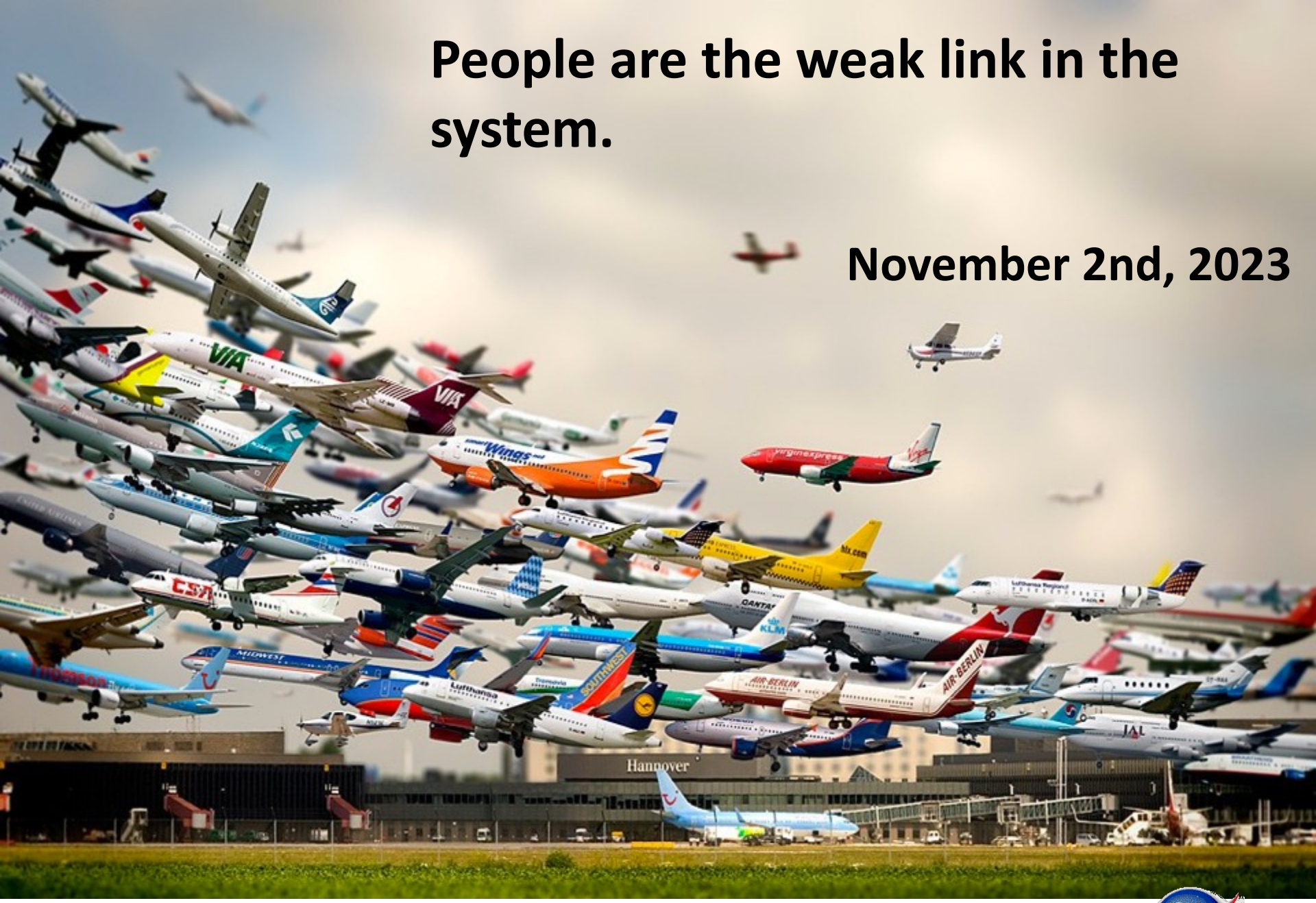


Human Systems integration division

Immanuel Barshi, NASA Ames Research Center

NASA

All technical systems fail

- Much of the cost of building and running technical systems goes into figuring out how things can fail, building in defenses, fail-safes, and redundancies.
- Safe organizations invest in failure
  - Procedures and backup plans
  - Practice, simulation, and training
  - Hard work, fortitude, and culture

Failure investment ≠ Failure proof

- All of this investment does not make systems failure proof!
- The goal of this investment should not just be to prevent failures from happening, or problems from occurring.
- The goal should also include preparing for, responding to, and recovering from failures (which will happen).

How do we think about the Operation?

Traditional Thinking ("Safety-I")	
Focused on ensuring that "as few things as possible go wrong"	
Humans are a source of errors and hazards: Control and correct	
Variability is a threat—minimize it	
Focus on incident rates	
Focus on what we don't want: injuries and incidents	
Procedures are complete and correct	
Systems are well designed, work as designed, and are well maintained	

** See Hollnagel, Wears, & Braithwaite (2015)*

How do we think about the Operation?

Traditional Thinking ("Safety-I")	"Safety-II" Thinking*
Focused on ensuring that "as few things as possible go wrong"	Focused on ensuring that "as many things as possible go right"
Humans are a source of errors and hazards: Control and correct	Humans are a source of flexibility and resilience: Learn and adapt
Variability is a threat—minimize it	Variability is normal—manage it
Focus on incident rates	Focus on learning
Focus on what we don't want: injuries and incidents	Focus on what we do want: how safety is created; how problems are solved
Procedures are complete and correct	Procedures are under-specified and must be interpreted and adapted
Systems are well designed, work as designed, and are well maintained	Systems are complex and will degrade; there will always be flaws and glitches

** See Hollnagel, Wears, & Braithwaite (2015)*

Responding to Mishap Findings

Finding from Mishap Analysis	Traditional Risk Mgmt. Response (Safety-I)	RE/HRO/Safety-II Response
• People had concerns but did not speak up.	• Encourage workers to speak up (e.g., "if you see something, say something").	• Change meeting format: ask open-ended questions, leader speaks last. • Encourage cross-checks and promote cross-role understanding.
• No one noticed the emerging problem.	• Attribute to complacency or loss of situation awareness. • Encourage workers to be careful and pay attention.	• Look for evidence of dismissing problems, prioritizing authority over expertise, simplified root-cause analyses. • Implement structured pre-mission briefs focused on reinforcing awareness of risks and contingencies.
• There was a failure in responding to the unexpected.	• Create rules that specify what the correct response should be.	• Build tangible experience with uncertain and unpredicted events. • Develop drills and simulations to practice noticing subtle cues and responding to surprise.
• Mishap was a recurring anomaly.	• Create more documentation of incidents and lessons learned. • Require workers to review and study them.	• Expand analysis methods and breadth of learning opportunities. • Identify similar events in which things went well, and ask, “what can we learn from our success?”

Impacts of systematically limiting data (by thinking only in terms of "safety I")

- Human performance includes both desired and undesired actions – actions that promote safety, as well as actions that can reduce safety.

- When our safety thinking systematically restricts the data we collect and analyze, it
  - Restricts our opportunities to learn, and it
  - Affects our policies and decision making.

How do we think about the Operation?

Traditional Thinking ("Safety-I")	"Safety-II" Thinking*
Focused on ensuring that "as few things as possible go wrong"	Focused on ensuring that "as many things as possible go right"
Humans are a source of errors and hazards: Control and correct	Humans are a source of flexibility and resilience: Learn and adapt
Variability is a threat—minimize it	Variability is normal—manage it
Focus on incident rates	Focus on learning
Focus on what we don't want: injuries and incidents	Focus on what we do want: how safety is created; how problems are solved
Procedures are complete and correct	Procedures are under-specified and must be interpreted and adapted
Systems are well designed, work as designed, and are well maintained	Systems are complex and will degrade; there will always be flaws and glitches

** See Hollnagel, Wears, & Braithwaite (2015)*

A thought experiment

- Human error has been implicated in 70% to 80% of accidents in civil and military aviation (Weigmann & Shappell, 2003).

