Microsoft Azure

Building resilience

How to learn more from incidents

Nick Stenning (@nickstenning)

written with Jessica DeVita (@ubergeekgirl)

http://www.americanairmuseum.com/aircraft/10376

Agenda

1. Why learn from incidents?

Agenda

1. Why learn from incidents?

2. Four common traps.

Agenda

1. Why learn from incidents?

2. Four common traps.

3. Four helpful practices.

Why should we learn from incidents?

How Complex Systems Fail

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

Richard I. Cook, MD

https://aka.ms/csfail

"Complex systems contain changing mixtures of failures latent within them."

https://aka.ms/csfail

“Complex systems contain changing mixtures of failures latent within them.”

“Complex systems run in degraded mode.”

https://aka.ms/csfail

“Complex systems contain changing mixtures of failures latent within them.”

“Complex systems run in degraded mode.”

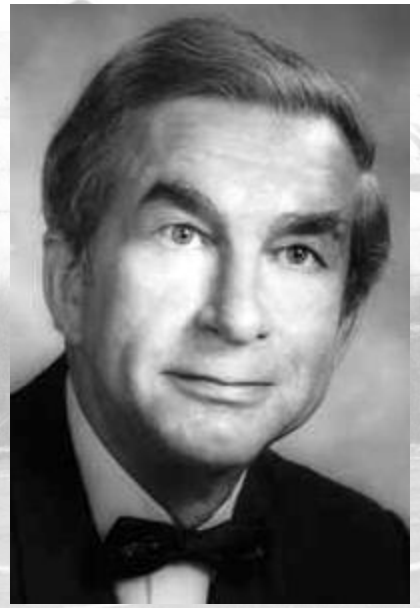
“Catastrophe is always just around the corner.”

