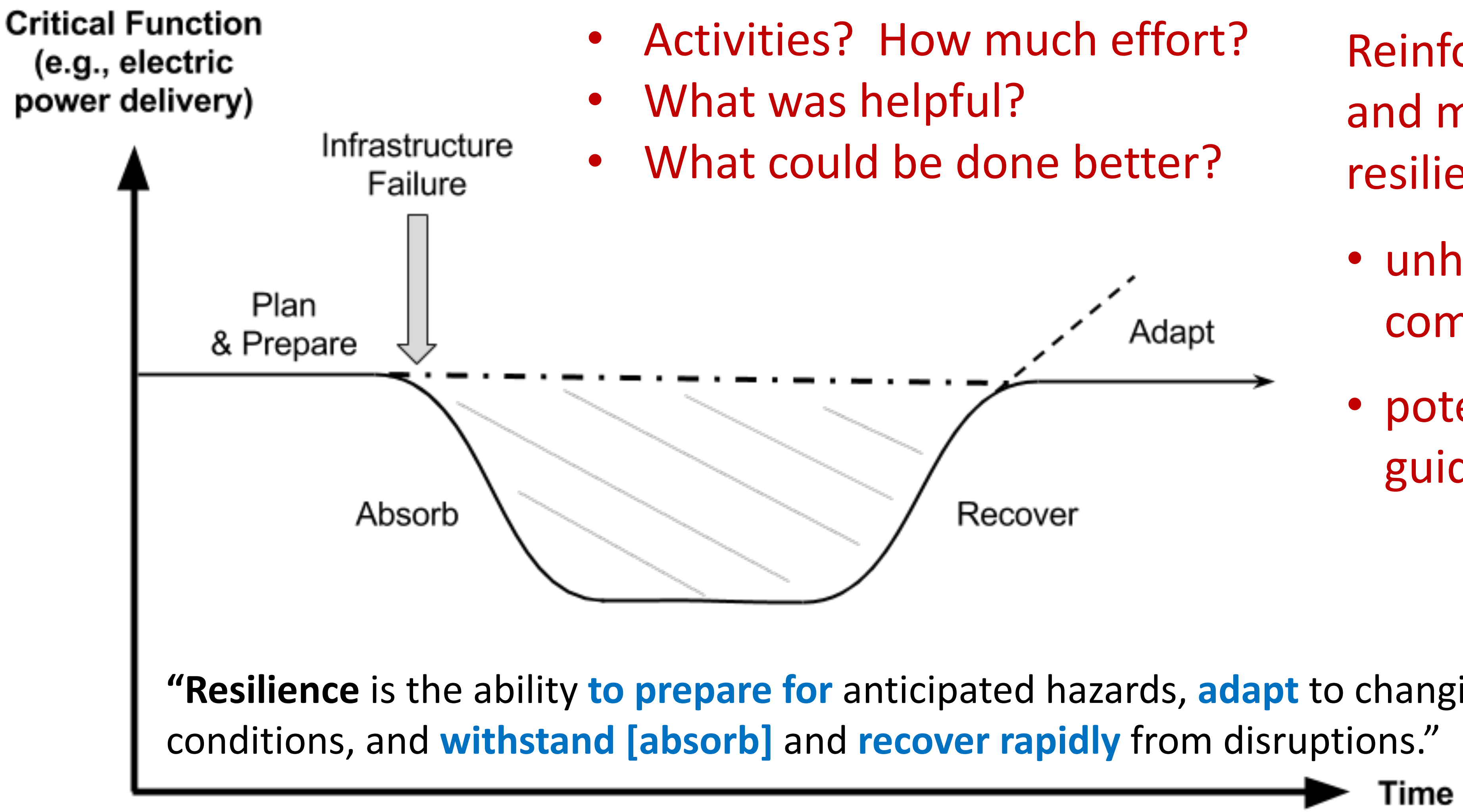


This reframing is joint work with Dan Eisenberg, NPS.

Making sense of "Resilience"

- The concept of resilience is <u>important</u> and <u>popular</u>
  - Represents a new societal need, particularly given frequent surprise
- Over the last 10+ years, it has been <u>overused</u> to mean many different things
  - It has bureaucratic definitions that are not helpful for assessing systems
  - The use of resilience as a term is noisy and confusing
- Our goal:
  - Provide a framework for thinking about different meanings of resilience
  - Illustrate with practical examples
  - Explain the tradeoffs that exist for different resilience goals

The "Resilience Curve" is a Poor Model of Resilience



Process-Outcome Confusion

- Activities? How much effort?
- What was helpful?
- What could be done better?

Reinforces oversimplifications and misconceptions about resilience

- unhelpful for understanding complex systems
- potentially dangerous for guiding decisions

"**Resilience** is the ability **to prepare for** anticipated hazards, **adapt** to changing conditions, and **withstand [absorb]** and **recover rapidly** from disruptions."

Official Definition for Resilience from NIST, DHS, FEMA, etc.

Four Notions of Resilience*

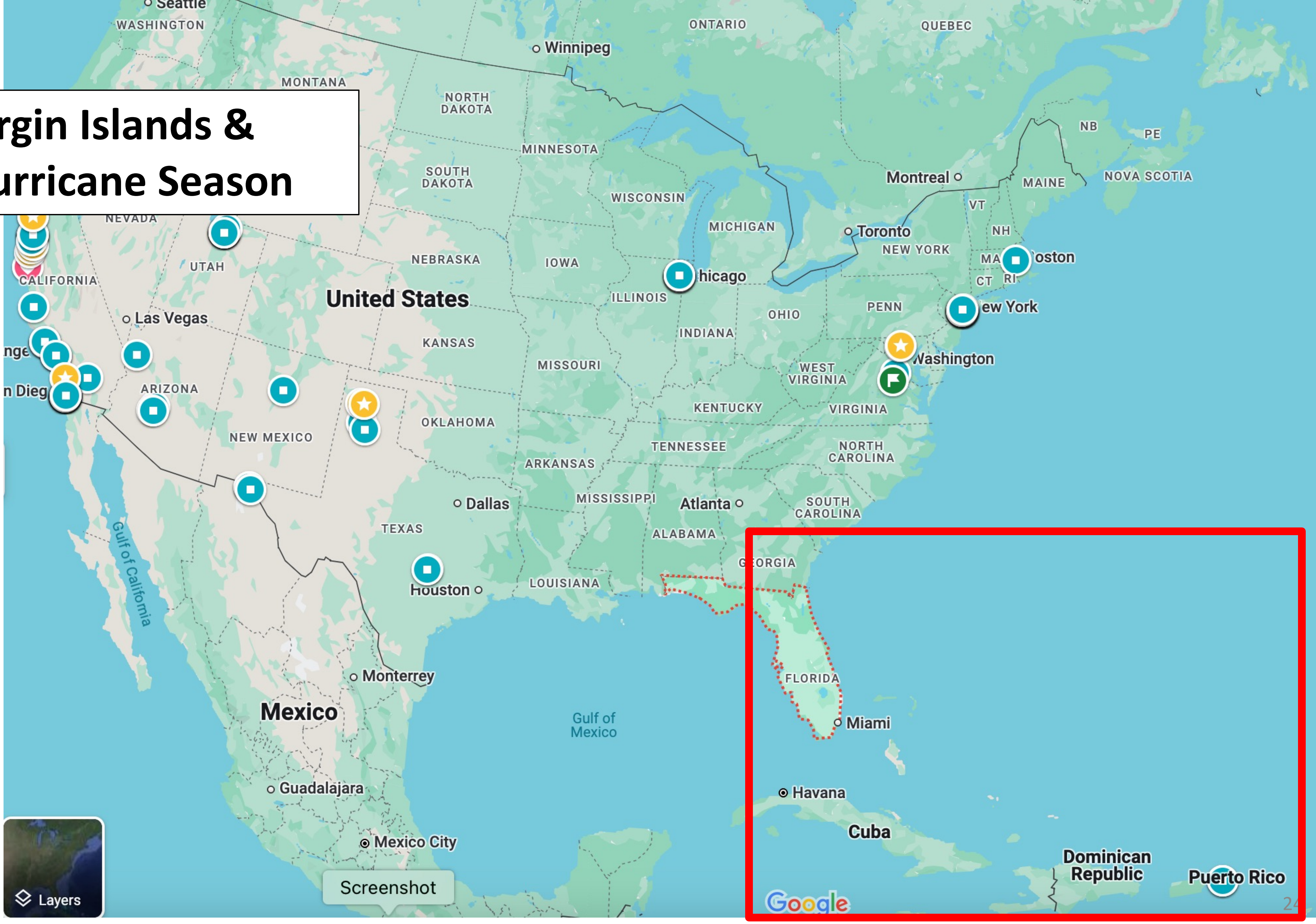
1. **Rebound** from traumatic events
2. **Robust** in the ability to adapt from well-modeled disruptions
3. **(Graceful) Extensibility** = the capacity to stretch/extend near and beyond system boundaries
4. **(Sustained) Adaptability** = manage adaptive capacities (via architectures, rules of governance) near hard limits in tradeoff spaces

* D.D. Woods, 2015, “Four concepts for resilience and the implications for the future of resilience engineering,” *Reliability Engineering and System Safety* 141: 5-9.