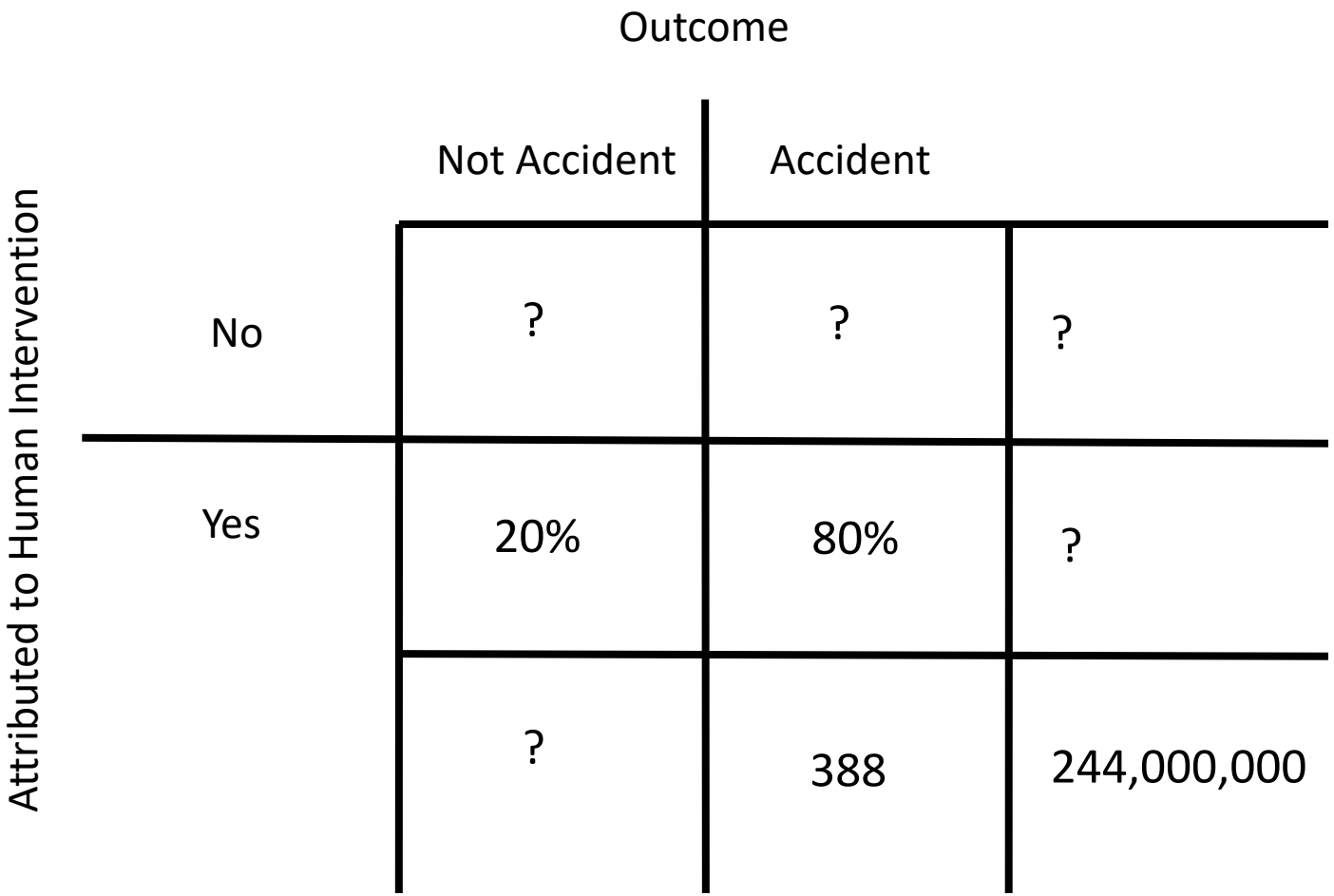
Holbrook, J. (2018, April). *Human performance contributions to safety in commercial aviation* [PowerPoint presentation]. NASA Ames Research Center, Moffett Field, CA.

A thought experiment

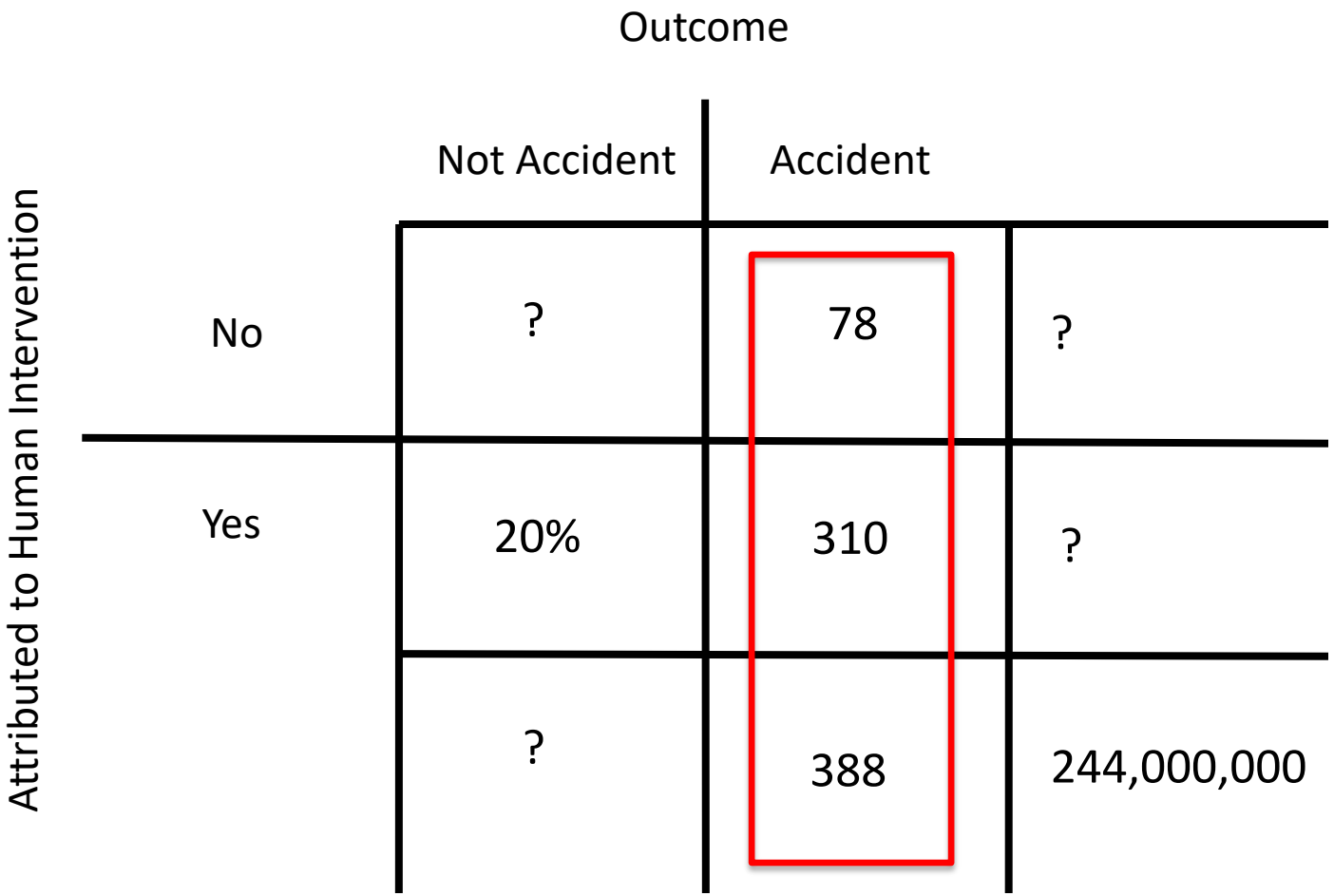
- Human error has been implicated in 70% to 80% of accidents in civil and military aviation (Weigmann & Shappell, 2003).
- Pilots intervene to manage aircraft malfunctions on 20% of normal flights (PARC/CAST, 2013).