https://aka.ms/csfail

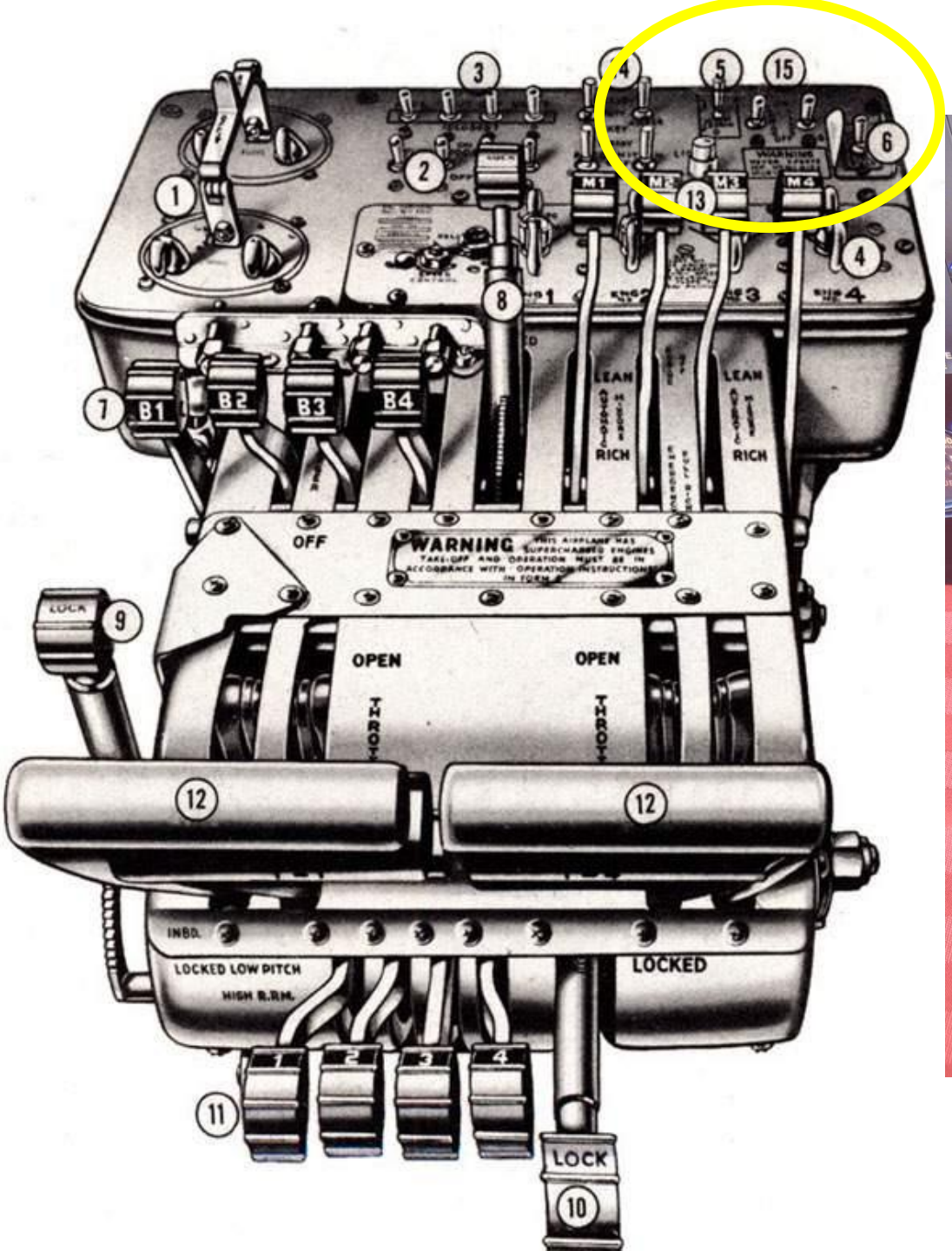
Prevent a catastrophe

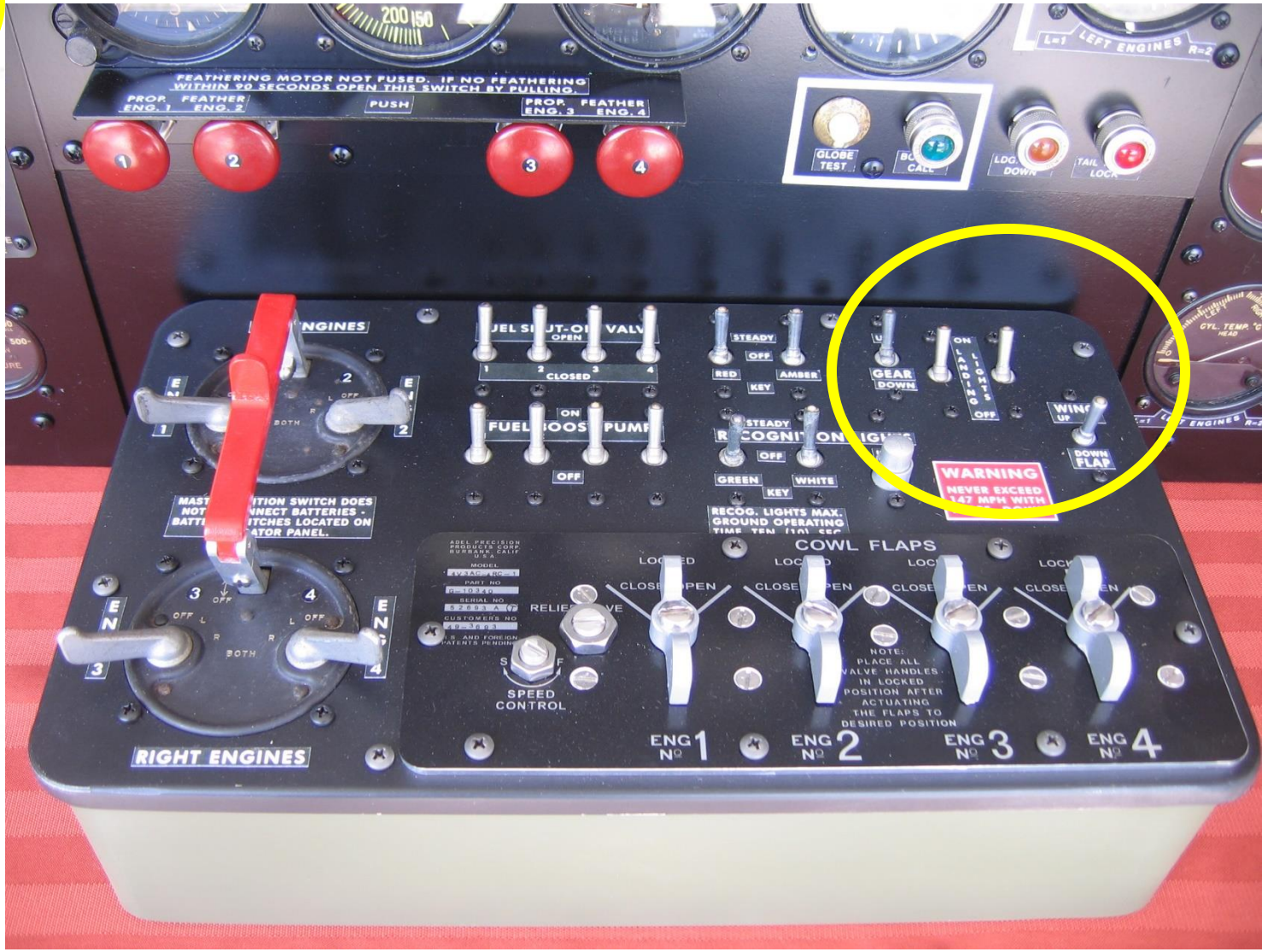
Respond to a catastrophe

Language matters

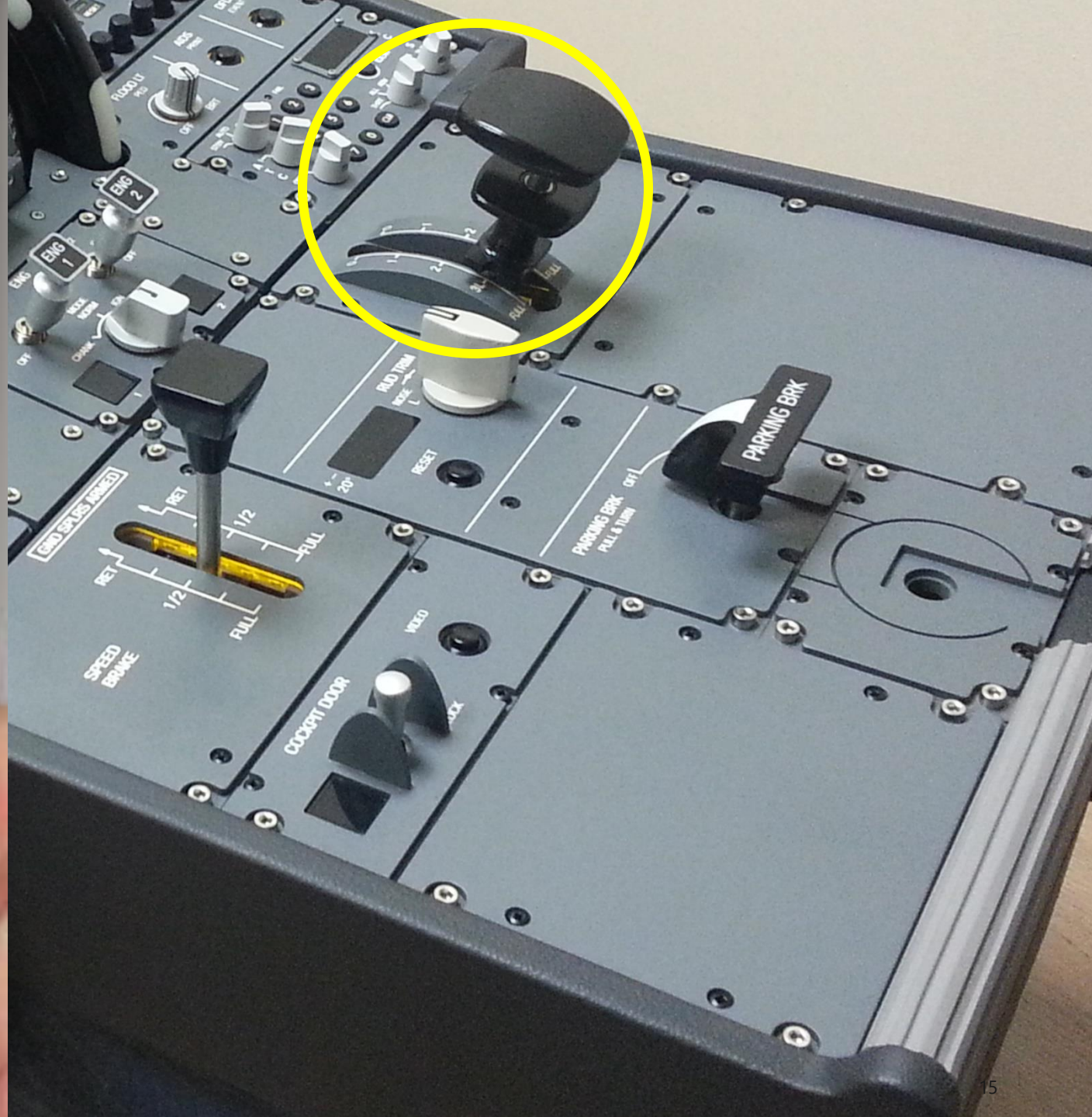


Alphonse Chapanis


1
2
3
4
5
6
7
8
9
10
11
12
13
15
B1
B2
B3
B4
M1
M2
M3
M4
LEAN
RICH
OFF
WARNING
OPEN
THROT
INBD.
LOCKED LOW PITCH
HIGH R.P.M.
LOCKED
LOCK


FEATHERING MOTOR NOT FUSED. IF NO FEATHERING WITHIN 90 SECONDS OPEN THIS SWITCH BY PULLING.
PROP. FEATHER ENG. 1 ENG. 2
PUSH
PROP. FEATHER ENG. 3 ENG. 4
GLOBE TEST
LDG. DOWN
TAIL LOCK
LEFT ENGINES
CLOSED
STEADY
RED
AMBER
GEAR DOWN
LANDING LIGHTS
WING UP
DOWN FLAP
WARNING
NEVER EXCEED 147 MPH WITH
GREEN
WHITE
RECOG. LIGHTS MAX. GROUND OPERATING
COWL FLAPS
SPEED CONTROL
RIGHT ENGINES
ENG Nº 1
ENG Nº 2
ENG Nº 3
ENG Nº 4