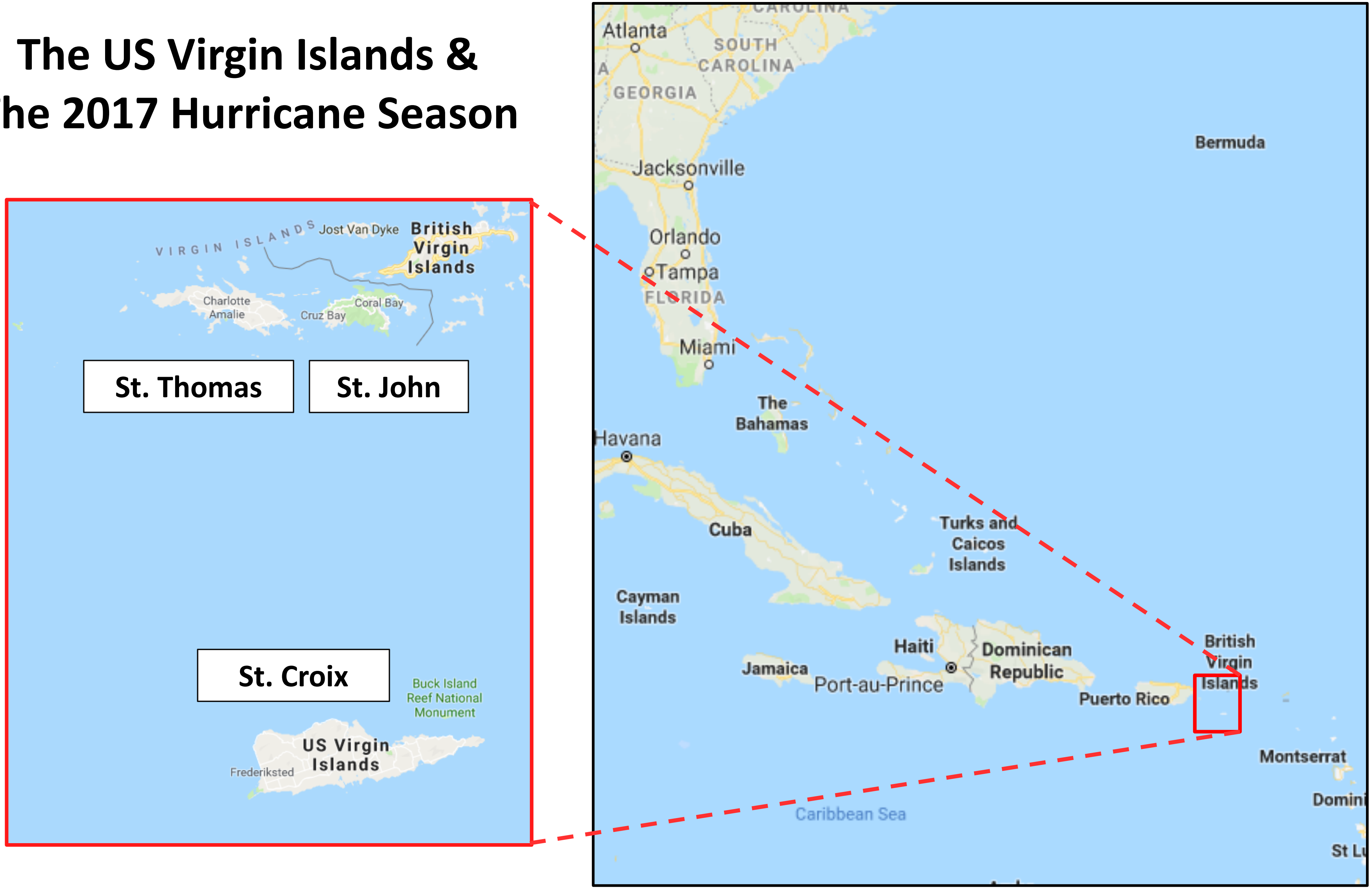
See also

Sharkey TC, Nurre Pinkley SG, Eisenberg DA, Alderson DL. "In search of network resilience: An optimization-based view," *Networks*. 2020;1-30. https://doi.org/10.1002/net.21996

The US Virgin Islands & The 2017 Hurricane Season

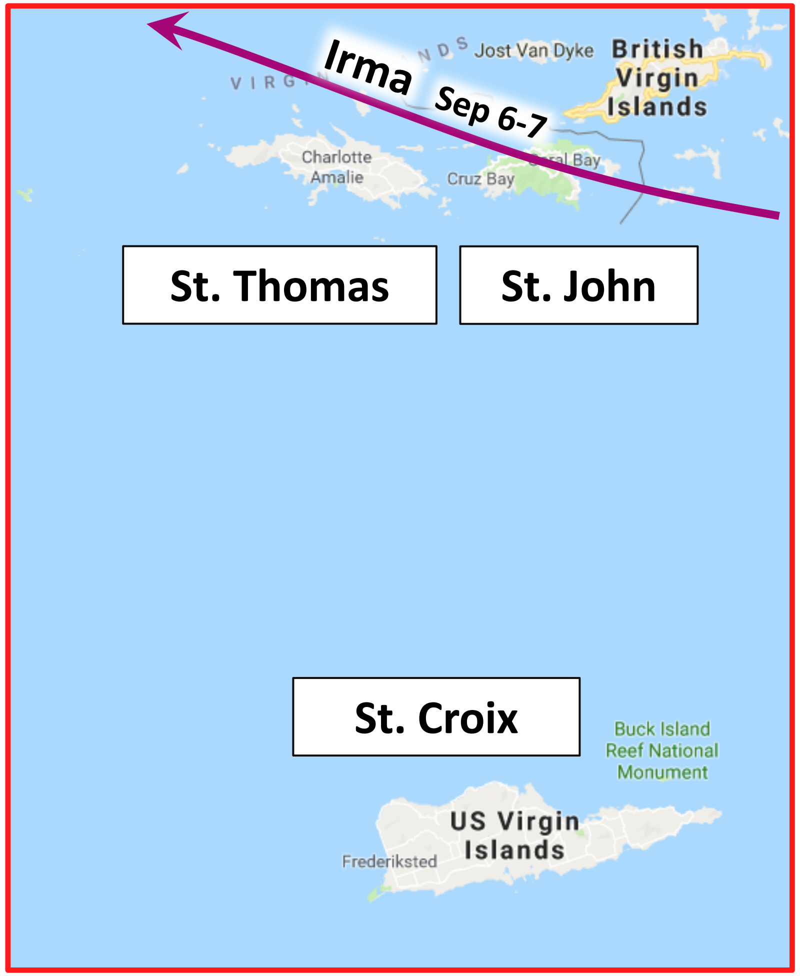


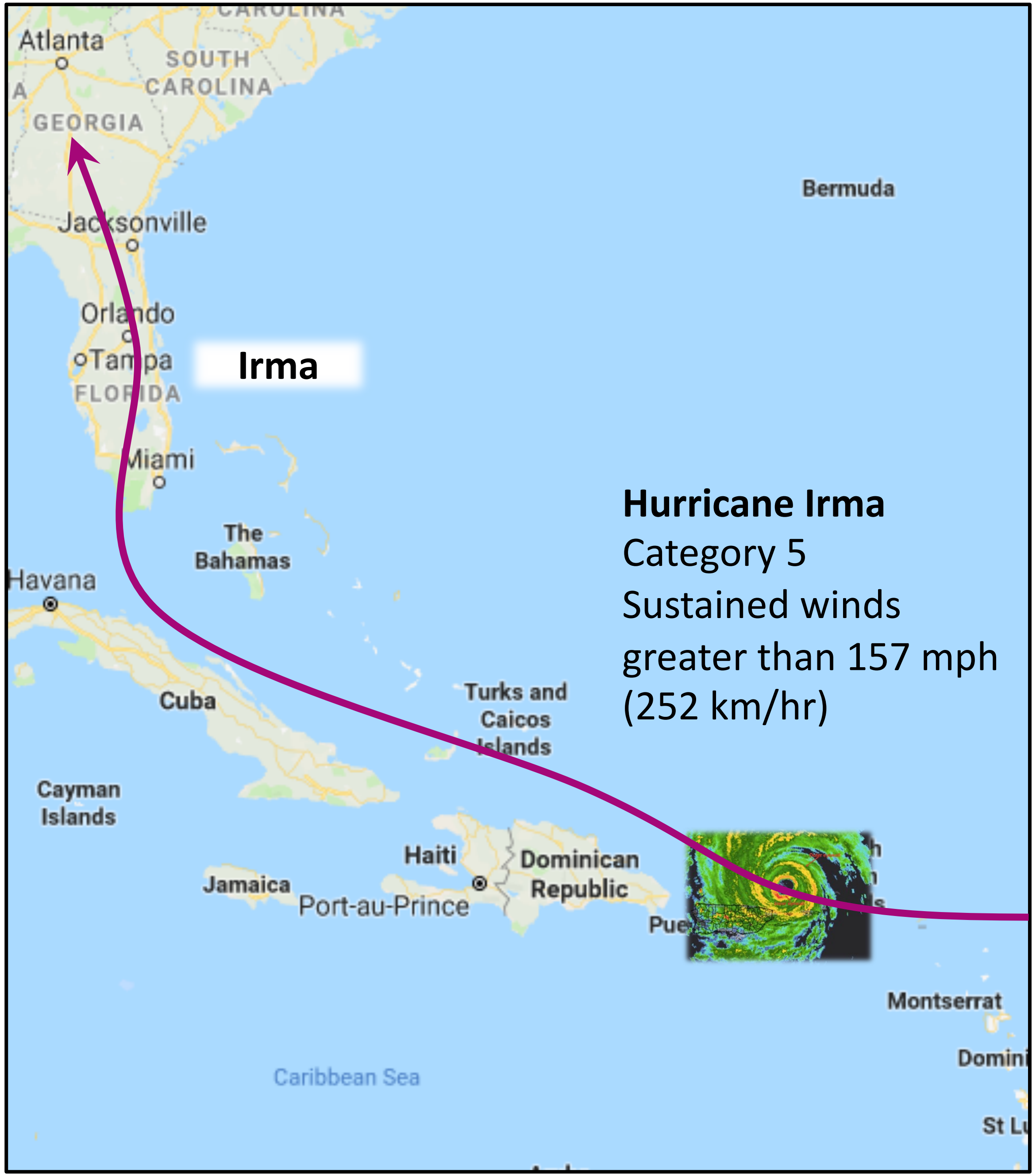
The US Virgin Islands & The 2017 Hurricane Season



