October 18, 2022

Sam Chanoski
Idaho National Laboratory

Always look on the bright side of life
Taking a different perspective on cybersecurity performance

Battelle Energy Alliance manages INL for the
U.S. Department of Energy's Office of Nuclear Energy

INL Idaho National Laboratory

INL/CON-22-69772

First, Some HOP Concepts

Proven approaches from some of the leading minds in Safety

Dr. Todd Conklin

- Senior Advisor, Los Alamos National Laboratory

- PhD in Organizational Communication, University of New Mexico

- If you read one thing: *Pre-Accident Investigations: An Introduction to Organizational Safety* (2012)

"We don't design human error *out* of our work systems."

Conklin, T. Pre-Accident Investigations: Better Questions
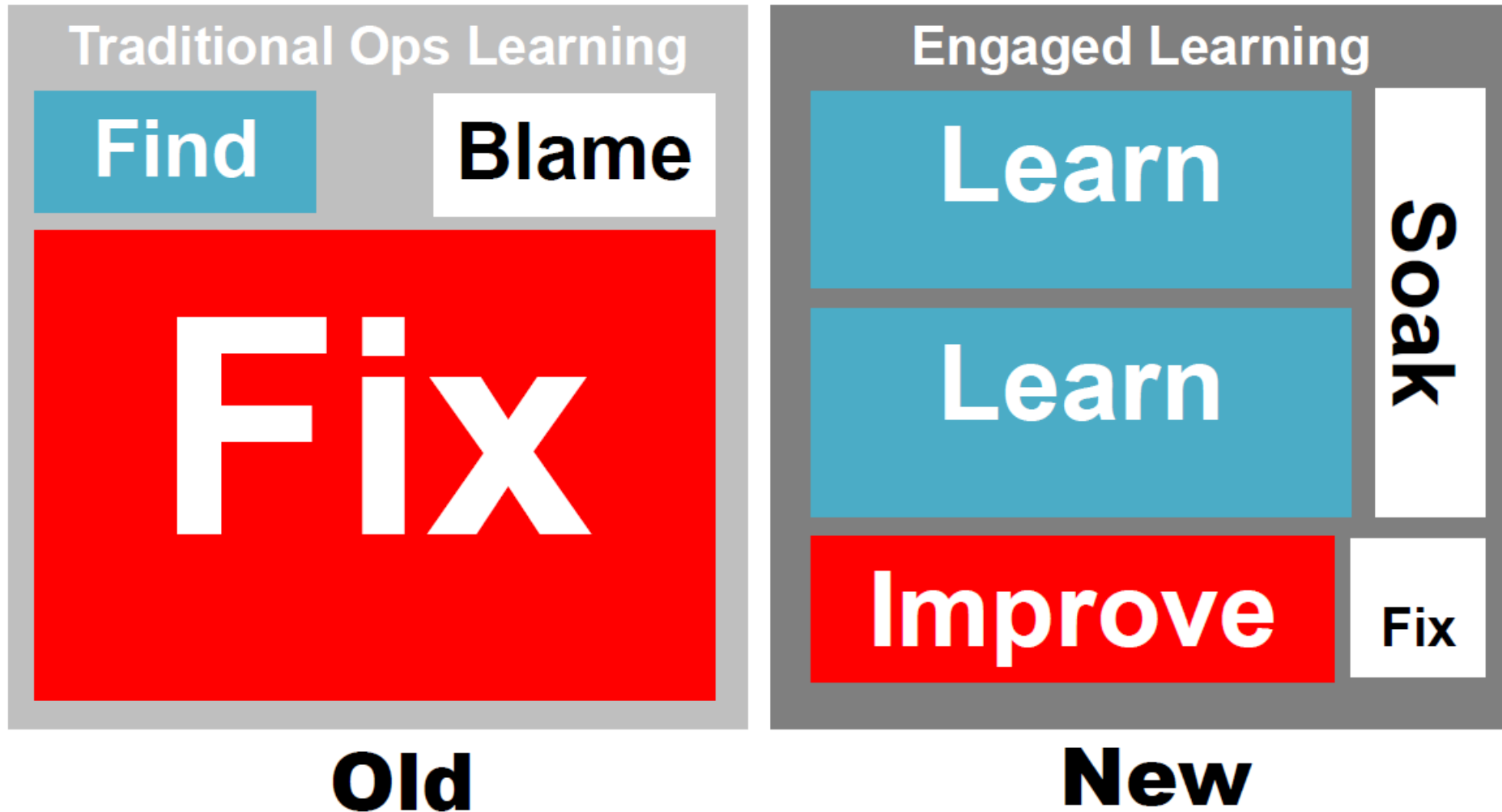
IDAHO NATIONAL LABORATORY

Human Performance is a Systems issue

"We don't design human error *out of* our work systems."

"We design human error *into* our work systems."

Conklin, T. Pre-Accident Investigations: Better Questions

IDAHO NATIONAL LABORATORY

Learning from events and incidents

Traditional Ops Learning
Find
Blame
Fix

Engaged Learning
Learn
Learn
Soak
Improve
Fix

Old

New

Conklin, T. Pre-Accident Investigations: Better Questions

"Safety is not the absence of accidents."

Conklin, T. Pre-Accident Investigations: Better Questions

What is Safety?

"Safety is not the absence of accidents."

"Safety is the presence of capacity."