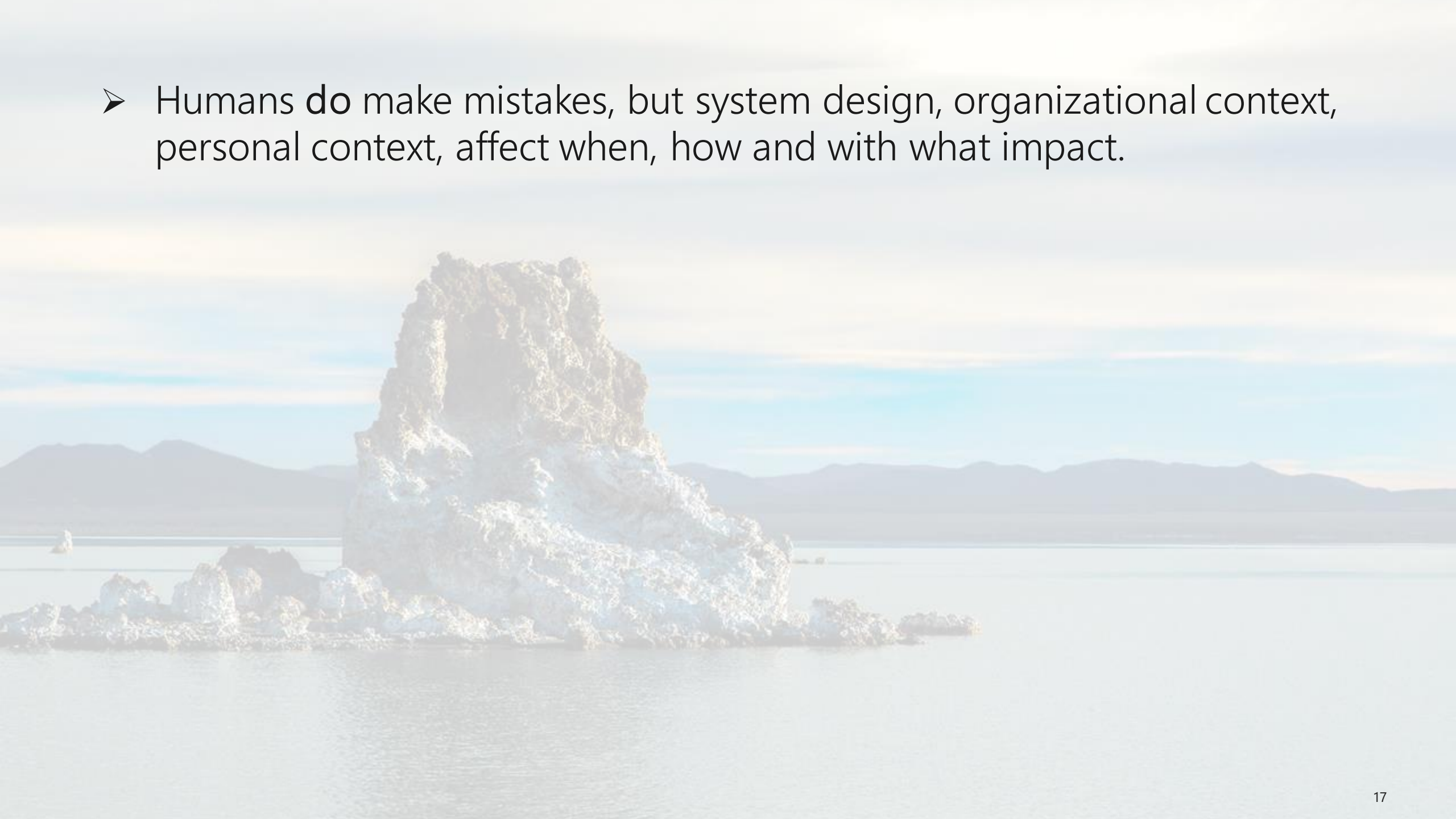
UP
DOWN

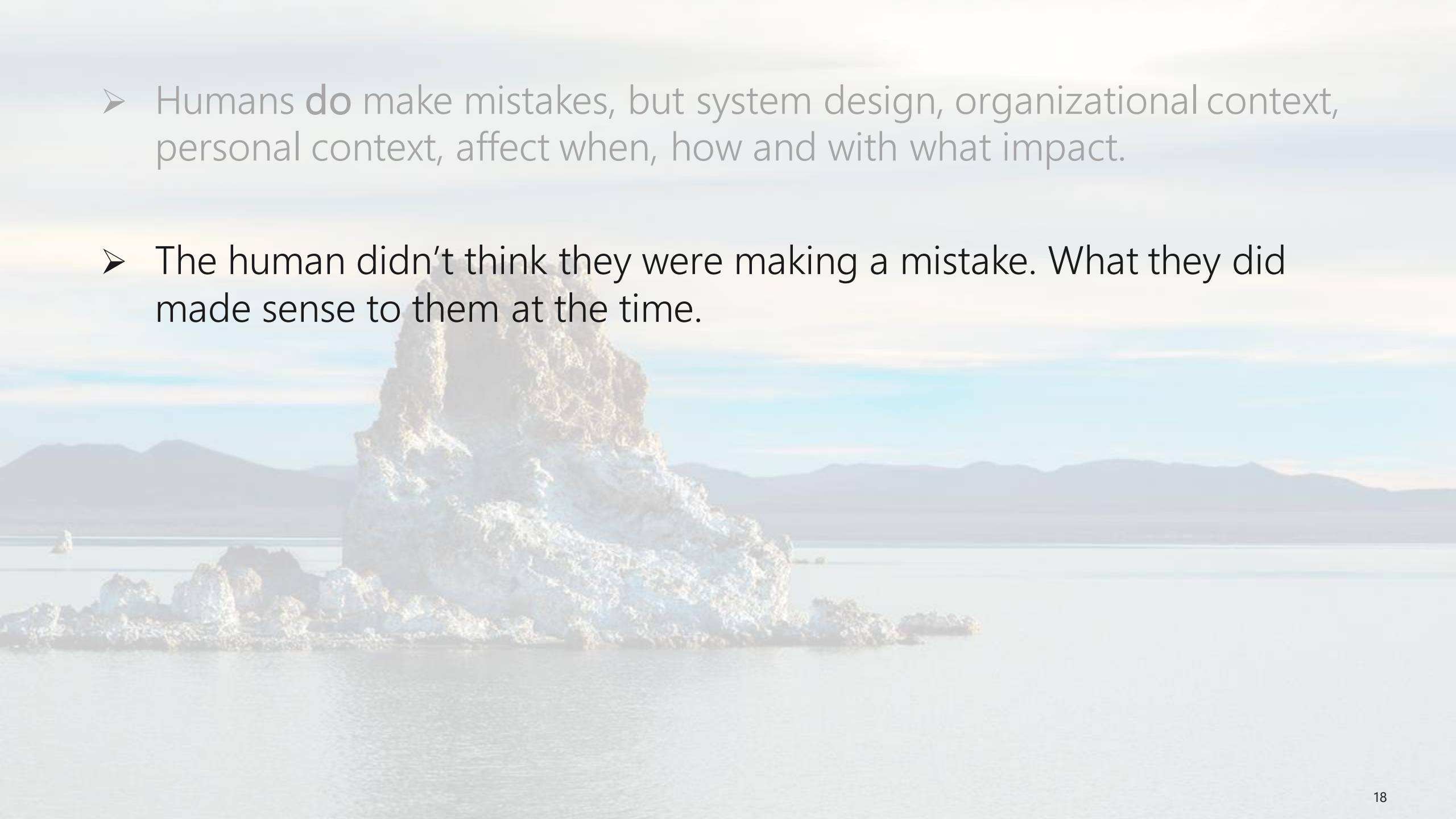

ENG 2
ENG 1
RUD TRIM
RESET
PARKING BRK
RET
1/2
FULL
SPEED BRAKE
COCKPIT DOOR
VIDEO

Trap #1: Attribution to “human error”

Photograph by Sheila Sund (https://flic.kr/p/FzZFb1)