Courtesy: Jeff Good

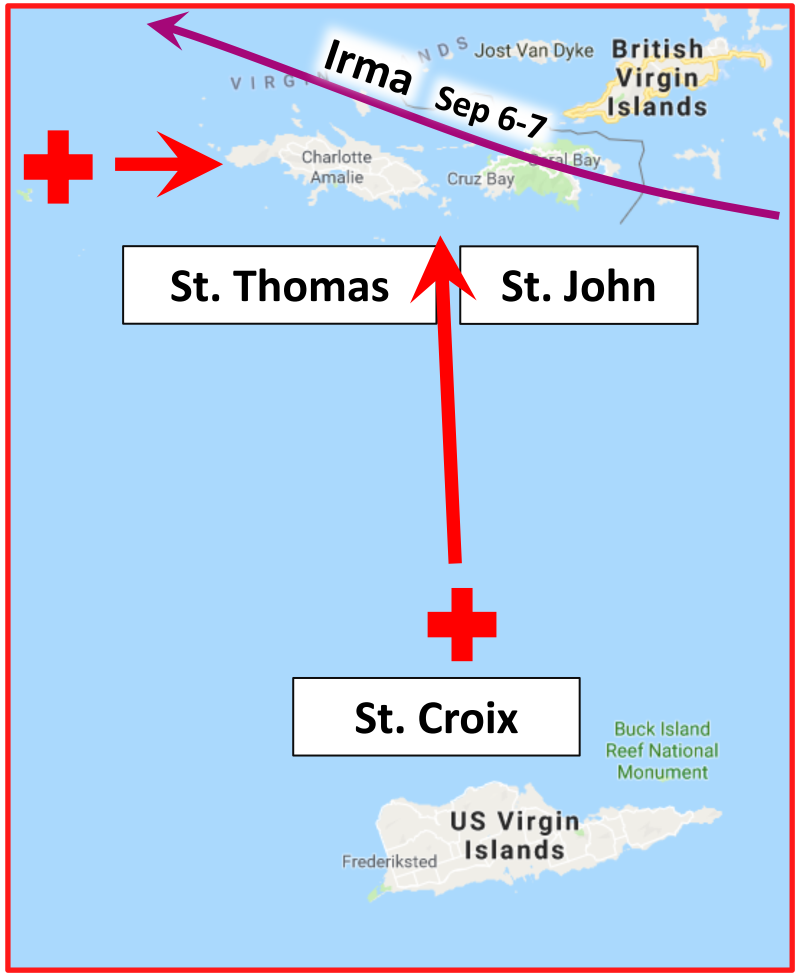
The US Virgin Islands &
The 2017 Hurricane Season





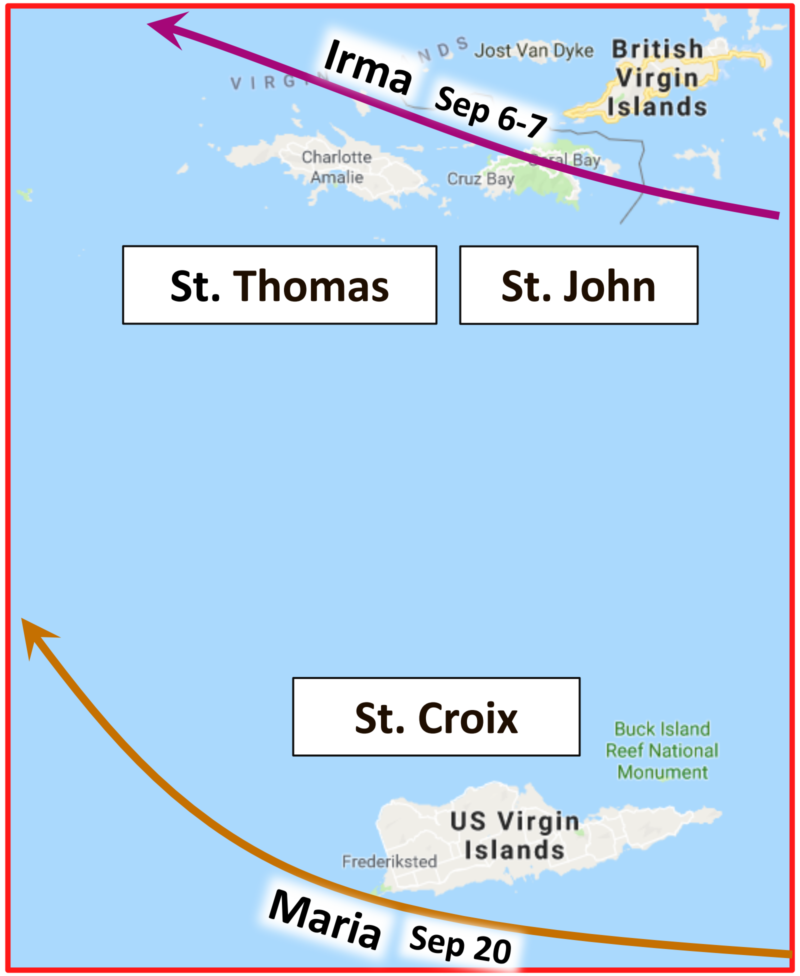
Courtesy:
Jeff Good

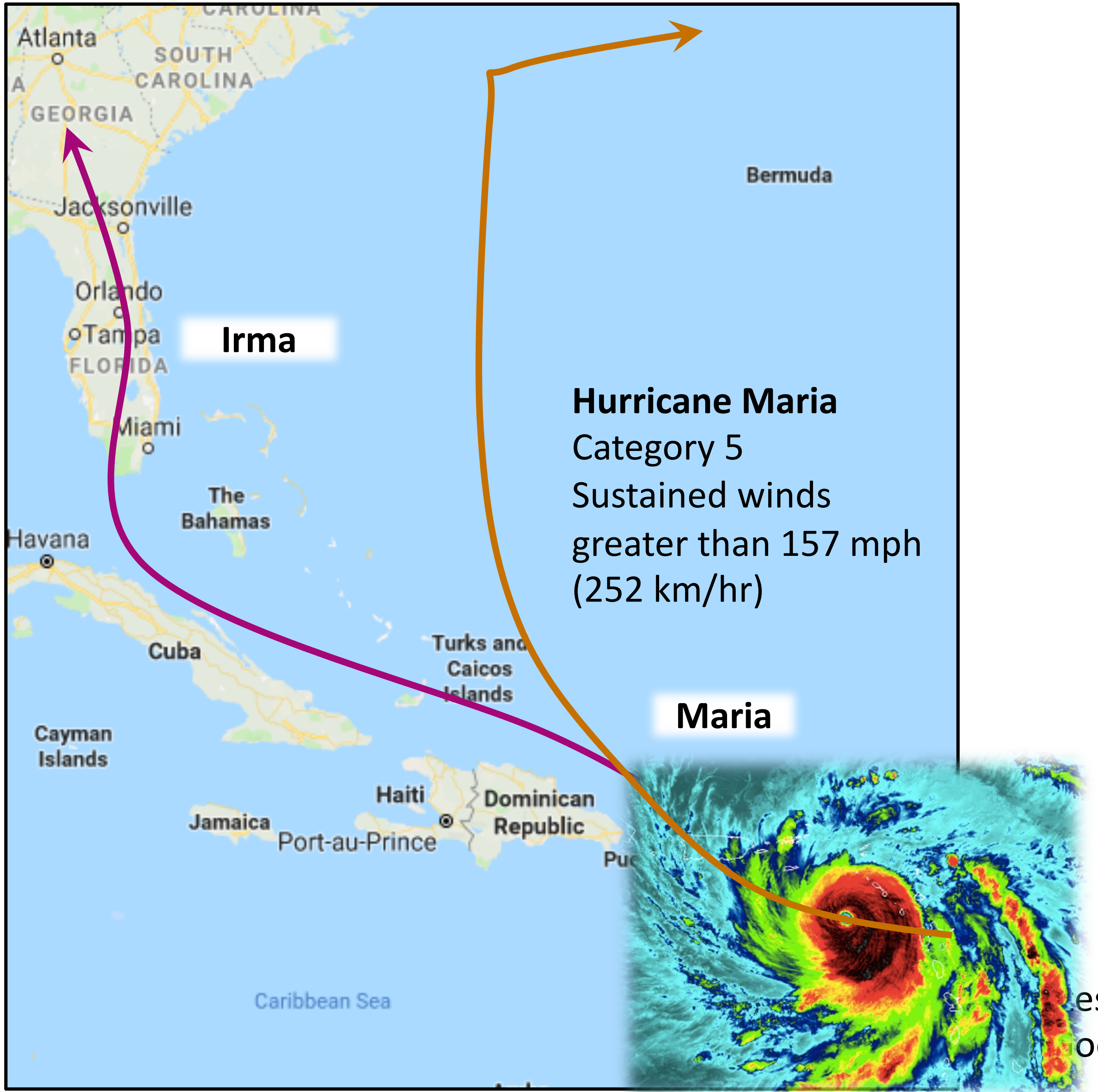
The US Virgin Islands &
The 2017 Hurricane Season