Conklin, T. Pre-Accident Investigations: Better Questions

The role of our Workforce

The **Change** in How We Think about Workers

Historical

- Outsiders
  - not responsible
  - not smart
  - should stay in their place
- Uninformed
- Automatons
- Single issue
- Shallow knowledge
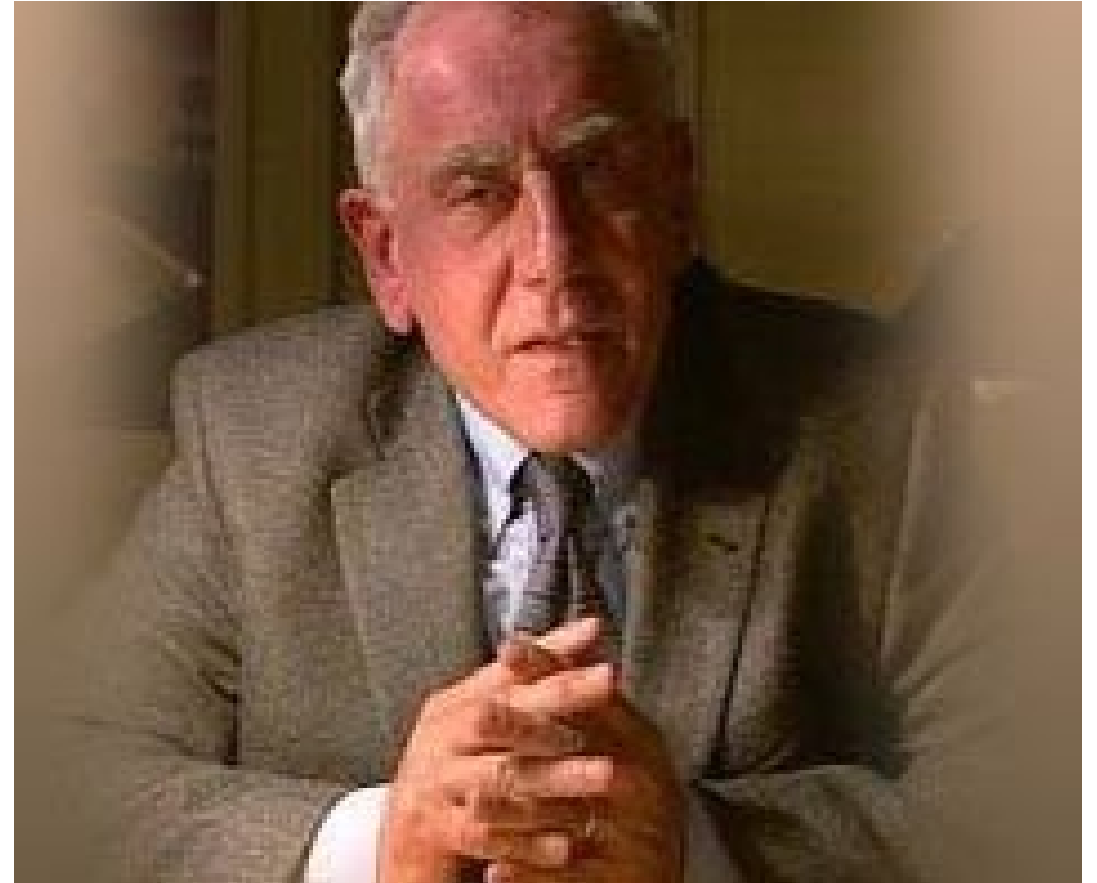- Process Users
- Error-Proofed

New View

- Insiders
  - Very Responsible
  - Very smart
  - Idea generators
- Important Informants
- Creative/Adaptive
- Problem identifiers
- Problem fixers
- Profound process owners
- Fail Often, Safe, and Fast

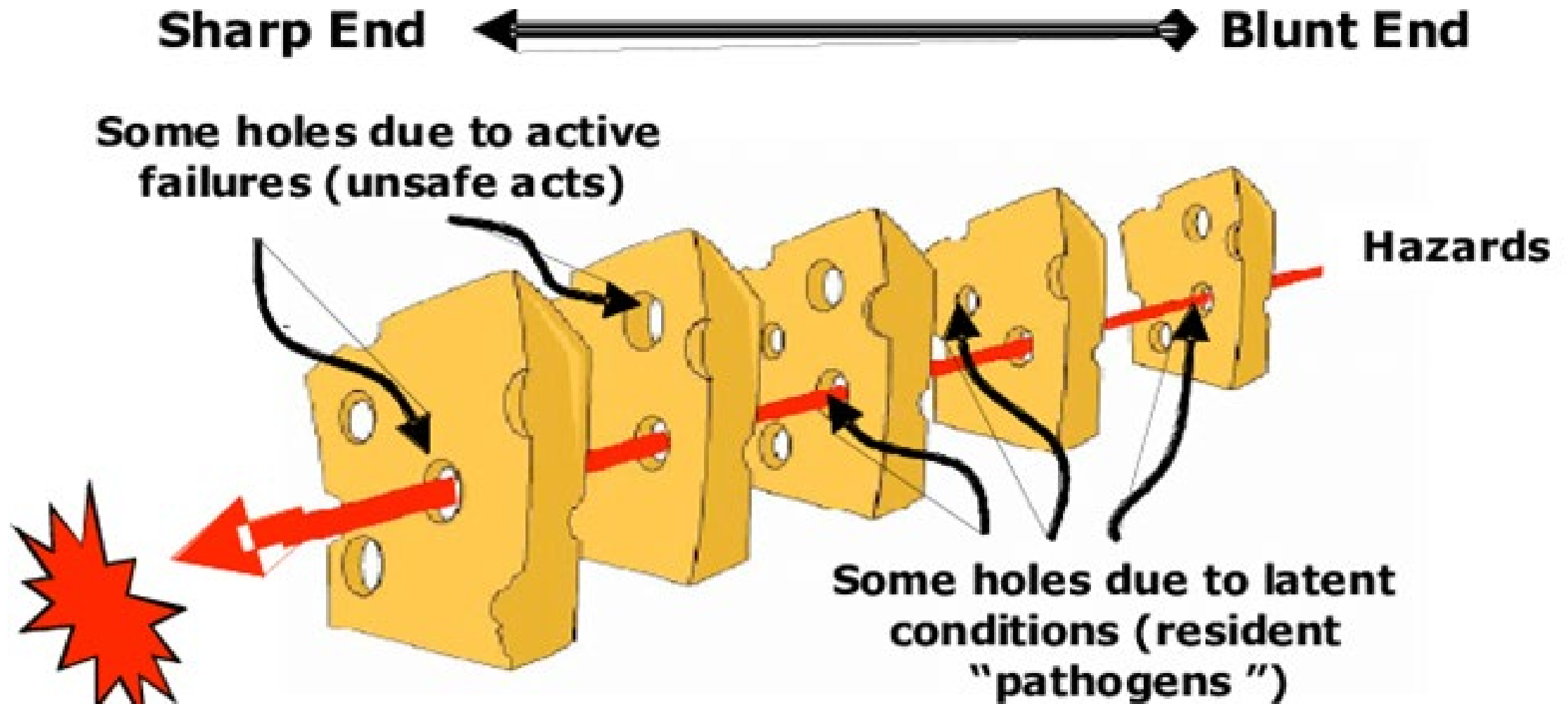Conklin, T. Pre-Accident Investigations: Better Questions