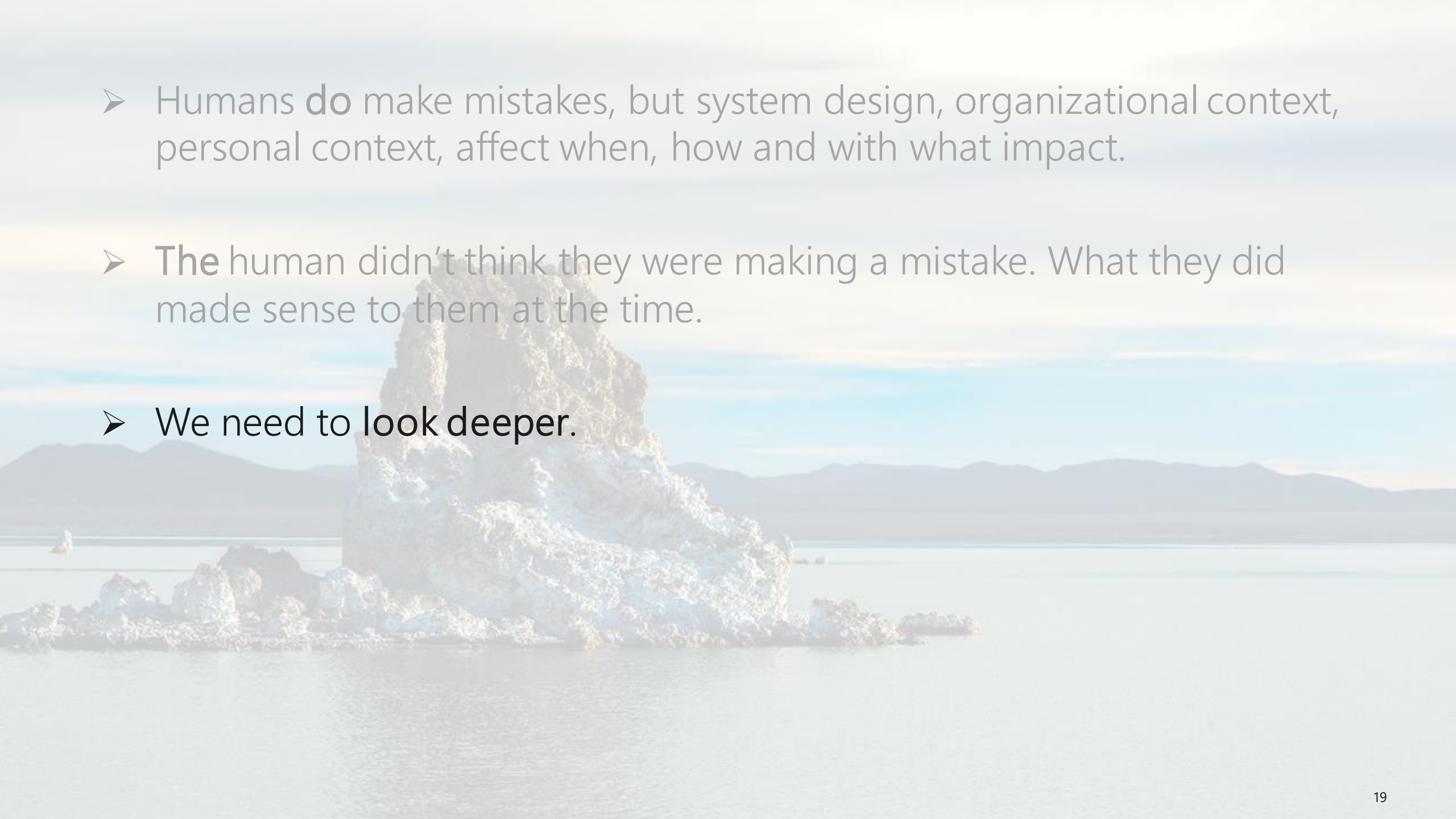
- Humans **do** make mistakes, but system design, organizational context, personal context, affect when, how and with what impact.





- Humans **do** make mistakes, but system design, organizational context, personal context, affect when, how and with what impact.

- The human didn't think they were making a mistake. What they did made sense to them at the time.



- Humans **do** make mistakes, but system design, organizational context, personal context, affect when, how and with what impact.

- **The** human didn't think they were making a mistake. What they did made sense to them at the time.

- We need to **look deeper**.

- Humans **do** make mistakes, but system design, organizational context, personal context, affect when, how and with what impact.

- The human didn't think they were making a mistake. What they did made sense to them at the time.

- We need to look deeper.

- **The problem:** "Human error" is *a label which causes us to stop investigating* at precisely the moment when we're about to discover something interesting about our system.

Trap #2: Counterfactual reasoning

Photograph by Einheit 00 (https://flic.kr/p/oQ5X91)

- Counterfactual reasoning: when you hear “should have,” “could have,” “would have,” “failed to,” “did not.”

- Counterfactual reasoning: when you hear “should have,” “could have,” “would have,” “failed to,” “did not.”

- Counterfactual reasoning is telling a story about events that *did not happen*, in order to explain events that did.

- Counterfactual reasoning: when you hear “should have,” “could have,” “would have,” “failed to,” “did not.”

- Counterfactual reasoning is telling a story about events that *did not happen*, in order to explain events that did.

- “The engineer failed to check the validity of the configuration” … “This could been have picked up in the canary environment”

- Counterfactual reasoning: when you hear “should have,” “could have,” “would have,” “failed to,” “did not.”

- Counterfactual reasoning is telling a story about events that *did not happen*, in order to explain events that did.