Courtesy:
Jeff Good

The US Virgin Islands & The 2017 Hurricane Season





esy:
ood

Following Hurricanes Irma and Maria
NPS was asked by FEMA to help if we could




Operational Resilience Analysis and Capacity Building in the USVI 2018-2021

Current Capabilities (St. Croix)

Electric Power Model

- **Determine optimal load shed to keep critical loads running**

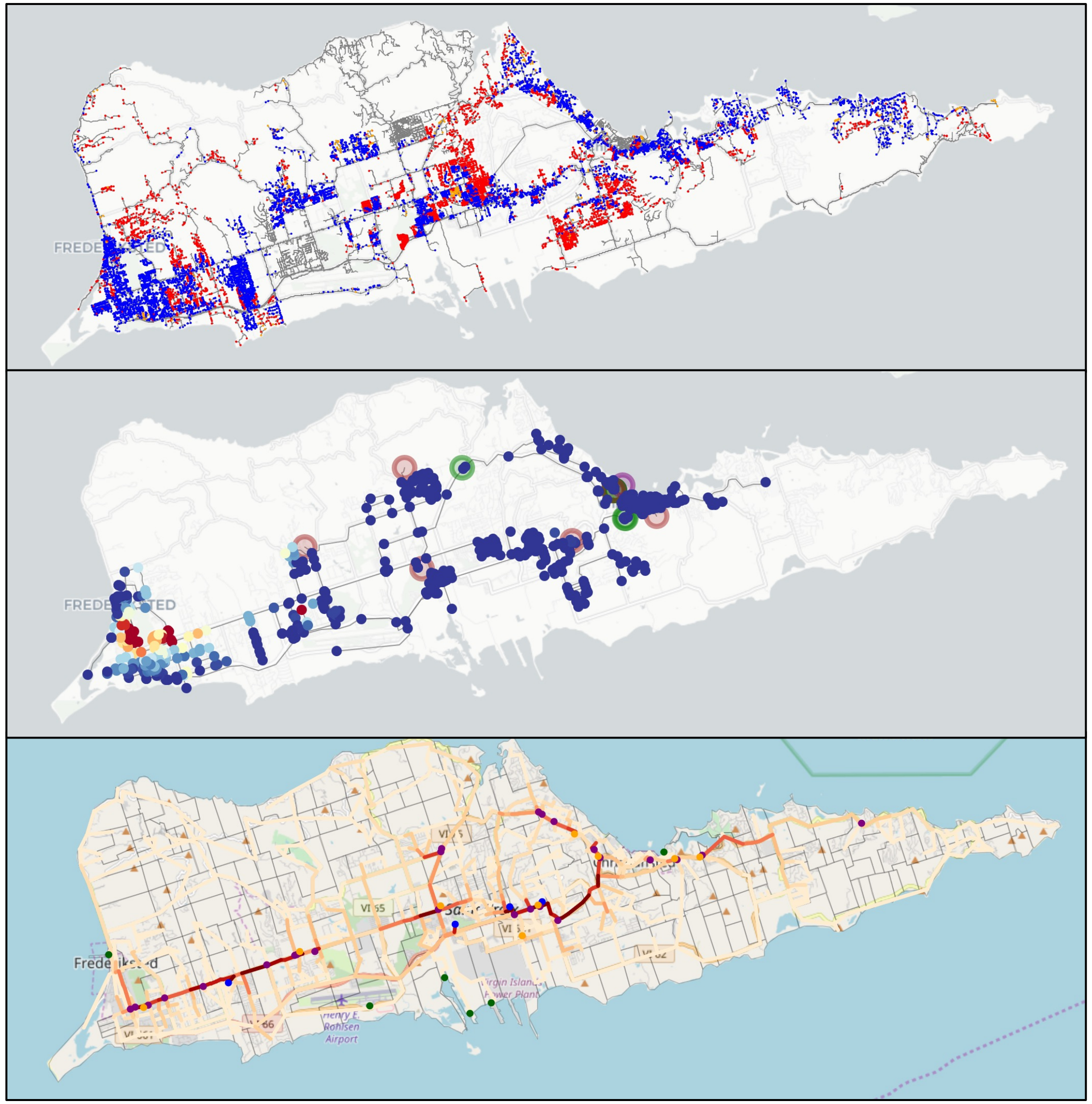
Water Distribution Model

- **Identify where water services will be lost when pumps & tanks fail**

Transportation Model

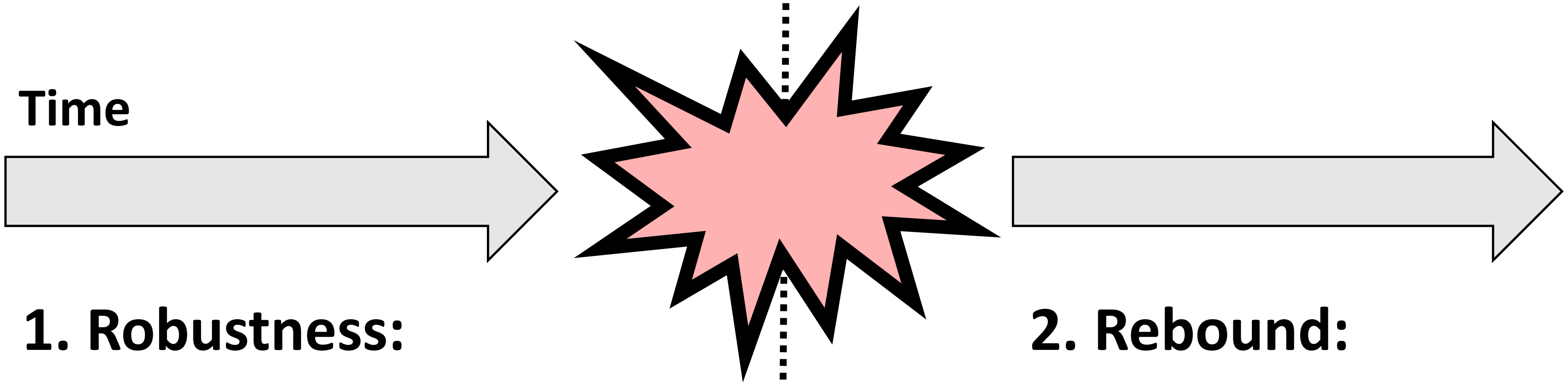
- **Measure optimal supply and roadway congestion post-disaster**

<u>Goal</u>: Assessing and improving operational resilience of individual infrastructure systems and their interdependent operation



Four key concepts of resilience

Pre-Event **Stressful Event** **Post-Event**



1. Robustness:
System *continues* to function as intended

2. Rebound:
System *returns* to previous function

Woods, David D. "Four concepts for resilience and the implications for the future of resilience engineering." Reliability Engineering & System Safety 141 (2015): 5-9.