A thought experiment

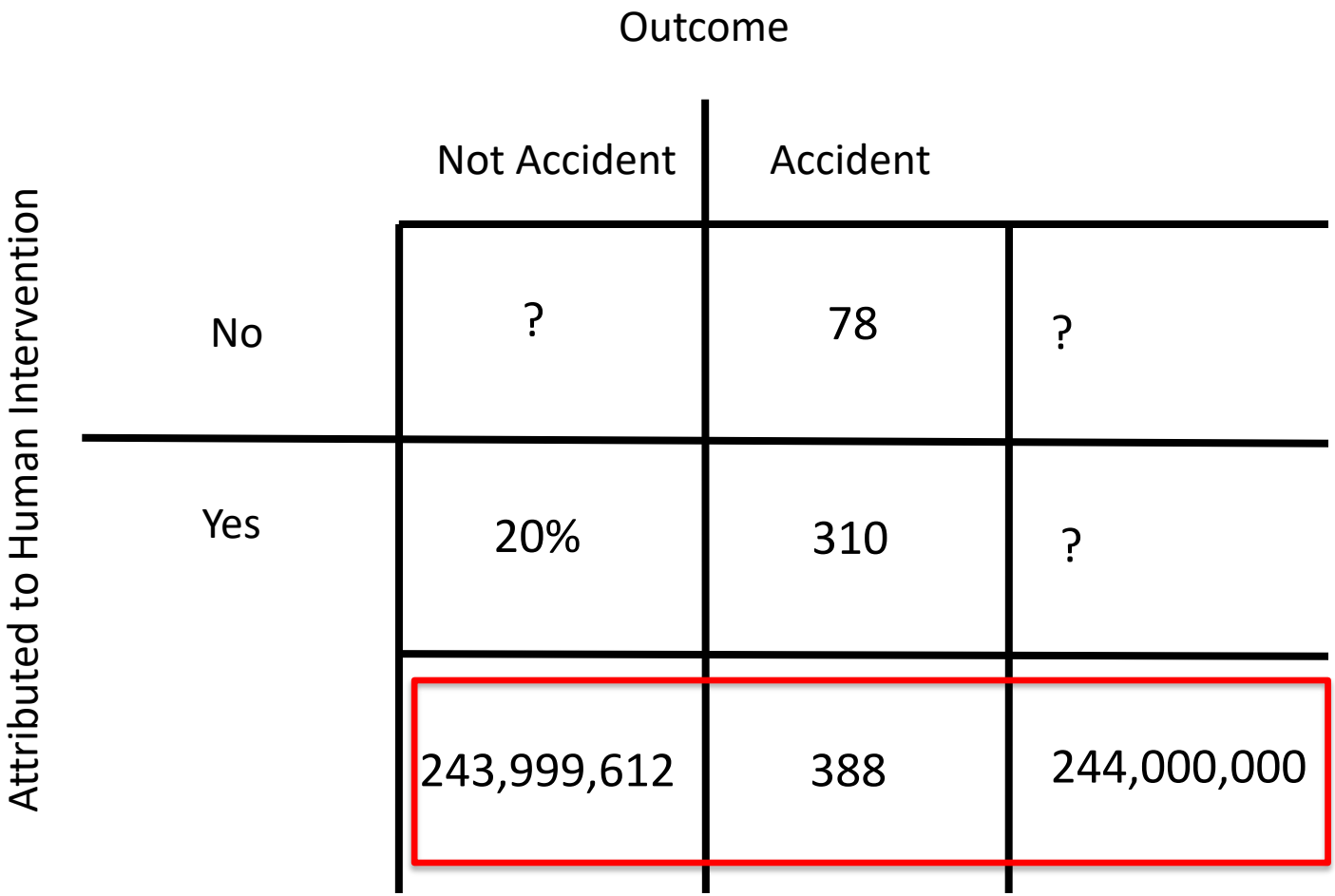
- Human error has been implicated in 70% to 80% of accidents in civil and military aviation (Weigmann & Shappell, 2003).
- Pilots intervene to manage aircraft malfunctions on 20% of normal flights (PARC/CAST, 2013).
- World-wide jet data from 2007-2016 (Boeing, 2016)
  - 244 million departures
  - 388 accidents



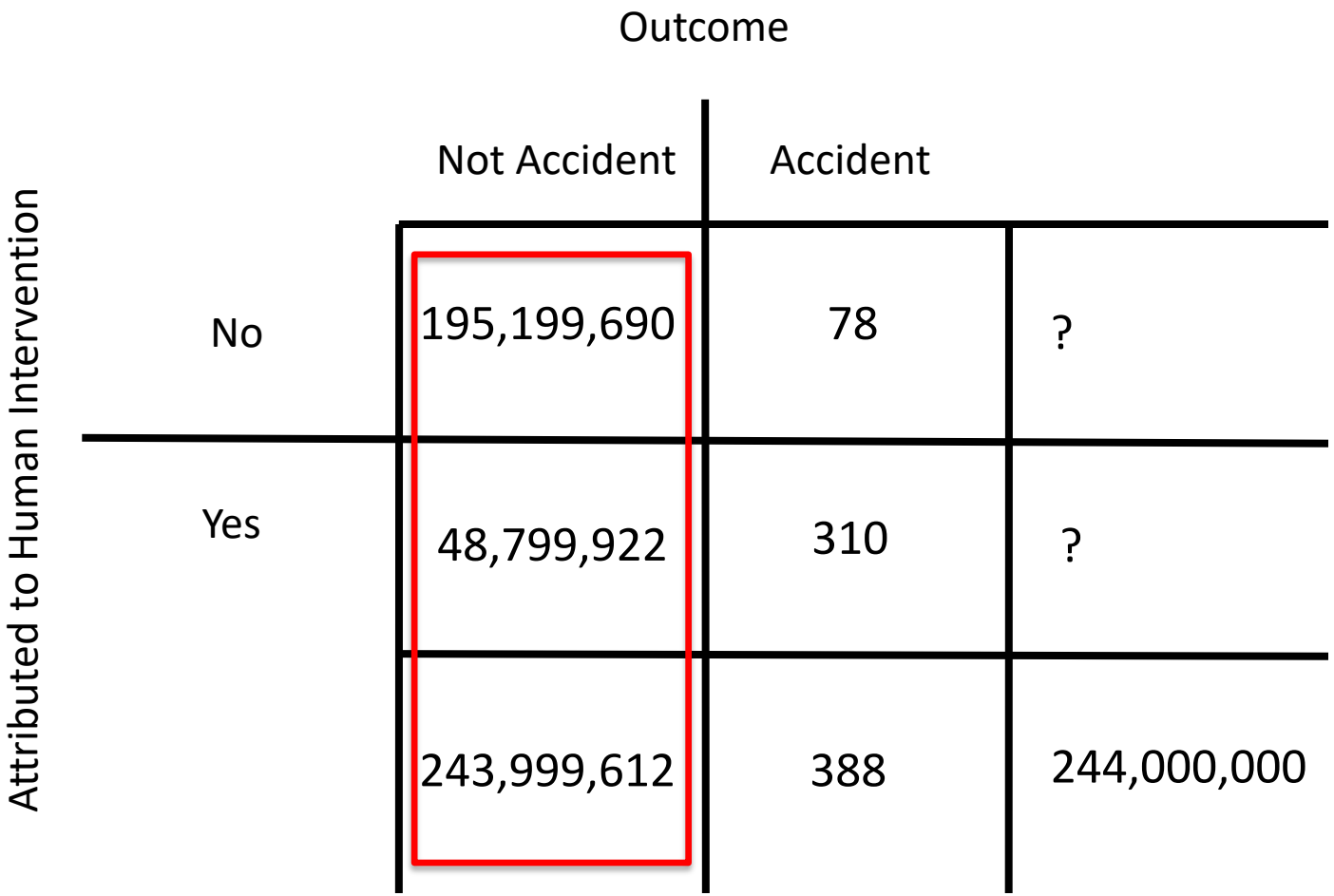
- Human error implicated in 80% of accidents.
- Pilots manage malfunctions on 20% of normal flights.
- 388 accidents over 244M departures.