WWTCS?
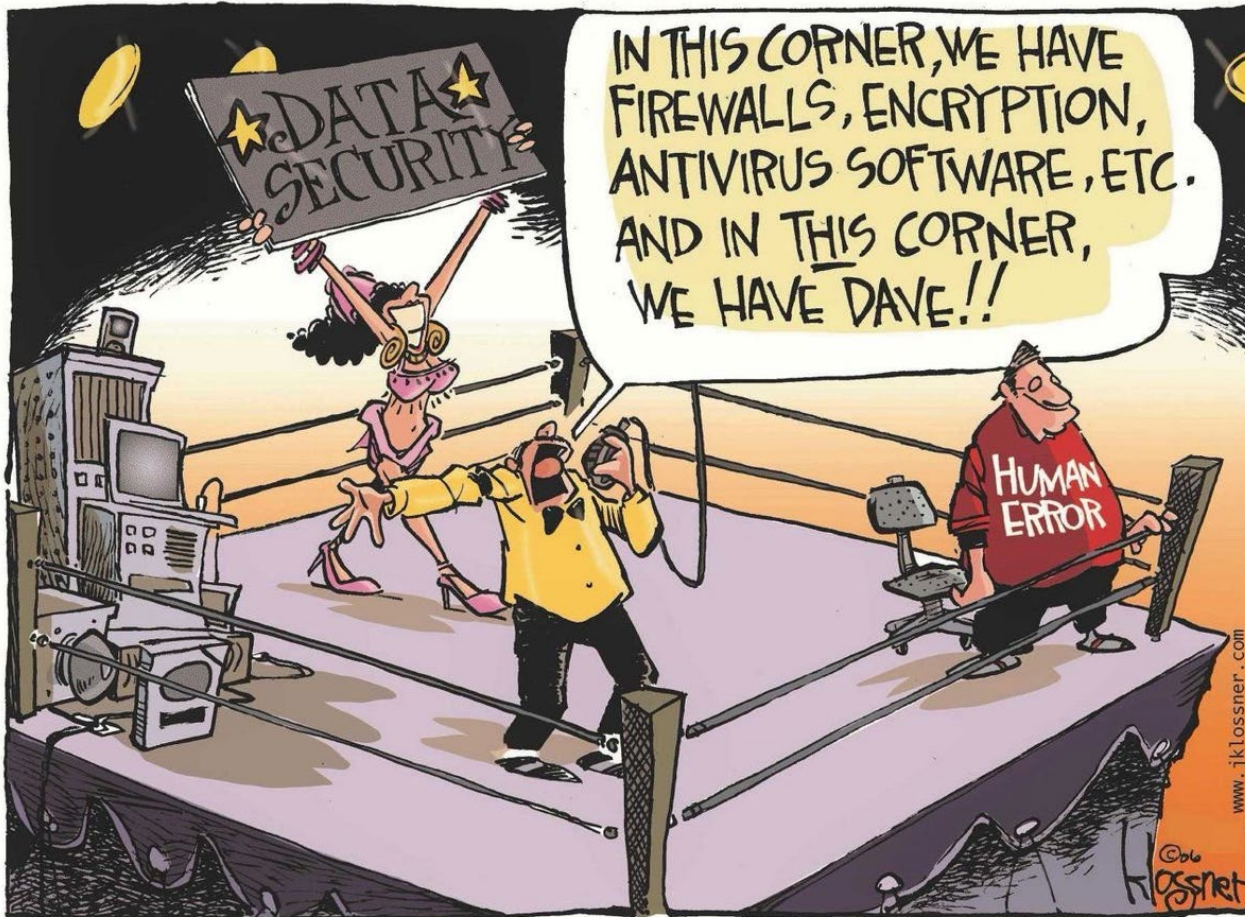
Dr. James Reason

- Professor Emeritus of Psychology, University of Manchester

- PhD in Psychology, University of Leicester

- If you read one thing: *Managing the Risk of Organizational Accidents* (1997)

Accident Causality

Sharp End ⟵————————⟶ Blunt End

Some holes due to active failures (unsafe acts)

Hazards

Some holes due to latent conditions (resident "pathogens")