1. Robustness: Composite Power Poles

https://viconsortium.com/VIC/?p=76179

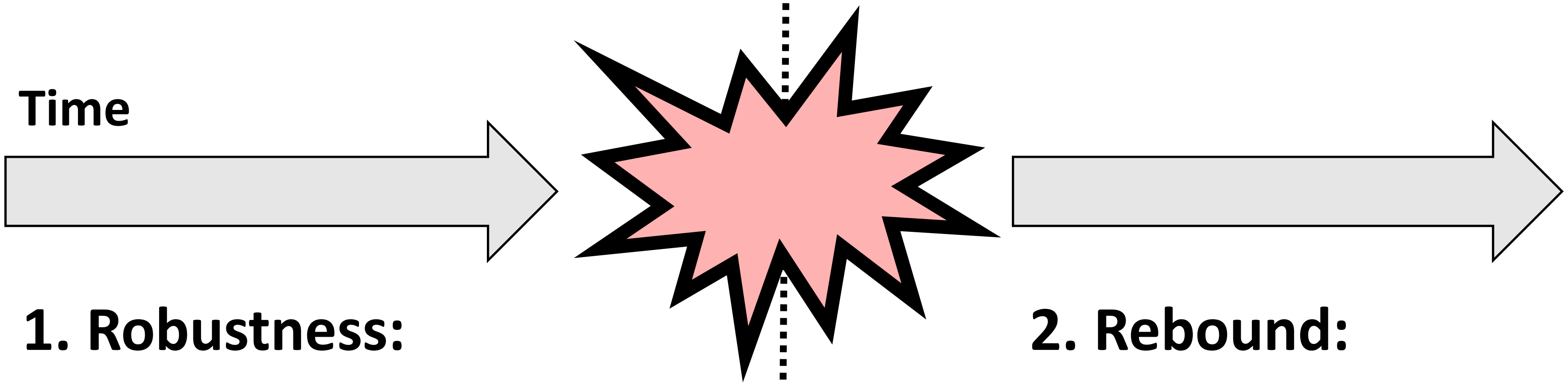
2. Rebound: Deployable Line Crews

https://www.hauglandgroup.us/projects/

Four key concepts of resilience

Pre-Event | **Stressful Event** | **Post-Event**

Time



1. Robustness:
System *continues* to function as intended

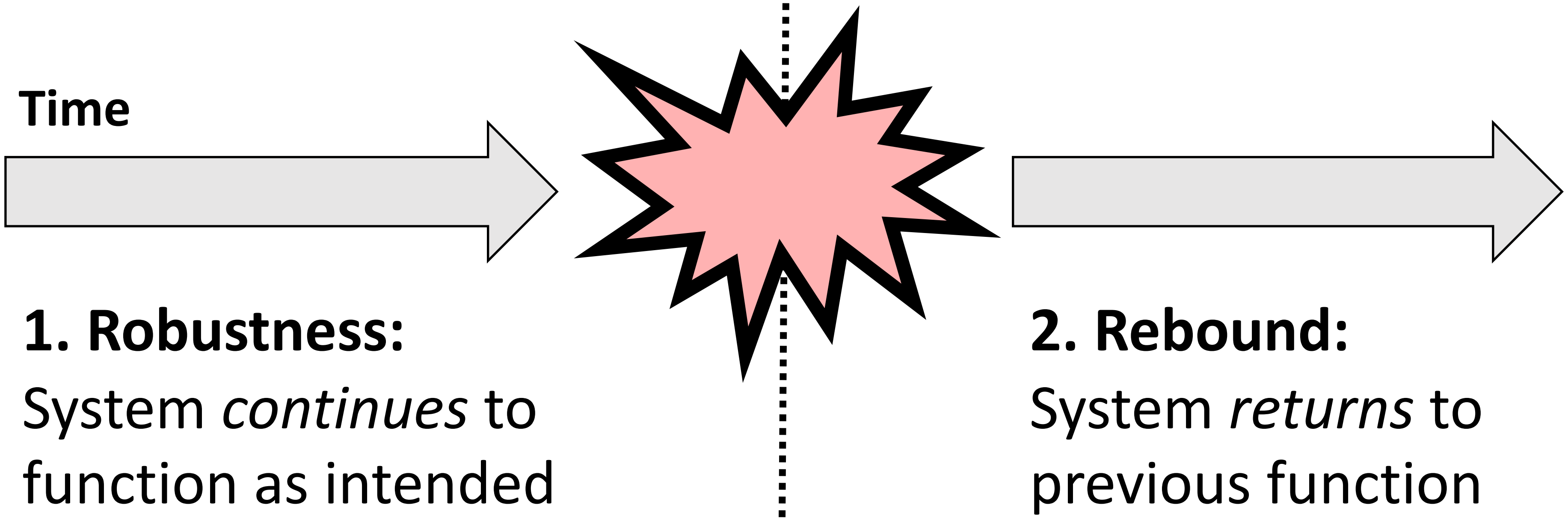
2. Rebound:
System *returns* to previous function

Woods, David D. "Four concepts for resilience and the implications for the future of resilience engineering." Reliability Engineering & System Safety 141 (2015): 5-9.

Four key concepts of resilience

Pre-Event | **Stressful Event** | **Post-Event**

Time



1. Robustness:
System *continues* to function as intended

2. Rebound:
System *returns* to previous function

Even if we prepare in this way, we will be surprised…

Woods, David D. "Four concepts for resilience and the implications for the future of resilience engineering." Reliability Engineering & System Safety 141 (2015): 5-9.

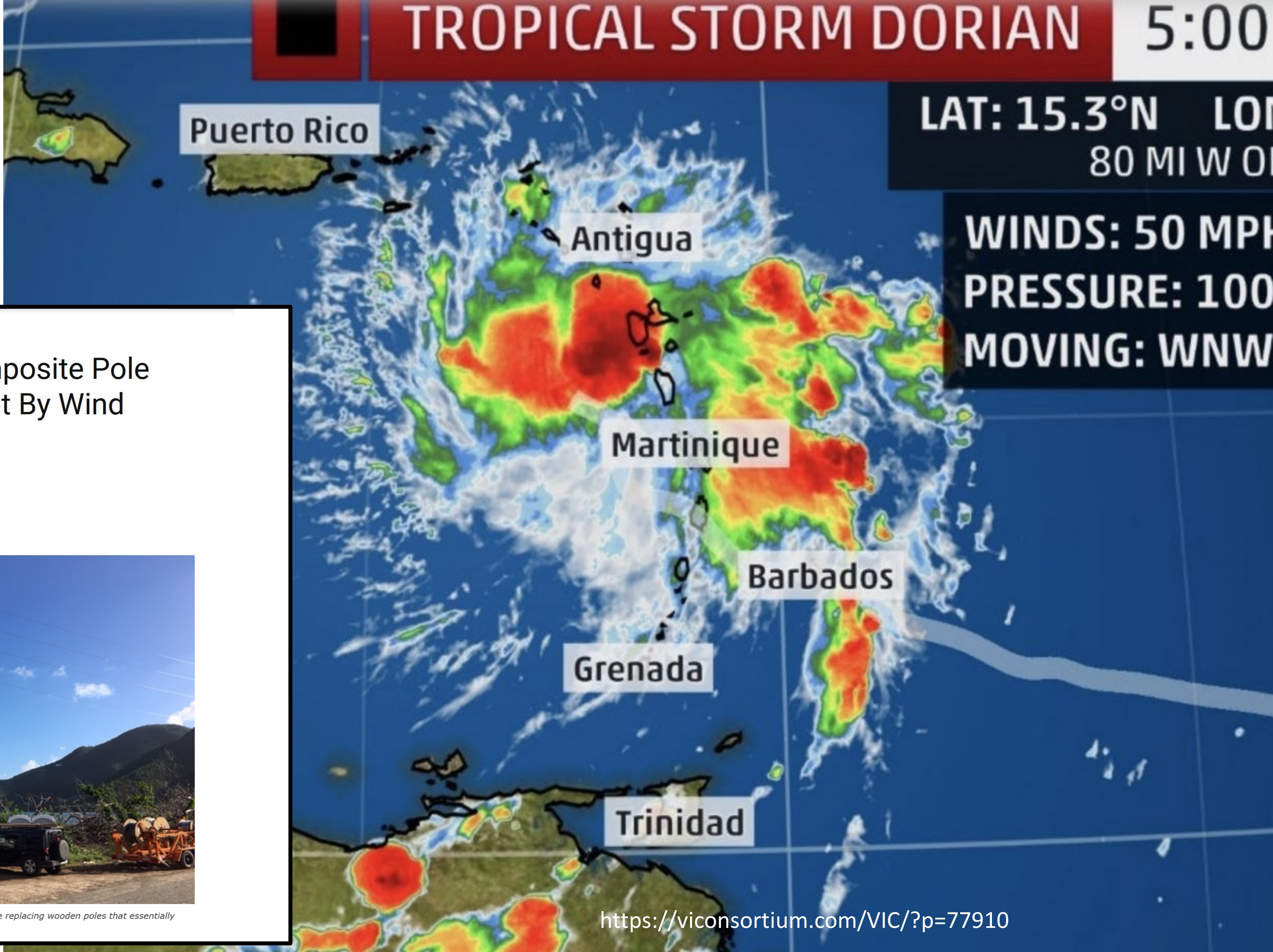
Surprise Happens…

News Local news

Hurricane Resistant Composite Pole Toppled in Dorian But Not By Wind *Correction*

Bill Kossler August 30, 2019

Workmen raise another composite pole on St. John. The new poles are replacing wooden poles that essentially haven't changed significantly in more than 100 years.



https://viconsortium.com/VIC/?p=77910

Four key concepts of resilience

Pre-Event | **Stressful Event** | **Post-Event**

Time

1. Robustness:
System *continues* to function as intended

2. Rebound:
System *returns* to previous function

3. Resilient systems **Extend:**
System function *stretches* to support new needs

4. Resilient systems **Adapt:**
System *changes* to function in new ways

Woods, David D. "Four concepts for resilience and the implications for the future of resilience engineering." Reliability Engineering & System Safety 141 (2015): 5-9.