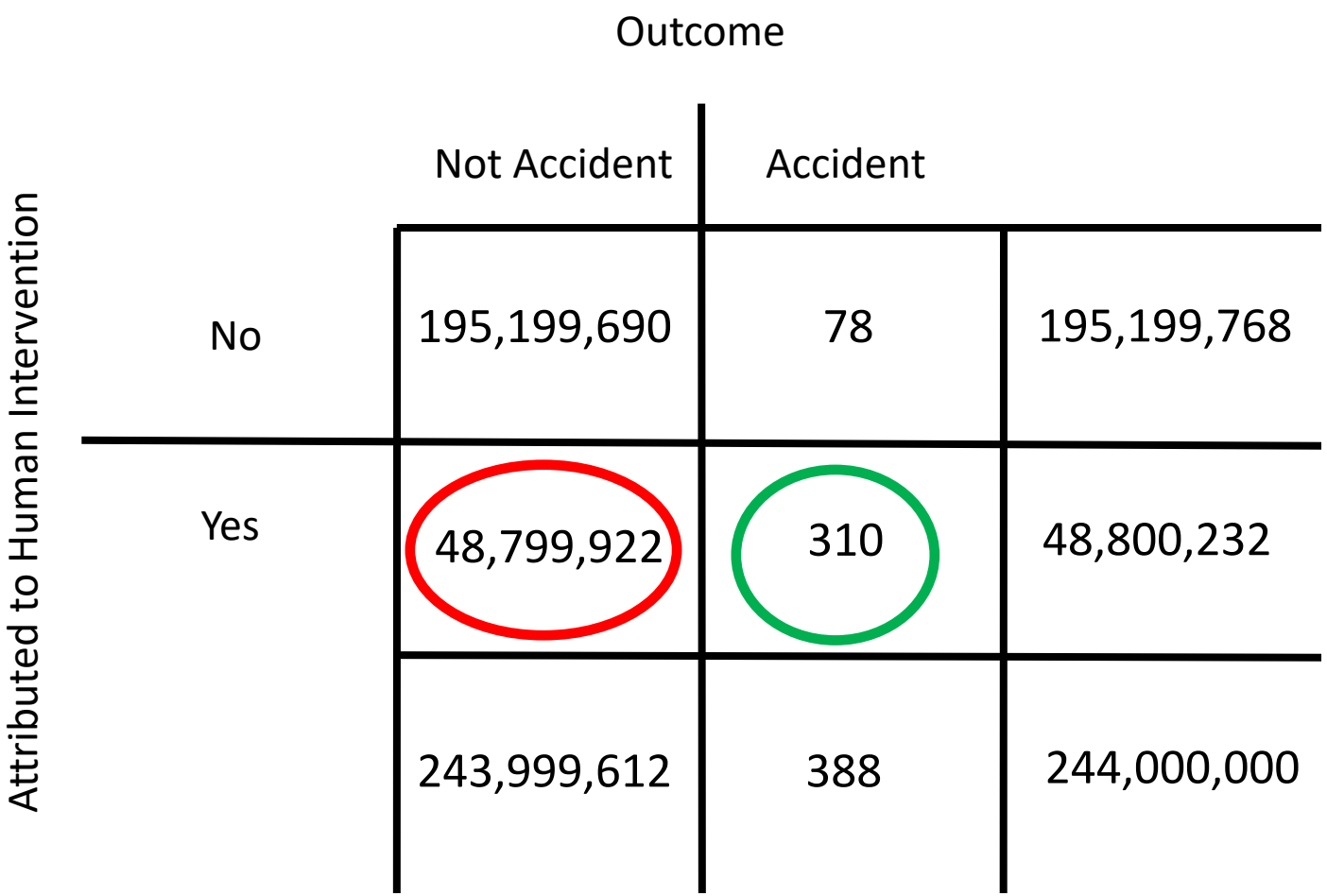
- Human error implicated in 80% of accidents.
- Pilots manage malfunctions on 20% of normal flights.
- 388 accidents over 244M departures.



- Human error implicated in 80% of accidents.
- Pilots manage malfunctions on 20% of normal flights.
- 388 accidents over 244M departures.



- Human error implicated in 80% of accidents.
- Pilots manage malfunctions on 20% of normal flights.
- 388 accidents over 244M departures.



When we characterize safety only in terms of errors and failures, we ignore the vast majority of human impacts on the system.

A Couple of Problems with our Assumptions

- Human error has been implicated in 70% to 80% of accidents in civil and military aviation (Weigmann & Shappell, 2003).

Wrong! 100% of accidents are due to human limitations!

A Couple of Problems with our Assumptions

- Human error has been implicated in 70% to 80% of accidents in civil and military aviation (Weigmann & Shappell, 2003).

Wrong! 100% of accidents are due to human limitations!

And 100% of successful operations are due to human capabilities!

A Couple of Problems with our Assumptions

- Human error has been implicated in 70% to 80% of accidents in civil and military aviation (Weigmann & Shappell, 2003).

Wrong! 100% of accidents are due to human limitations and 100% of successful operations are due to human capabilities!

- Pilots intervene to manage aircraft malfunctions on 20% of normal flights (PARC/CAST, 2013).

Pilots intervene in various ways on 100% of flights!

Our thinking affects our policies and plans

- When policy decisions are based only on failure data, they are based on a very small sample of non-representative data
  - Without understanding the mechanisms by which problems are solved, any estimate or claim about the predicted safety of autonomous machine capabilities is inherently suspect.
  - Removing the human demonstrated reliable source of safety-producing behavior without first understanding the capability being removed introduces unknown risks.

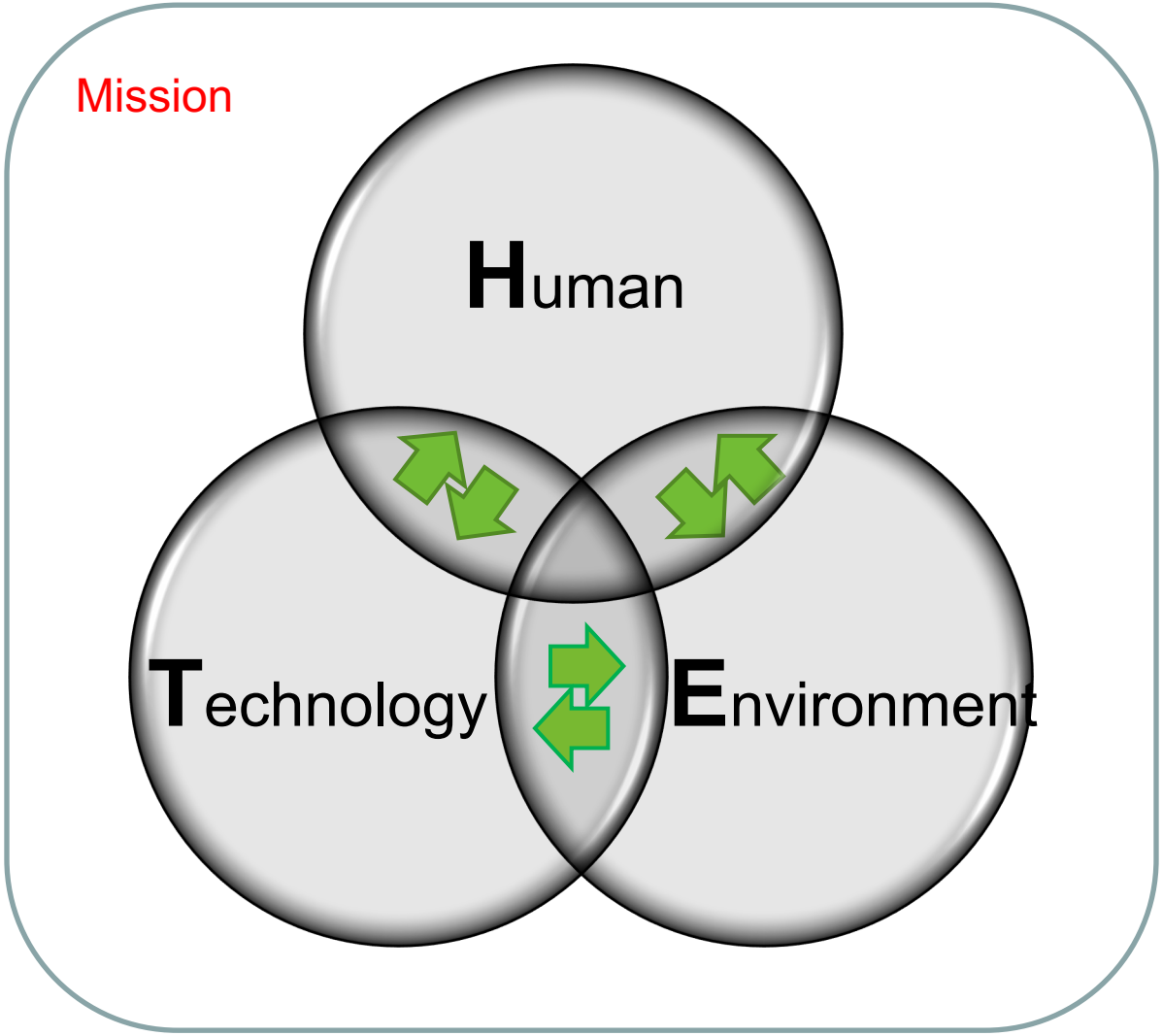
How do we think about the Operation?