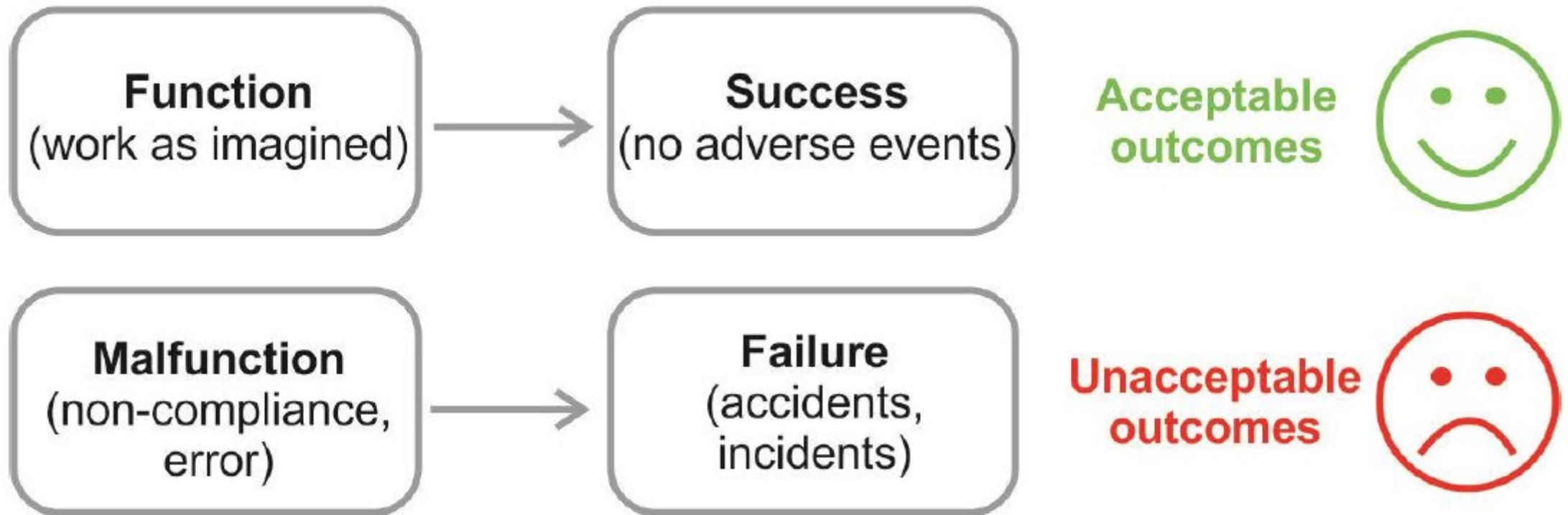Reason, J. Managing the Risks of Organizational Accidents

Dr. Erik Hollnagel

- CEO, Institute of Resilient Systems+

- PhD in Psychology, University of Aarhus

- If you read one thing: *Safety-I and Safety-II: The Past and Future of Safety Management* (2014)
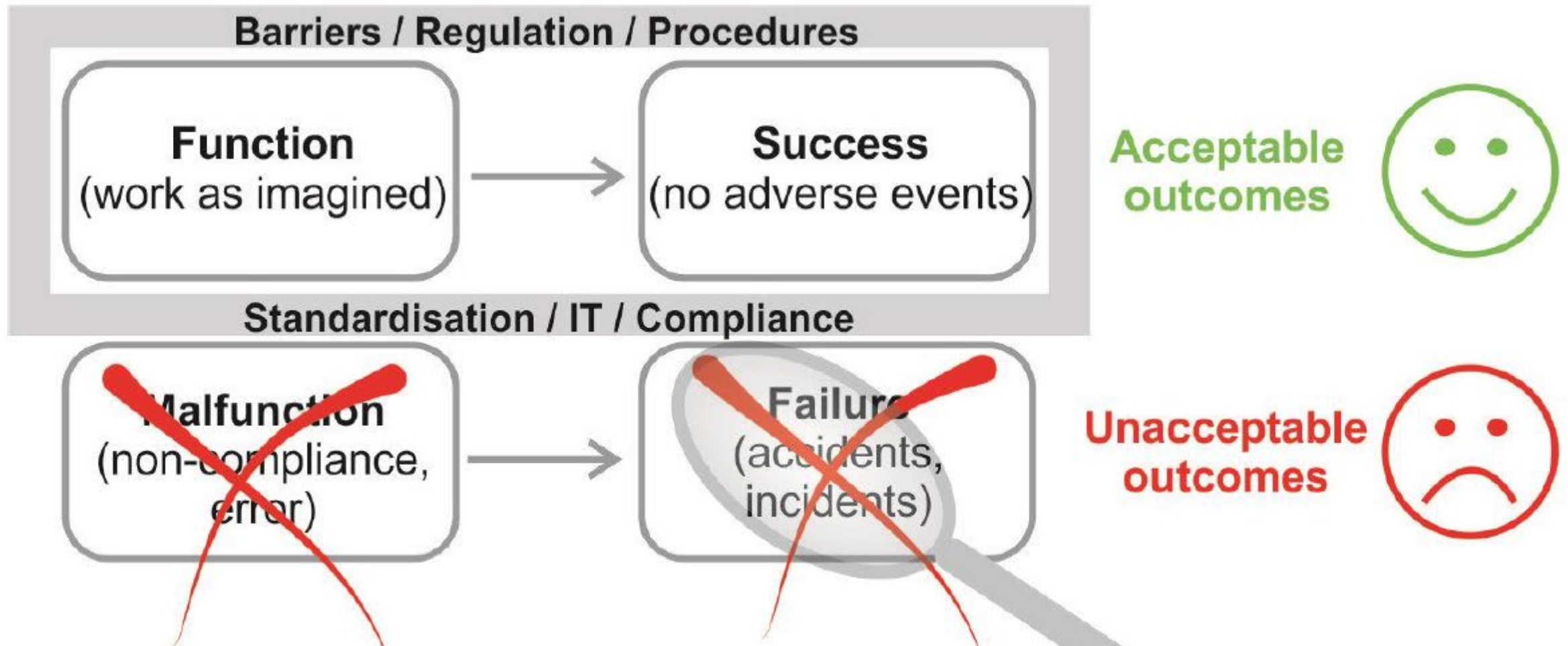
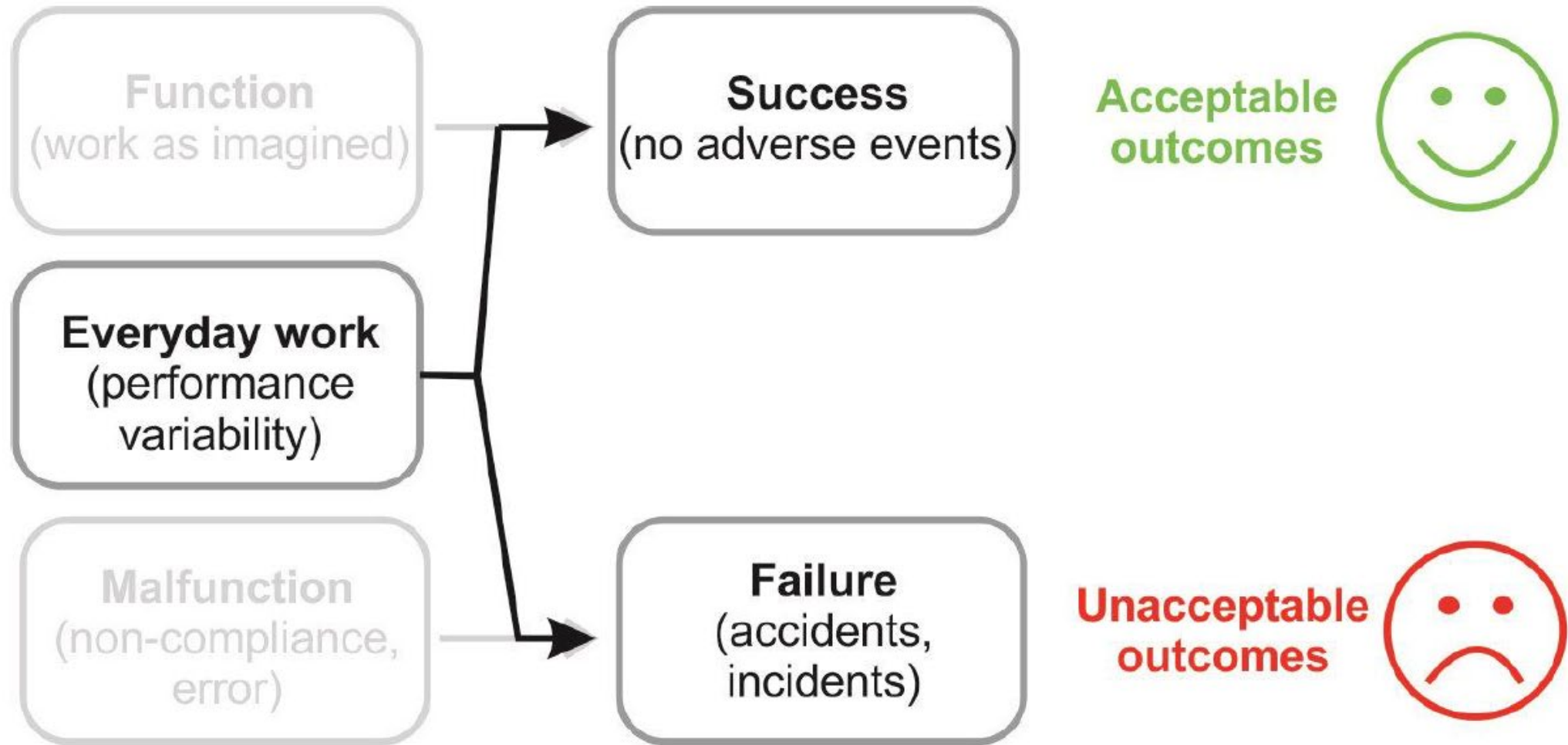# Safety-I, "How We've Always Done it"