3. Extending function: e.g., Emergency Generators

https://www.ecmag.com/section/your-business/backup-generators-anew

Does having an emergency generator make you resilient?

- Not if you don't have fuel
- Not if you don't know how to use it
- Not if you have not maintained it

Key Idea

Resilience is not what you ***have***

Resilience is what you ***do***

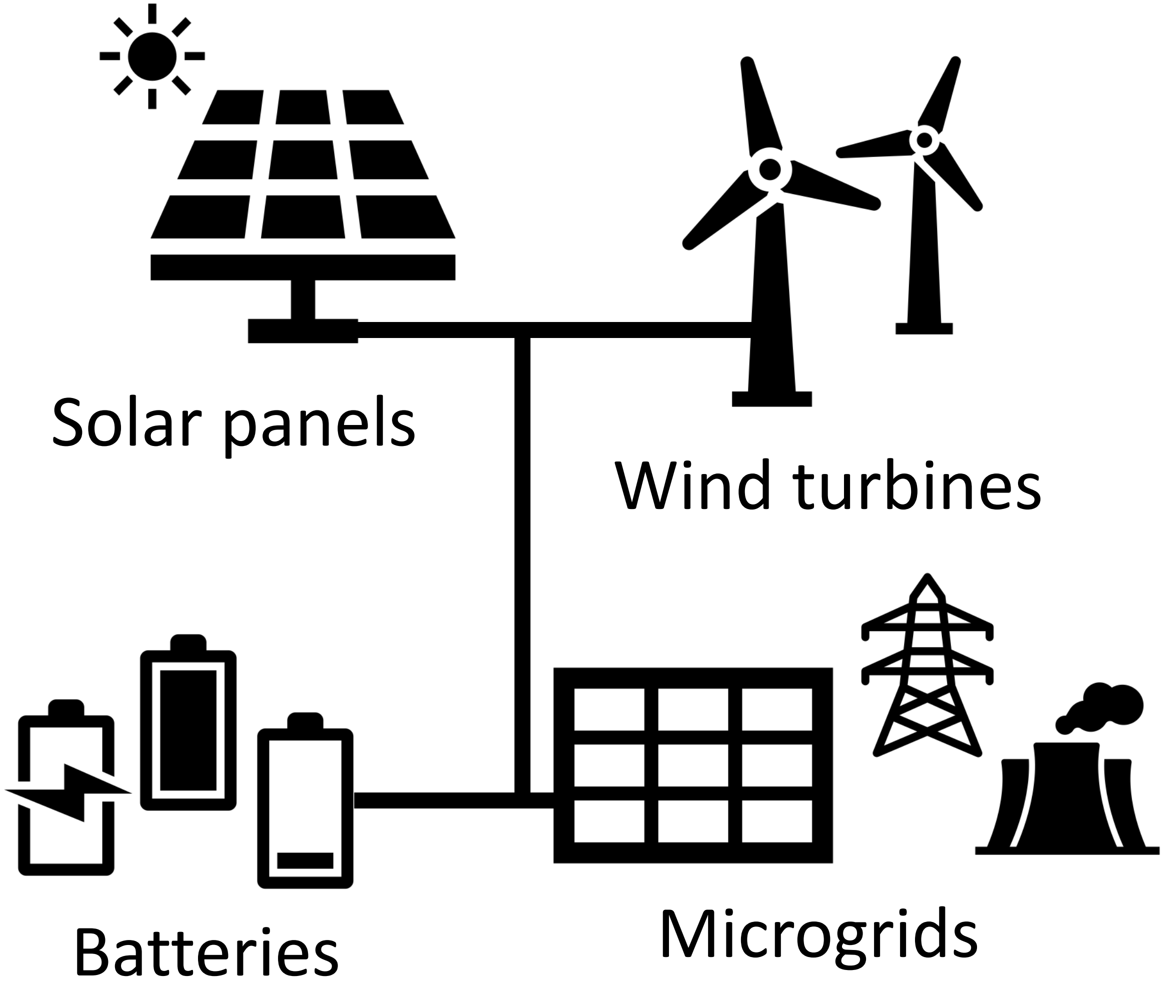
Think of resilience as a verb, not a noun!

~~resiliency~~

3. Extending function: e.g., Emergency Generators

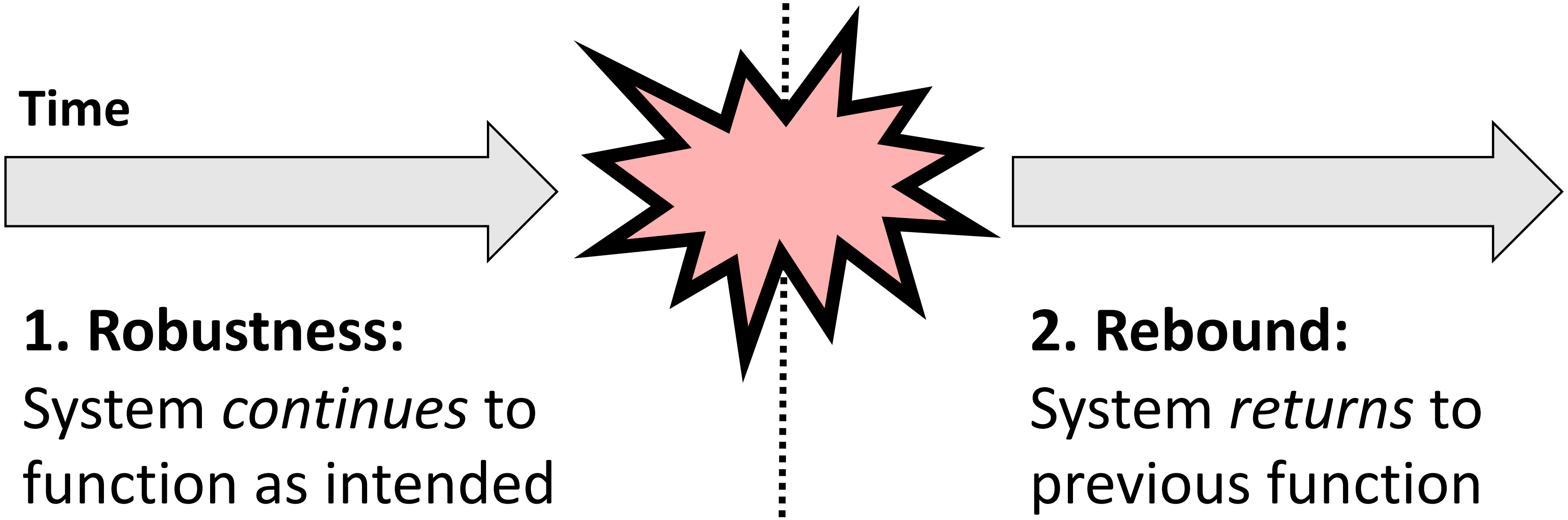
https://www.ecmag.com/section/your-business/backup-generators-anew

4. Adapting the system: Re-configuration of components



Four key concepts of resilience

Pre-Event | **Stressful Event** | **Post-Event**



1. Robustness:
System *continues* to function as intended

"Keep things the same"

2. Rebound:
System *returns* to previous function

3. Resilient systems **Extend:**
System function *stretches* to support new needs

"Embrace the new"

4. Resilient systems **Adapt:**
System *changes* to function in new ways

Four key concepts of resilience

"Keep thing
the same"

"Embrace
the new"

- These four notions of resilience are distinct
- They are not merely additive
- There are tradeoffs between them
- Focusing on one can leave to us blind to the others
- Investing in one might come at the expense of another
- We should be aware of these tradeoffs
- Beware of simple scoring mechanisms

Any single perspective
simultaneously ***reveals*** and ***obscures***

We must be able to ***shift perspectives***
if we are to avoid blind spots

The Premise…

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify ***vulnerabilities***
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build ***resilience***…
- …and assure the mission!

…This Is Not Working!!