Traditional Thinking ("Safety-I")	"Safety-II" Thinking*
Focused on ensuring that "as few things as possible go wrong"	Focused on ensuring that "as many things as possible go right"
Humans are a source of errors and hazards: Control and correct	Humans are a source of flexibility and resilience: Learn and adapt
Variability is a threat—minimize it	Variability is normal—manage it
Focus on incident rates	Focus on learning
Focus on what we don't want: injuries and incidents	Focus on what we do want: how safety is created; how problems are solved
Procedures are complete and correct	Procedures are under-specified and must be interpreted and adapted
Systems are well designed, work as designed, and are well maintained	Systems are complex and will degrade; there will always be flaws and glitches

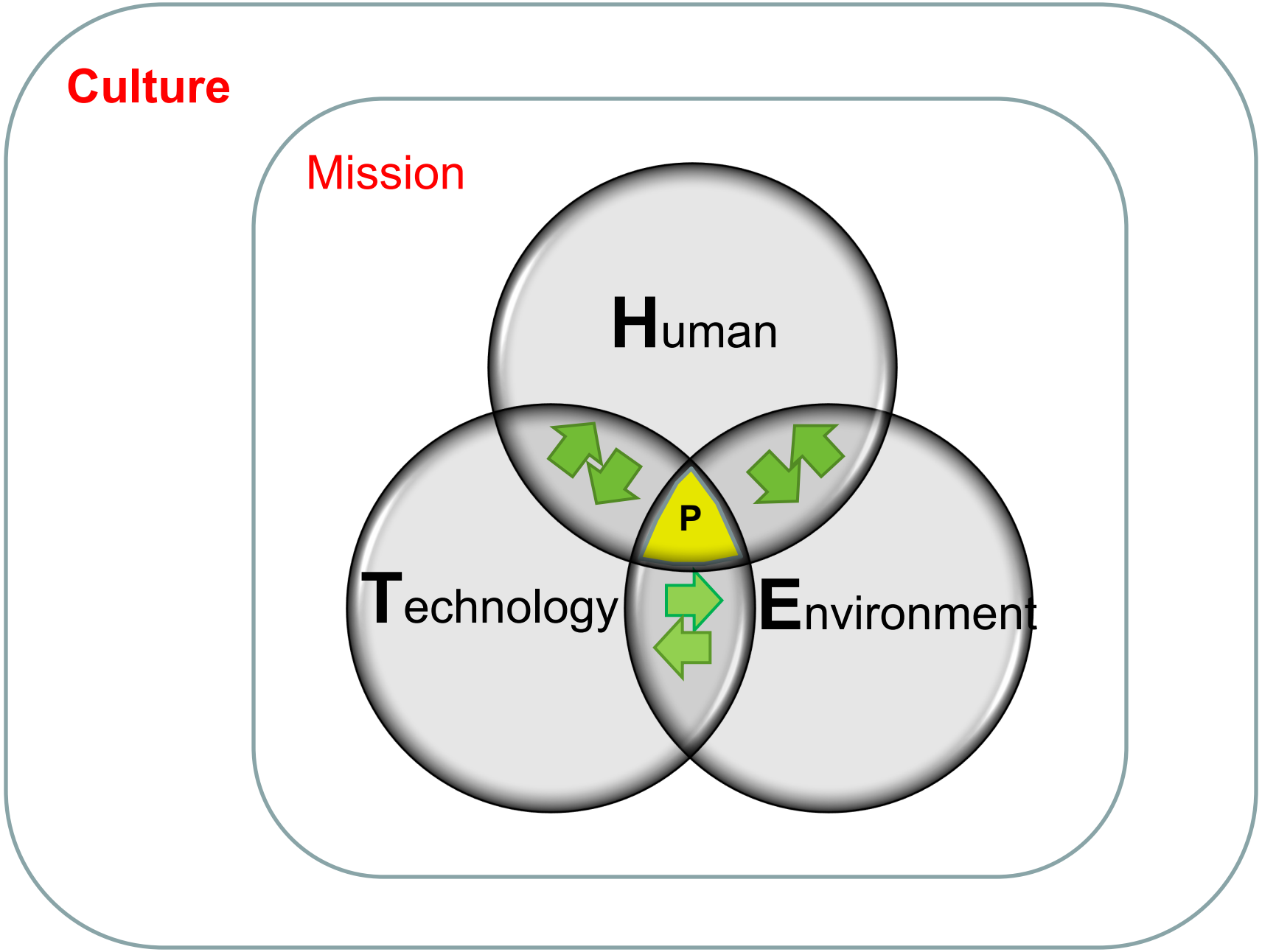
** See Hollnagel, Wears, & Braithwaite (2015)*

How to make it easy to do the right thing?

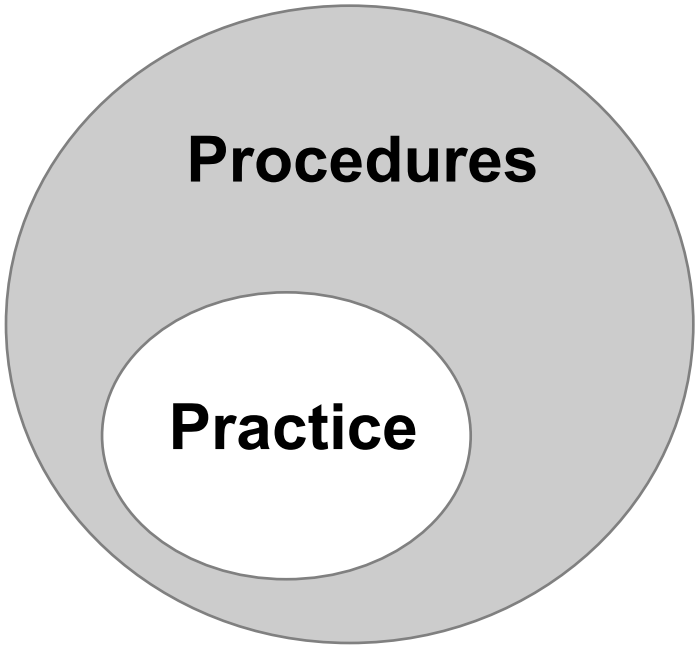
- By understanding the complexity of the operation and of the operator.
- By creating a clear, coherent, consistent, and comprehensive guidance throughout.
- The 4C's, THE Model, and the 4P's.