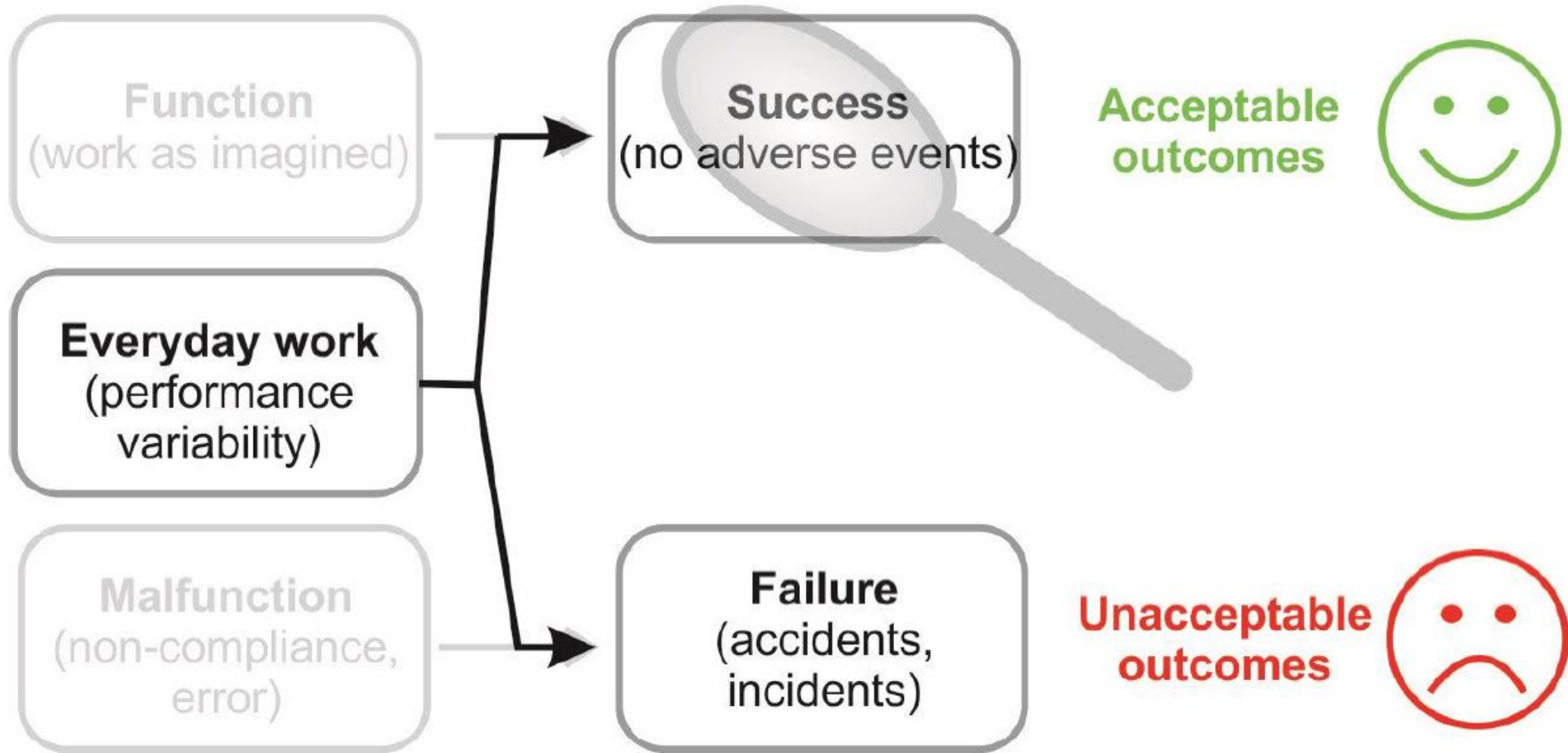Hollnagel E., Wears R.L. and Braithwaite J. From Safety I to Safety II: A White Paper