Journal of Critical Infrastructure Policy • Volume 2, Number 2 • Fall / Winter 2021

Strategic Perspectives

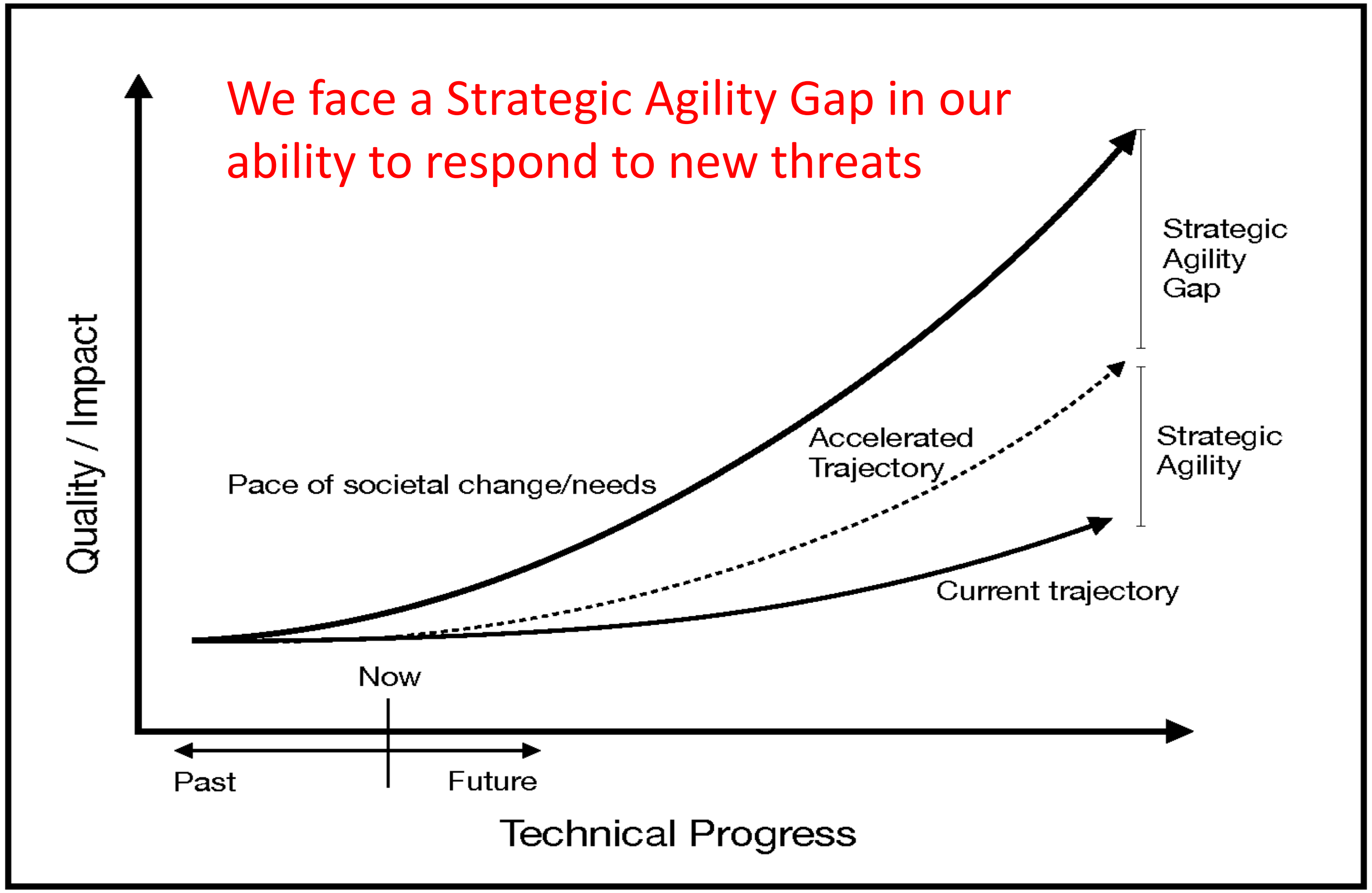
Progress toward Resilient Infrastructures: Are we falling behind the pace of events and changing threats?

David D. Woods[1] and David L. Alderson[2]

[1] Professor Emeritus, Dept of Integrated Systems Engineering, Ohio

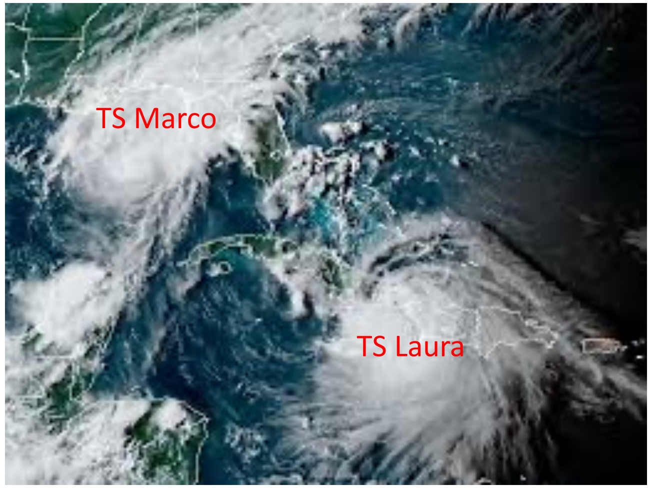
[2] Professor, Operations Research Dept, Naval Postgraduate School, d

- Growing system complexity
- New conflicts & threats
- Changing environment
- Changing tempos of activity



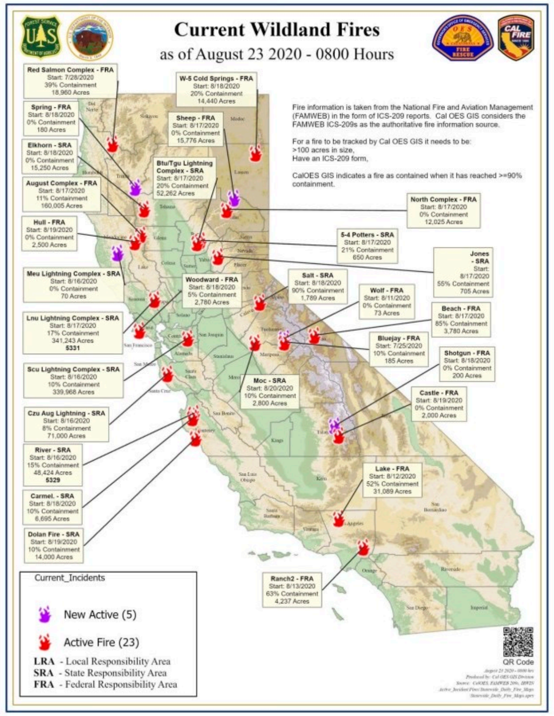
We are living in a world of [climate-driven] surprise.

Simultaneous Hurricanes?



August 23, 2020: ***"The temporal proximity and the geographic proximity of these storms pose a challenge that, quite frankly, we've not seen before,"*** *[Louisiana Governor] Edwards said Sunday.* ***"As a result, we don't know exactly what to expect,"*** *he said, warning it's a "very serious situation."*

https://www.npr.org/2020/08/23/905231988/louisiana-braces-for-one-two-punch-of-storms-as-marco-and-laura-approach-shore



More Destructive Fires?

Aug. 25, 2020: ***The fiery consequences of extreme heat are not a surprise****. In fact, [UCLA researcher Daniel] Swain co-authored a paper that came out just last week with a remarkably prescient and straightforward title: "Climate change is increasing the likelihood of extreme autumn wildfire conditions across California."* ***The timing is a shock****, however, since autumn is still a month away.*

https://www.mercurynews.com/2020/08/25/californias-climate-tinderbox-a-scientist-explains-the-fire-crisis/

Colder Deep Freeze?

WEATHER

Crushing deep freeze was expected but US was unprepared, weather experts say

Meteorologists started sounding warnings two weeks before the storms that crippled Texas and other parts of the U.S., and yet catastrophe happened.

Feb. 19, 2021: ***This week's killer freeze in the U.S. was no surprise.*** *Government and private meteorologists saw it coming, some nearly three weeks in advance. They started sounding warnings two weeks ahead of time. They talked to officials. They issued blunt warnings through social media.*

And yet catastrophe happened. At least 20 people have died and 4 million homes at some point lost power, heat or water.

By Seth Borenstein, Associated Press Science Writer

"Stationarity is dead."