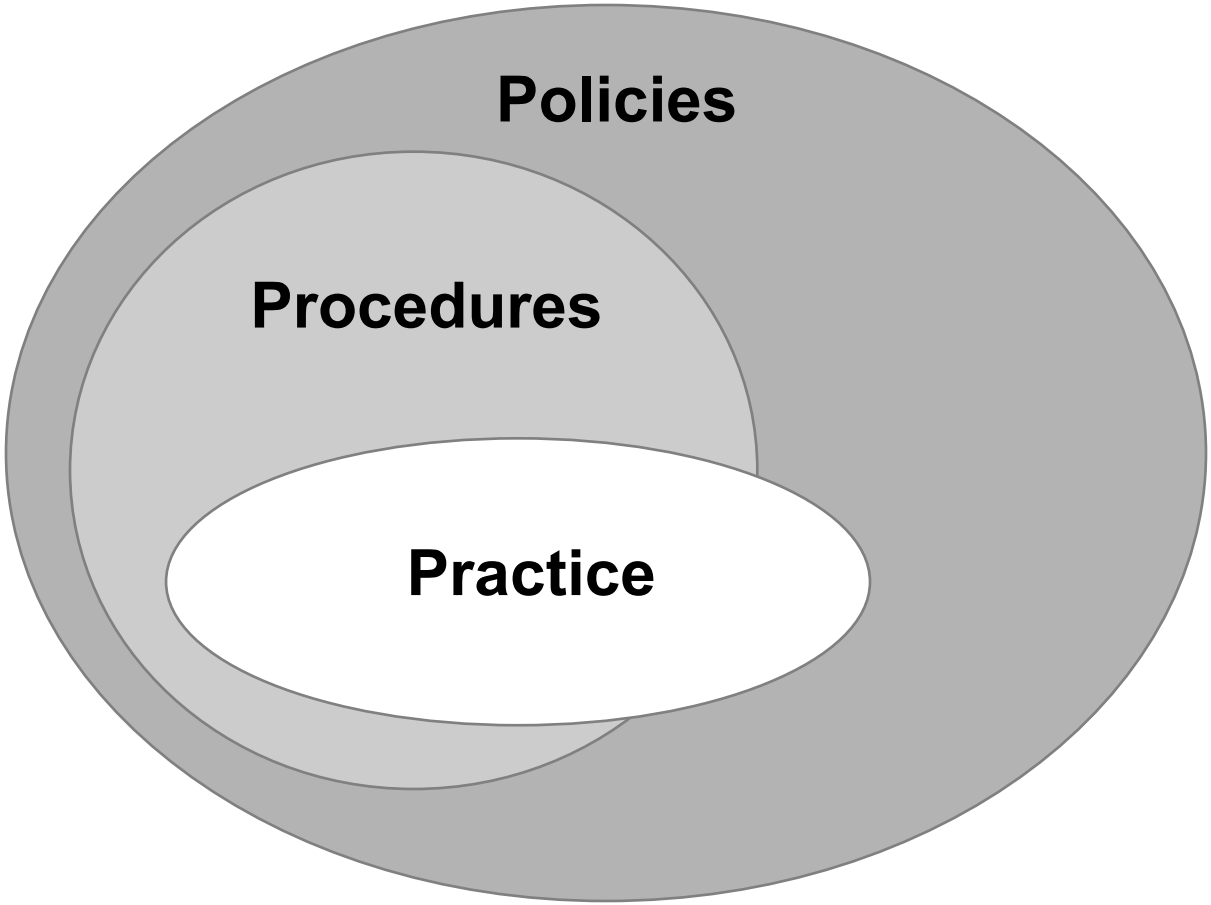


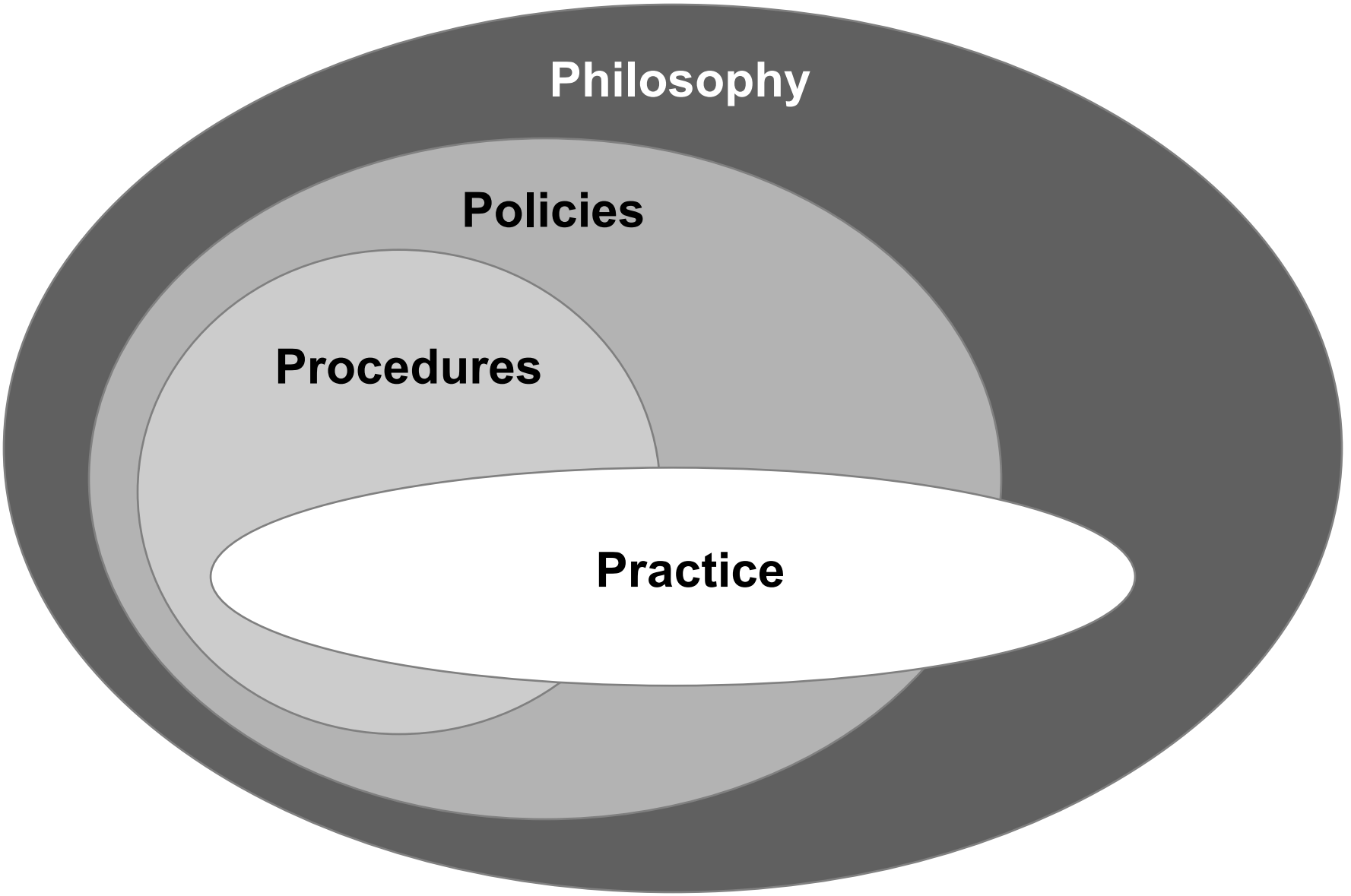
THE Model



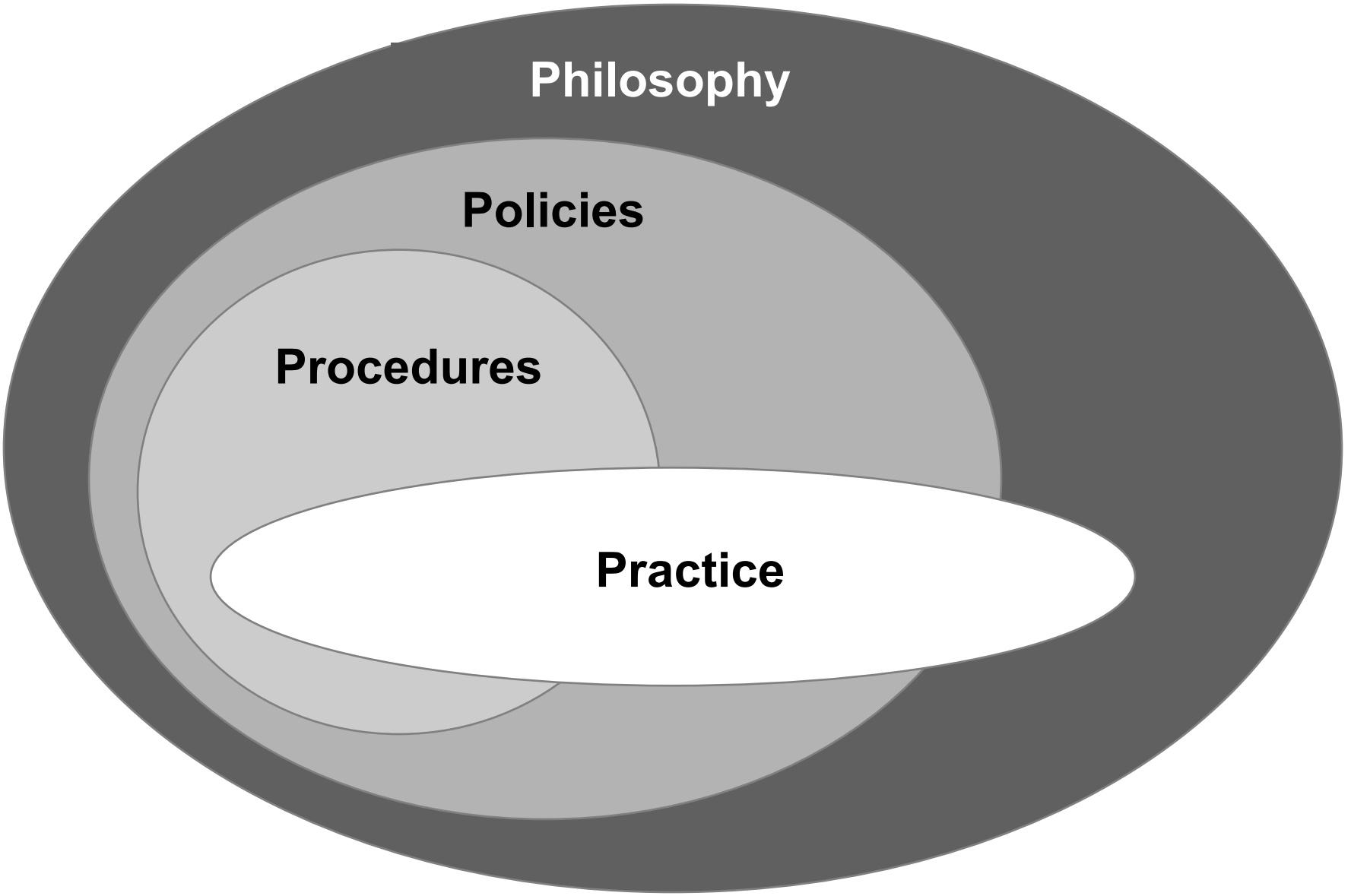
THE Model


Procedures
Practice

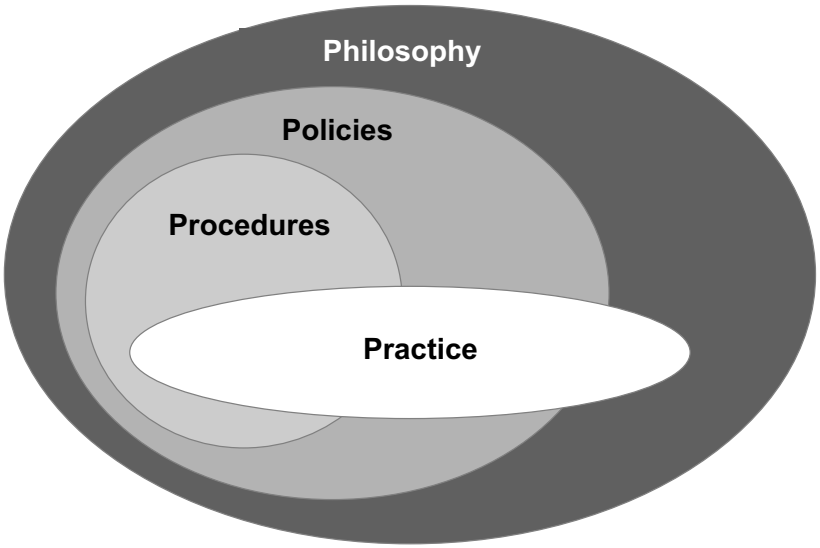

Policies
Procedures
Practice


Philosophy
Policies
Procedures
Practice

The 4P's



The 4P's



- Not a theoretical model.
- The result of observations.
- That's the way it's out there right now.
- The question is whether you want to make it explicit or not.