Safety-I, "How We've Always Done it"

Hollnagel E., Wears R.L. and Braithwaite J. From Safety I to Safety II: A White Paper

IDAHO NATIONAL LABORATORY

Safety-II, How It Really Happens

Function
(work as imagined)

Everyday work
(performance variability)

Malfunction
(non-compliance, error)

Success
(no adverse events)

Acceptable outcomes

Failure
(accidents, incidents)

Unacceptable outcomes

Hollnagel E., Wears R.L. and Braithwaite J. From Safety I to Safety II: A White Paper

IDAHO NATIONAL LABORATORY

Safety-I, "How We've Always Done it"

Hollnagel E., Wears R.L. and Braithwaite J. From Safety I to Safety II: A White Paper

IDAHO NATIONAL LABORATORY

The Nature of Human Error

"People" View
Accidents and incidents are caused by human error…
… and human error results from individual shortcomings (competence, attitude, motivation)…
… so we can prevent accidents and incidents by preventing human error…
… through policies, punitive discipline, training requirements controlling work

The Nature of Human Error

"People" View	"System" View
Accidents and incidents are caused by human error…	Human error is a symptom of pre-existing organizational shortcomings…
… and human error results from individual shortcomings (competence, attitude, motivation)…	… and these latent organizational weaknesses cause accidents and incidents (coincidentally exposing human error)…
… so we can prevent accidents and incidents by preventing human error…	… so we can reduce the consequences of accidents and incidents by remediating latent organizational weaknesses…
… through policies, punitive discipline, training requirements controlling work	… through improving the conditions and ecosystem surrounding work

Practical application: KnowledgeVine's approach

REMEDY™ Matrix

RE Reduce Errors + **M** Manage Change + **ED** Error Defenses = **Y** Yield

Set Expectations	Inspect What You Expect	Be a Learning Organization	**Informed Executives** Executives encourage a culture of trust which allows information to flow between all levels.
Lead by Example	Provide Coaching	Identify and correct LOWs	Empowered Leaders Leaders strengthen relationships to encourage worker feedback and are entrusted with the authority to act upon it.
Follow Expectations	Support Change	Communicate Concerns	**Engaged Employees** Employees contribute their experiences, skills, and abilities to help the organization succeed.

ABORATORY

Now, Let's Talk Security

What can we leverage from hard-earned improvements in safety, to improve cybersecurity?

But Isn't Cyber Different?

But Isn't Cyber Different?

- **V**isibility – the source of the harm is trying to remain undetected

But Isn't Cyber Different?

- **V**isibility – the source of the harm is trying to remain undetected

- **I**nitiation – some active failures are outside the influence of the target organization

But Isn't Cyber Different?

- **V**isibility – the source of the harm is trying to remain undetected

- **I**nitiation – some active failures are outside the influence of the target organization