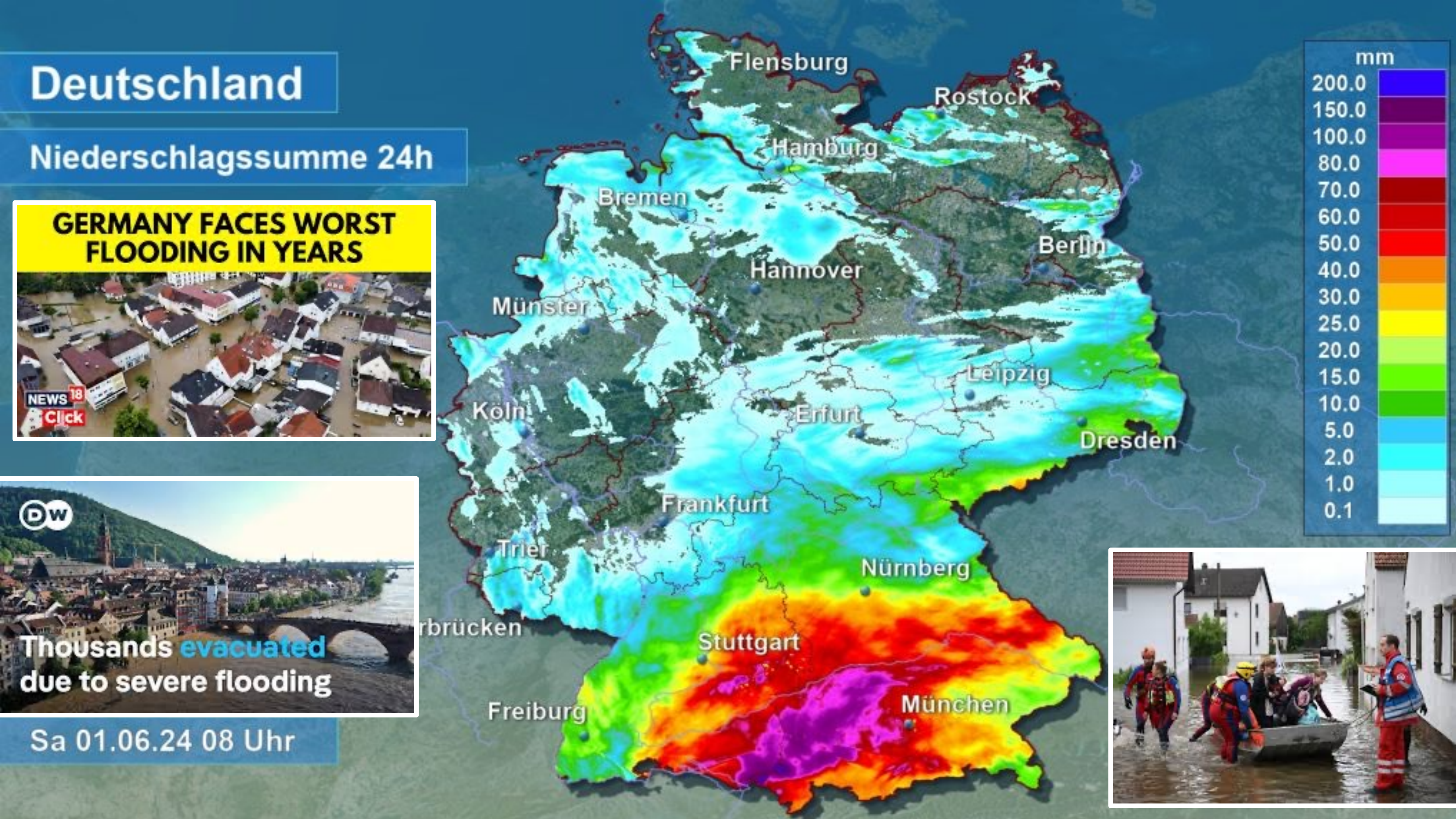
Milly, P., Julio, B., Malin, F., Robert, M., Zbigniew, W., Dennis, P., Ronald, J., 2007. Stationarity is dead. Ground Water News & Views 4, 6–8.


Countries affected by Storm Boris
Flooding reported
Water levels rising
POLAND
CZECH REPUBLIC
SLOVAKIA
AUSTRIA
ROMANIA
ITALY
HUNGARY
CROATIA
BBC


NEWS18
EASTERN EUROPE SEES WORST FLOOD IN DECADES


NEWS18
LIVE
SEVERE FLOODS INUNDATE POLAND


The Indian EXPRESS
News
Central Europe Flood Crisis
EU Commits Billions for Aid


Deutschland
Niederschlagssumme 24h
GERMANY FACES WORST FLOODING IN YEARS
NEWS18 Click
DW
Thousands evacuated due to severe flooding
Sa 01.06.24 08 Uhr
Flensburg
Rostock
Hamburg
Bremen
Berlin
Hannover
Münster
Leipzig
Köln
Erfurt
Dresden
Frankfurt
Trier
Nürnberg
rbrücken
Stuttgart
Freiburg
München
mm
200.0
150.0
100.0
80.0
70.0
60.0
50.0
40.0
30.0
25.0
20.0
15.0
10.0
5.0
2.0
1.0
0.1

The Premise…

- We can map out our infrastructure systems
- And their dependencies
- And ***model*** their operation
- To identify vulnerabilities
- Then fill holes and/or block cascading consequences
- And doing all this will allow us to build resilience…
- …and assure the mission!

…This Is Not Working!!

- We don't know our systems in their absolute entirety, and we never will!
- There is no single vantage point from where we can "see" everything
- And things are always changing
- There will always be hidden dependencies
- There will always be surprises!

Conclusions

We need to reframe how we think about resilience.

We should stop using an emergency management / risk mindset.

We need the **audacity to avoid FBC pressures**

and **stop building lean, efficient, fragile systems!**

We need to be brave and let go of what has not been working.

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***

Conclusions

We need to reframe how we think about resilience.

We should stop using an emergency management / risk mindset.

We need the **audacity to avoid FBC pressures**

and **stop building lean, efficient, fragile systems!**

We need to be brave and let go of what has not been working.

We need a different type of **architecture** for our mission critical systems.

One that goes beyond traditional optimization and design.

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

We cannot escape the complexity traps if we don't build **adaptive capacity**.

adaptive capacity

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

A Final Provocation

- You NEVER have complete knowledge of the system
- The system and its dependencies are ALWAYS evolving
- Better planning and forecasting will not get around this
- New technologies (e.g., AI/ML) will not get around this
- You WILL be surprised

- Business-as-usual in infrastructure research WILL make a good career…
- …But it WILL NOT change anything

- We need to find a better way. We need an ACT III. What will you do?

The End

Contact Information

- Dr. David Alderson

Executive Director, Center for Infrastructure Defense

Naval Postgraduate School

dlalders@nps.edu

http://faculty.nps.edu/dlalders

- NPS Center for Infrastructure Defense

http://www.nps.edu/cid

Additional References (1 of 2)

- Woods DD, Alderson DL, 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
- Sharkey TC, Nurre Pinkley SG, Eisenberg DA, Alderson DL, 2020. **"In search of network resilience: An optimization-based view,"** Networks. 2020;1-30. https://doi.org/10.1002/net.21996
- Woods, D.D. (2019). **Essentials of Resilience, Revisited**. In M. Ruth and S. G. Reisemann (Eds)., Handbook on Resilience of Socio-Technical Systems. Edward Elgar Publishing, pp. 52-65.
- Eisenberg, D.A., Seager, T.P., and Alderson, D.L., 2019, **"Rethinking Resilience Analytics,"** Risk Analysis, 39(9): 1870-1884.
- Woods, D. D. (2018). **The Theory of Graceful Extensibility: Basic rules that govern adaptive systems.** Environment Systems and Decisions, 38(4), 433-457.
- Woods, David D. **"Four concepts for resilience and the implications for the future of resilience engineering."** Reliability Engineering & System Safety 141 (2015): 5-9.

This work was supported by the Office of Naval Research, the Air Force Office of Scientific Research, the Defense Threat Reduction Agency, and the DOD Strategic Environmental Research and Development Program.

Additional References (2 of 2)

- Alderson, D.L., 2018, **"Overcoming Barriers to Greater Scientific Understanding of Critical Infrastructure Resilience, I**n M. Ruth & S. G. Reisemann (Eds), *Handbook on Resilience of Socio-technical Systems*, Edward Elgar Publishing.
- Salmerón, J., Alderson, D.L, and Brown, G.G., 2018, **"Resilience Report: Analysis of Hawaiian Electric Power Grid Vulnerability to Physical Attack (U)"**, Naval Postgraduate School Technical Report NPS-OR-18-001R, February.
- Alderson, D.L., Brown, G.G., Dell, R.F., Witwer, T.M., 2017, **"Studies of the Fuel Supply Chain in the Pacific Area of Responsibility (U),"** NPS Technical Report NPS-OR-17-003R, October.
- Alderson, D.L., Brown, G., and Carlyle, W.M., 2015, **"Operational Models of Infrastructure Resilience,"** *Risk Analysis* 35(4): 562-586 (received Award for Best Paper of 2015 in Risk Analysis).
- Alderson, D.L., G.G. Brown, W.M. Carlyle. 2014. **"Assessing and Improving Operational Resilience of Critical Infrastructures and Other Systems."** A. Newman, J. Leung, eds., *Tutorials in Operations Research: Bridging Data and Decision*. Institute for Operations Research and Management Science, Hanover, MD, 180-215.
- Alderson, D.L., G.G. Brown, W.M. Carlyle, L.A. Cox. 2013. **"Sometimes there is no 'most vital' arc: assessing and improving the operational resilience of systems."** *Military Operations Research* 18(1) 21-37.
- Brown, G., Carlyle, M., Salmerón, J. and Wood, K., 2006, **"Defending Critical Infrastructure,"** *Interfaces*, 36, pp. 530-544.

This work was supported by the Office of Naval Research, the Air Force Office of Scientific Research, the Defense Threat Reduction Agency, and the DOD Strategic Environmental Research and Development Program.

If we all agree on resilience, why don't we have it already?

Four barriers to resilience

1. AWARENESS: we don't know we need it
2. KNOWLEDGE: we don't know how to create it
3. INCENTIVES: We can't justify the investment in it
4. GOVERNANCE: Incompatibilities across organizational boundaries that lead to working at cross purposes

REFS:
Alderson, D.L., 2019, Overcoming Barriers to Greater Scientific Understanding of Critical Infrastructure Resilience, in M. Ruth & S. G. Reisemann (Eds), Handbook on Resilience of Socio-technical Systems, Edward Elgar Publishing, Northampton, MA.
Flynn, S.E. (2015), 'Bolstering critical infrastructure resilience after Superstorm Sandy: lessons for New York and the nation', Global Resilience Institute, Northeastern University, Boston, MA.