Figure 1. Mean Number of Problems on Target Items per Flight

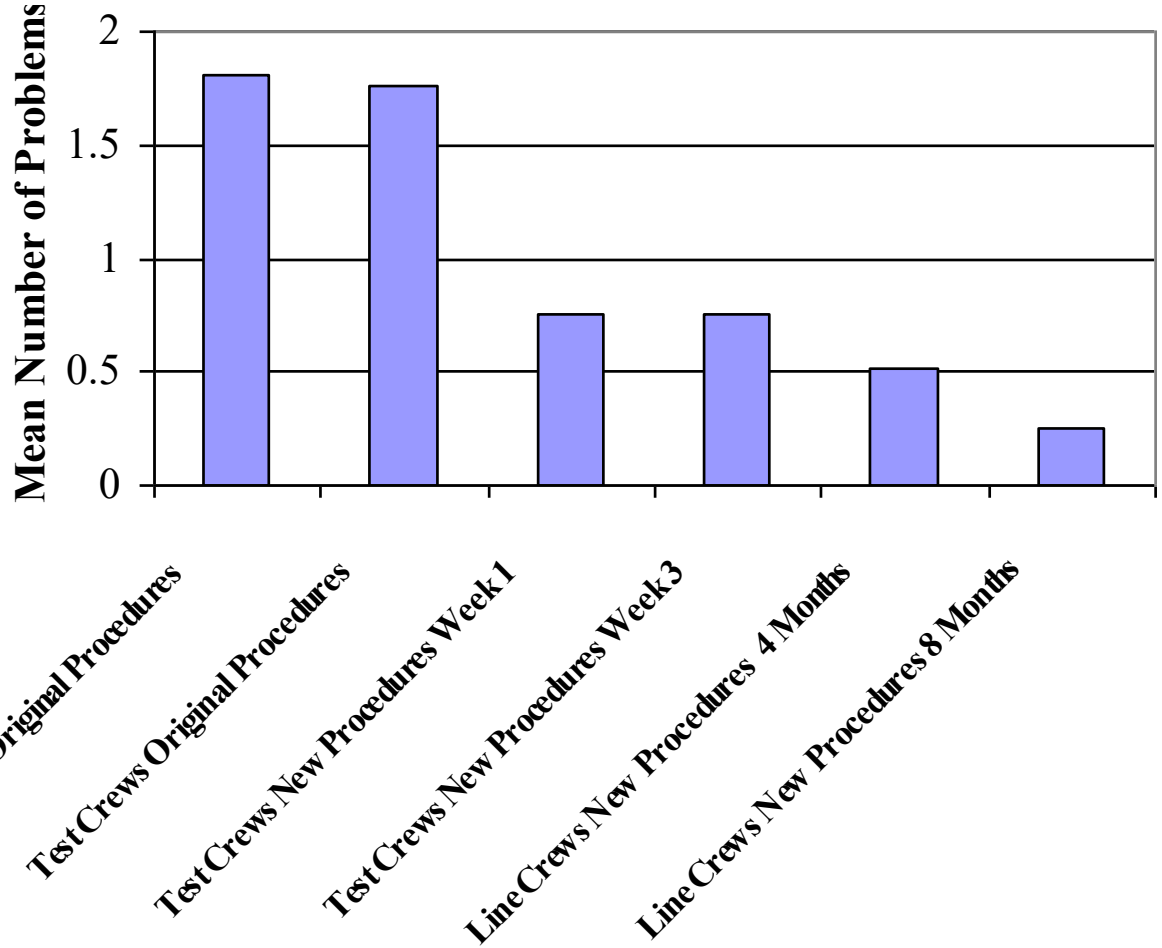


Figure 2. Average standard deviation in proportion of problems

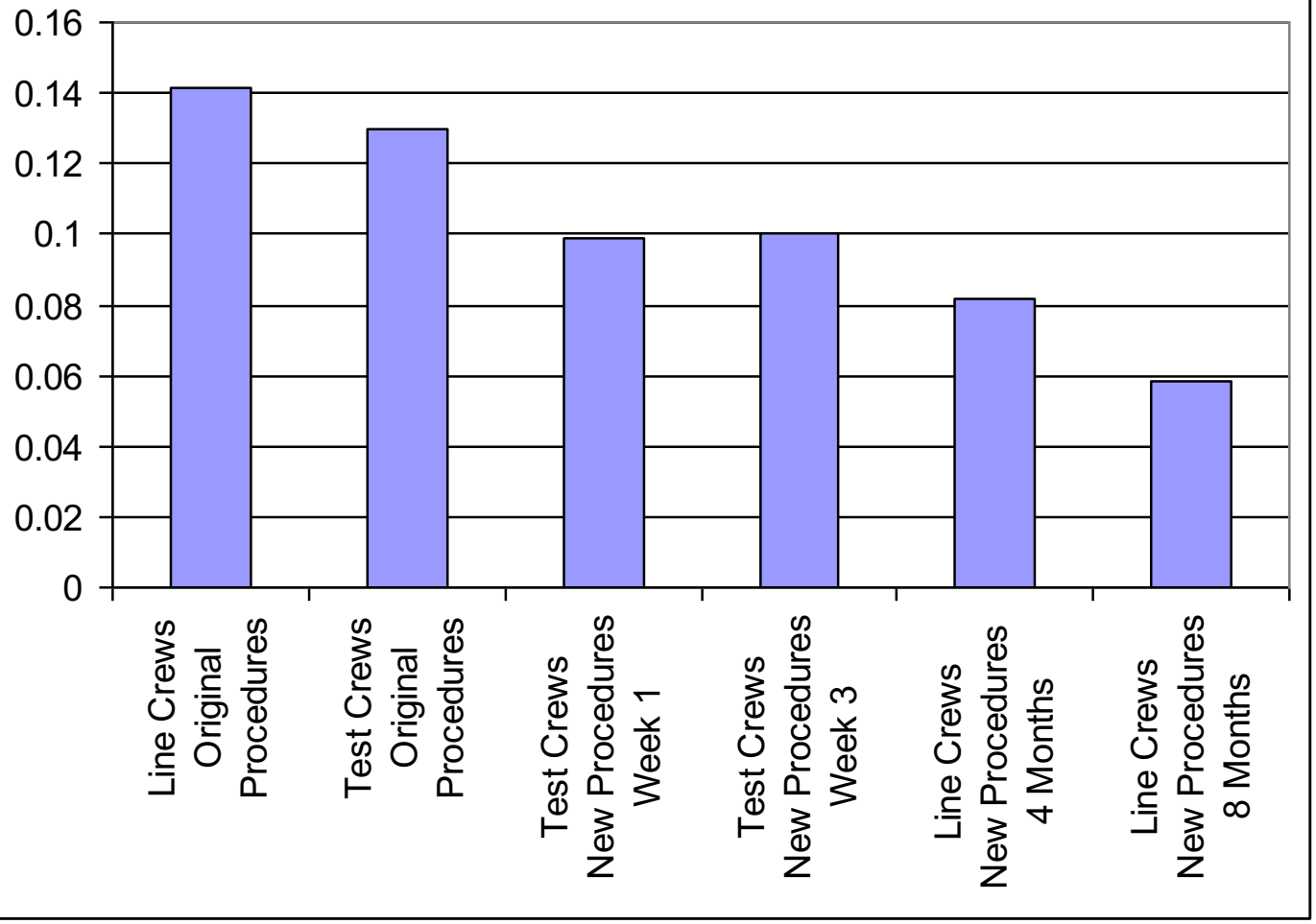
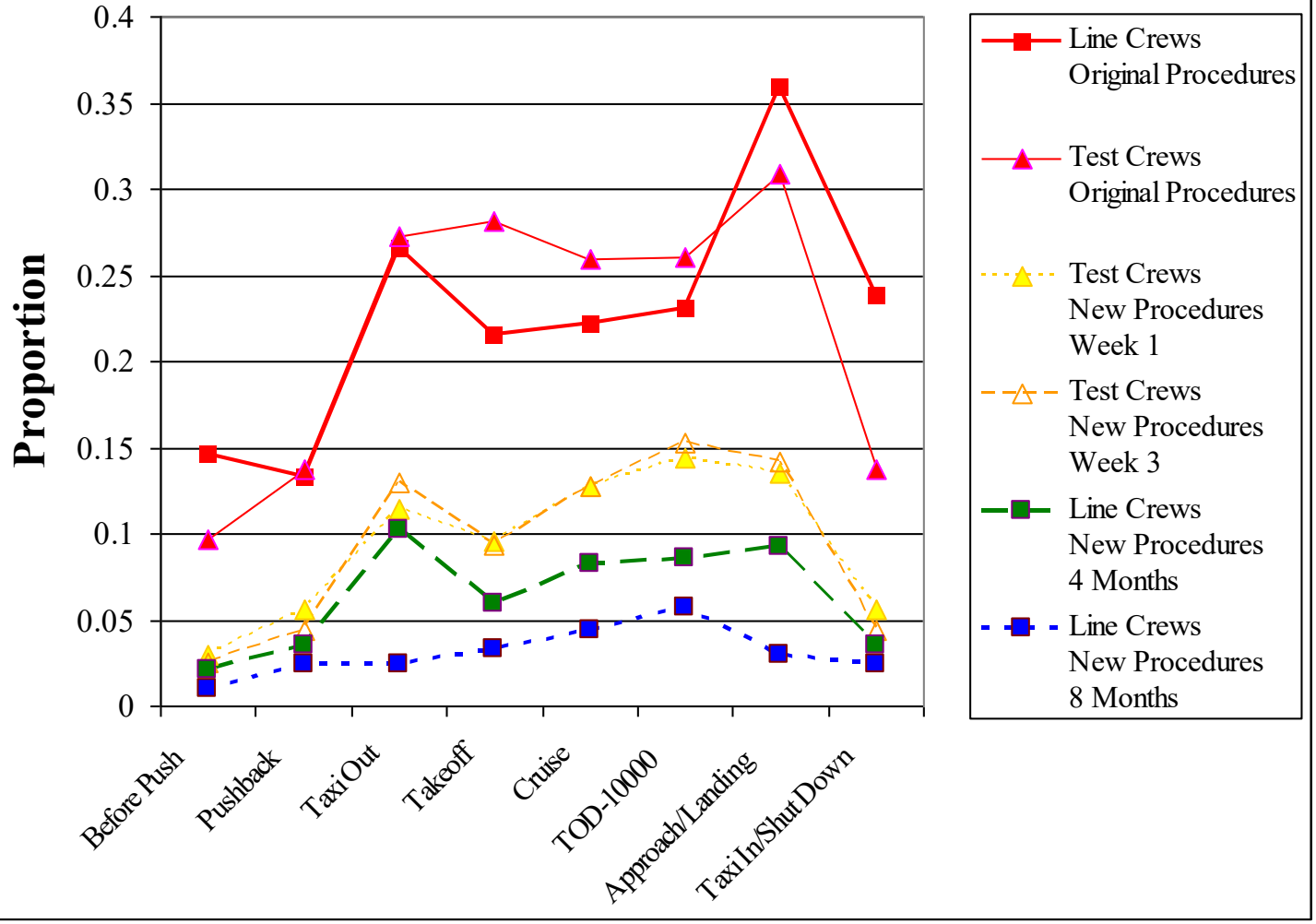


Figure 3. Problems on Target Items by Phase of Flight



How to "Change the Narrative…"

…that people are the safety problem

IMPLICATIONS

- Designs intended to "protect" the system from "error-prone" humans can design-out the capability for the human to effectively intervene/adapt, which is a far more common behavior
- Designs intended to replace humans often fail to acknowledge or understand the capabilities that humans routinely contribute to safety, and therefore fail (or don't have the data/knowledge) to design that into the system
- Designs that leverage a "safety pilot" who will only intervene to "save the day" in rare failure events fail to consider how our cognitive systems work and how they evolved to work. Such designs are setting up the safety pilot to fail.

How to "Change the Narrative…"

…that people are the safety problem

PROPOSED SOLUTION

- In today's aerospace industry, *data talks*
- When the only data that are available are about human failure, then data-driven designs only consider that humans fail
- To change the narrative, we need new data and new ways to examine data