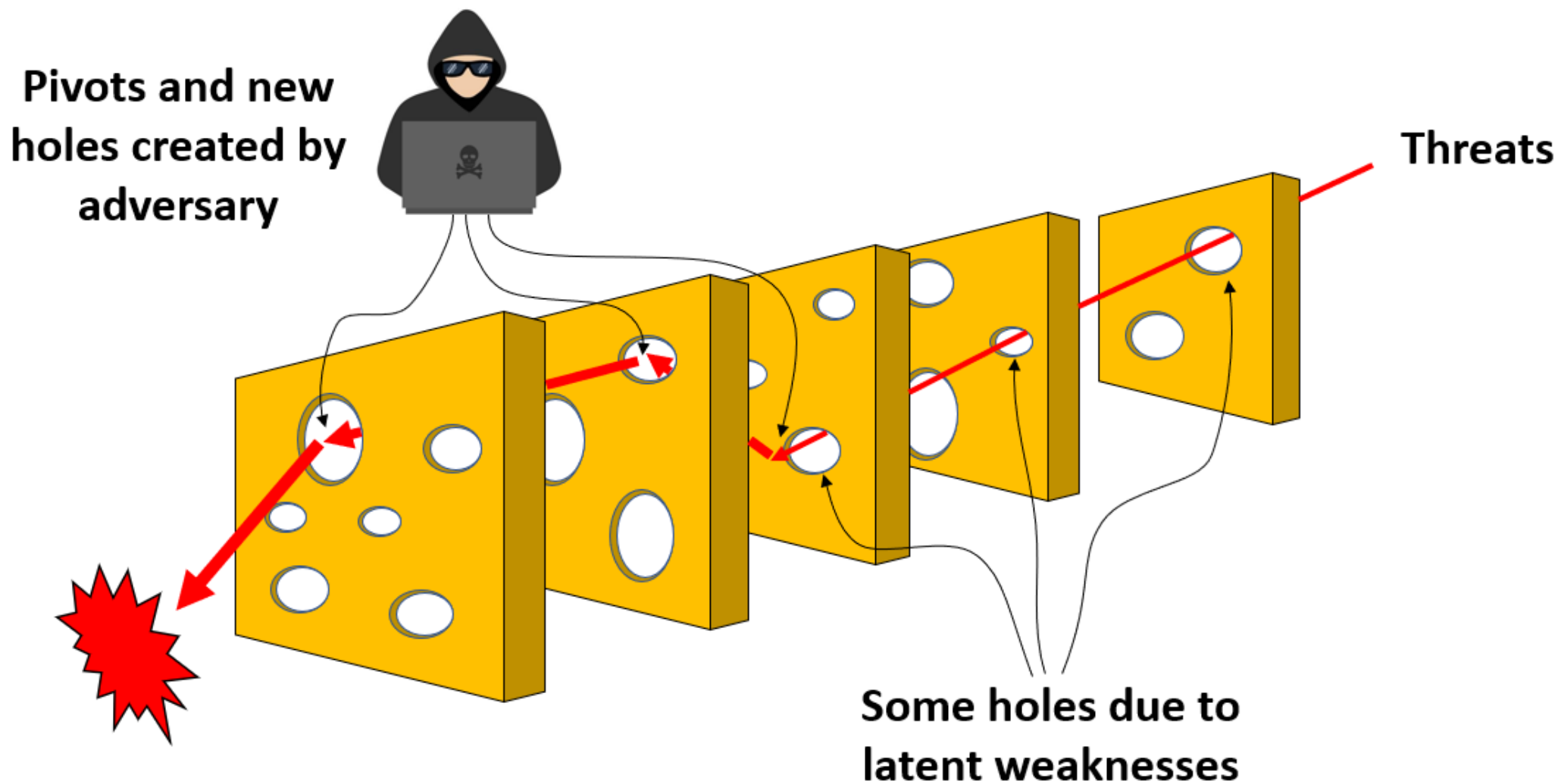- **S**entience – the source of the harm is human and deliberate

But Isn't Cyber Different?

- **V**isibility – the source of the harm is trying to remain undetected

- **I**nitiation – some active failures are outside the influence of the target organization

- **S**entience – the source of the harm is human and deliberate

- **T**ime – cybersecurity outcomes are far less dependent on real-time performance

But Isn't Cyber Different?

- **V**isibility – the source of the harm is trying to remain undetected

- **I**nitiation – some active failures are outside the influence of the target organization

- **S**entience – the source of the harm is human and deliberate

- **T**ime – cybersecurity outcomes are far less dependent on real-time performance

- **A**symmetry – small errors can lead to outsized consequences

Incident Causality

Pivots and new holes created by adversary

Threats

Some holes due to latent weaknesses
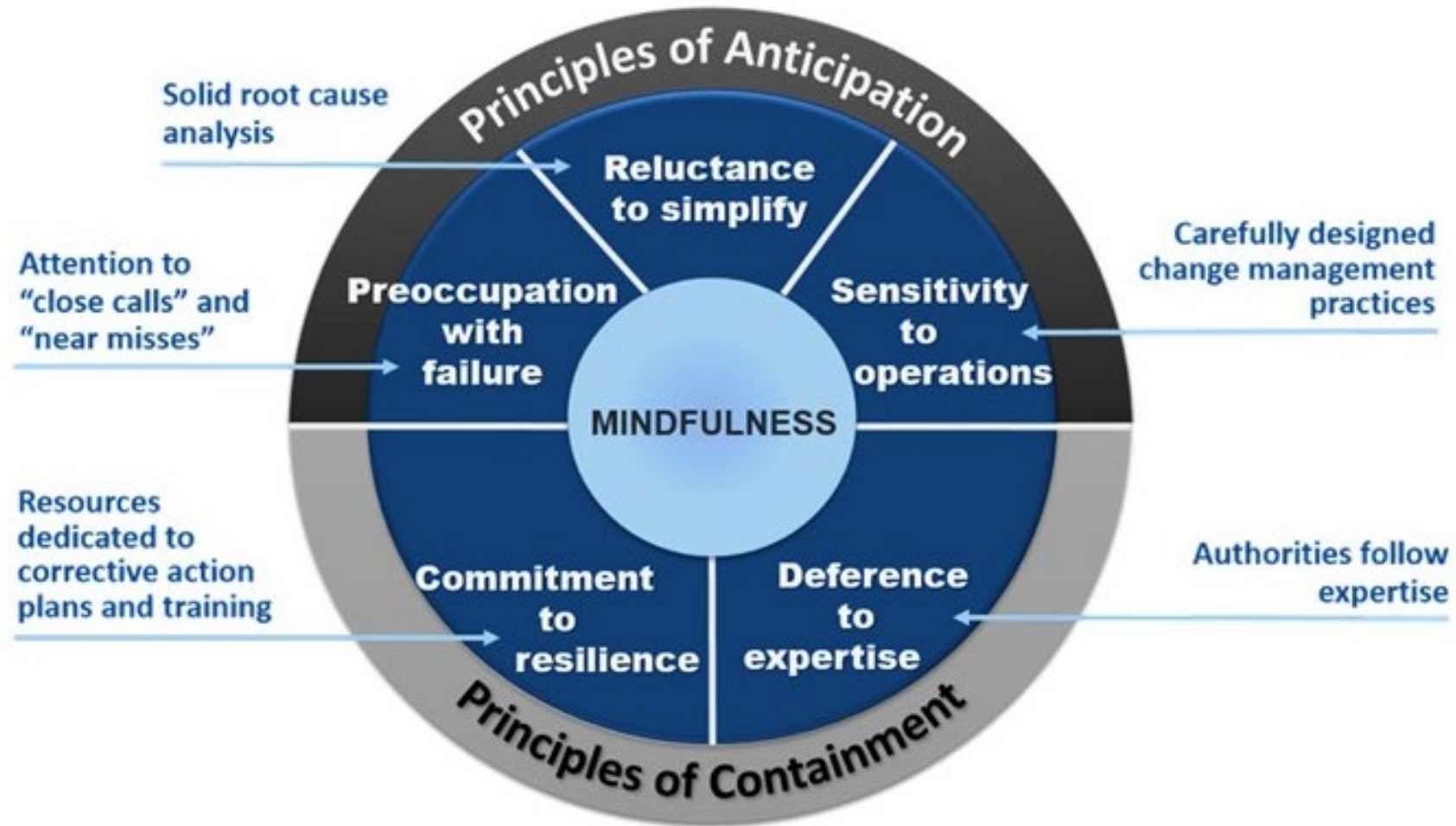
"Security is not the absence of incidents."