  - Specifically, data on how (and the processes by which) humans *contribute* to safety

IMPACTS

- Safer system designs
- Increased organizational awareness
- Improved operational learning/training
- System safety that is robust and resilient to future changes

Make it easy to do the right thing.

Make it difficult to do the wrong thing.

Make it extremely difficult (impossible?) to do the catastrophic thing.

Human Systems integration division

Additional Information:

NASA/TM—2016–219421

Designing Flightdeck Procedures

Immanuel Barshi
NASA Ames Research Center

Robert Mauro
Decision Research
University of Oregon

Asaf Degani
General Motors Advanced Technology Center

Loukia Loukopoulou
San Jose State University Foundation
SWISS International Air Lines

October 2016

NASA/TP—2017–219479

Designing Flightdeck Procedures: Literature Resources

Jolene Feldman
San Jose State University Research Foundation

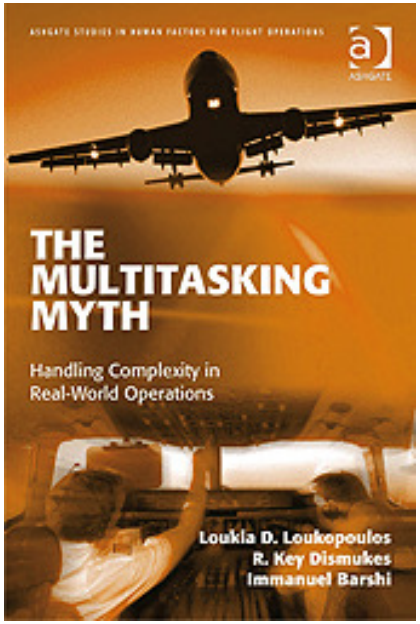
Immanuel Barshi
NASA Ames Research Center

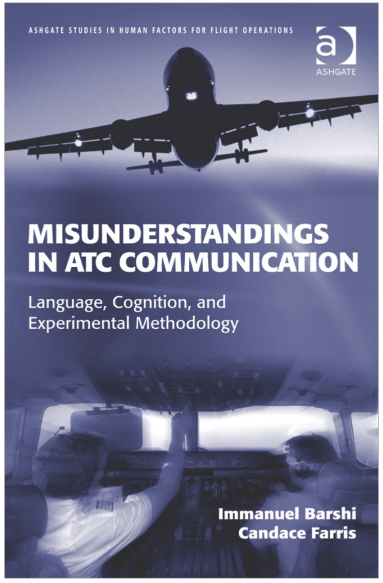
Asaf Degani
General Motors Advanced Technology Center

Loukia Loukopoulou
San Jose State University Research Foundation and the SWISS International Air Lines

Robert Mauro
Decision Research and the University of Oregon

March 2017





Or contact me at: Immanuel.Barshi@nasa.gov

Thank you!

November 2nd, 2023

Human Systems
integration division

Immanuel.Barshi@nasa.gov

NASA