So what about that 'look at the bright side' part?

"Security is not the absence of incidents."

"Security is the presence of defenses."

I need a HERO!

Midwest Reliability Organization, 2022

IDAHO NATIONAL LABORATORY

Monday morning quarterbacking your heroes

Behavior	When you succeed	When you fail
Sees what isn't working and adjusts	"great adaptability"	"used unproven methods"
Adapts to unfamiliar situations	"making it work"	"making stuff up"
Figures out ways to be more efficient	"highly productive"	"took shortcuts"
Uses experience to overcome insufficient resources	"resourceful"	"circumvented"
Uses knowledge to make sense of confusing situations	"experience is evident"	"making assumptions"

"Make G.O.A.T.s, not scapegoats!"

IDAHO NATIONAL LABORATORY

Can we assess this?

- Yes, by *validated* presence of
  - foundational technical controls
  - viable processes
  - curious individuals and a just culture
- KPI targets expressed as success instead of failure
  - mathematically equivalent
  - psychologically different
- DoD Cybersecurity Scorecard example
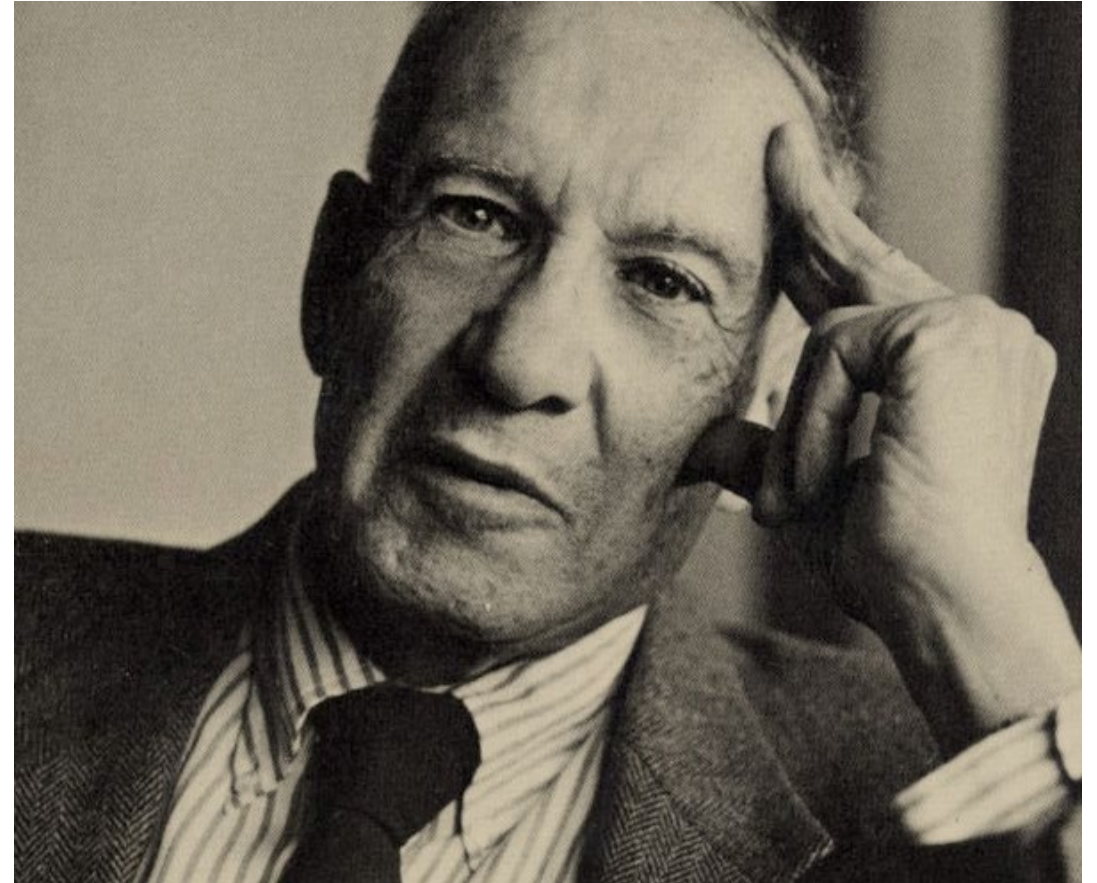
"What you call the disease?
I call it the remedy
And what you're callin' the cause,
I call the cure."

-David "Dicky" Barrett and Joseph Gittleman

Questions, Comments, Thoughts?!

Sam Chanoski
Technical Relationship Manager | Cybercore Integration Center
samuel.chanoski@inl.gov | 404-904-2480
Idaho National Laboratory | Atlanta, GA

IDAHO NATIONAL LABORATORY

Battelle Energy Alliance manages INL for the U.S. Department of Energy's Office of Nuclear Energy.
INL is the nation's center for nuclear energy research and development, and also performs research
in each of DOE's strategic goal areas: energy, national security, science and the environment.