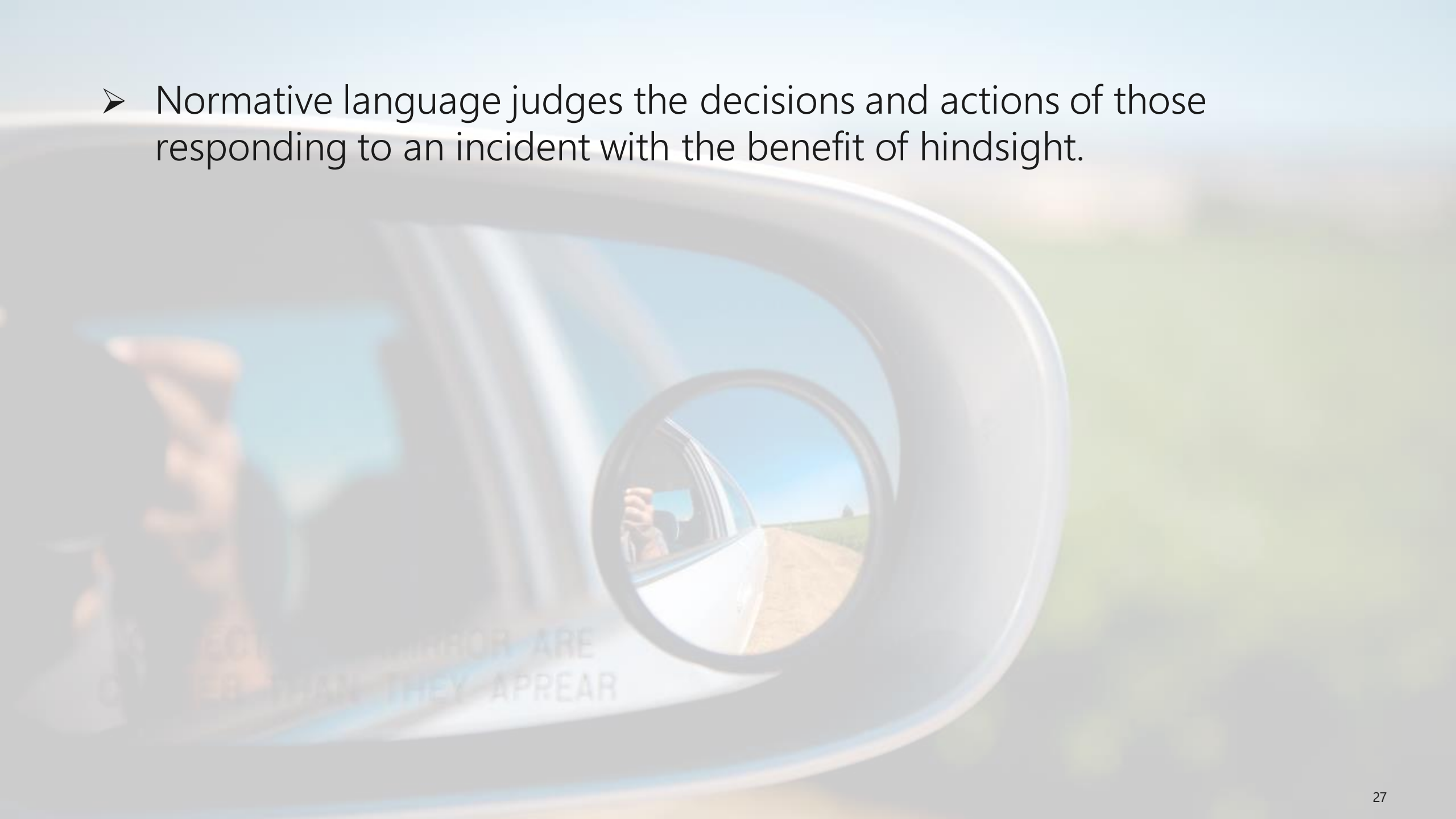
- “The engineer failed to check the validity of the configuration” … “This could been have picked up in the canary environment”

- **The problem:** we’re talking about things that *didn’t happen* instead of taking the time to understand how what happened, happened.

Trap #3: Normative language

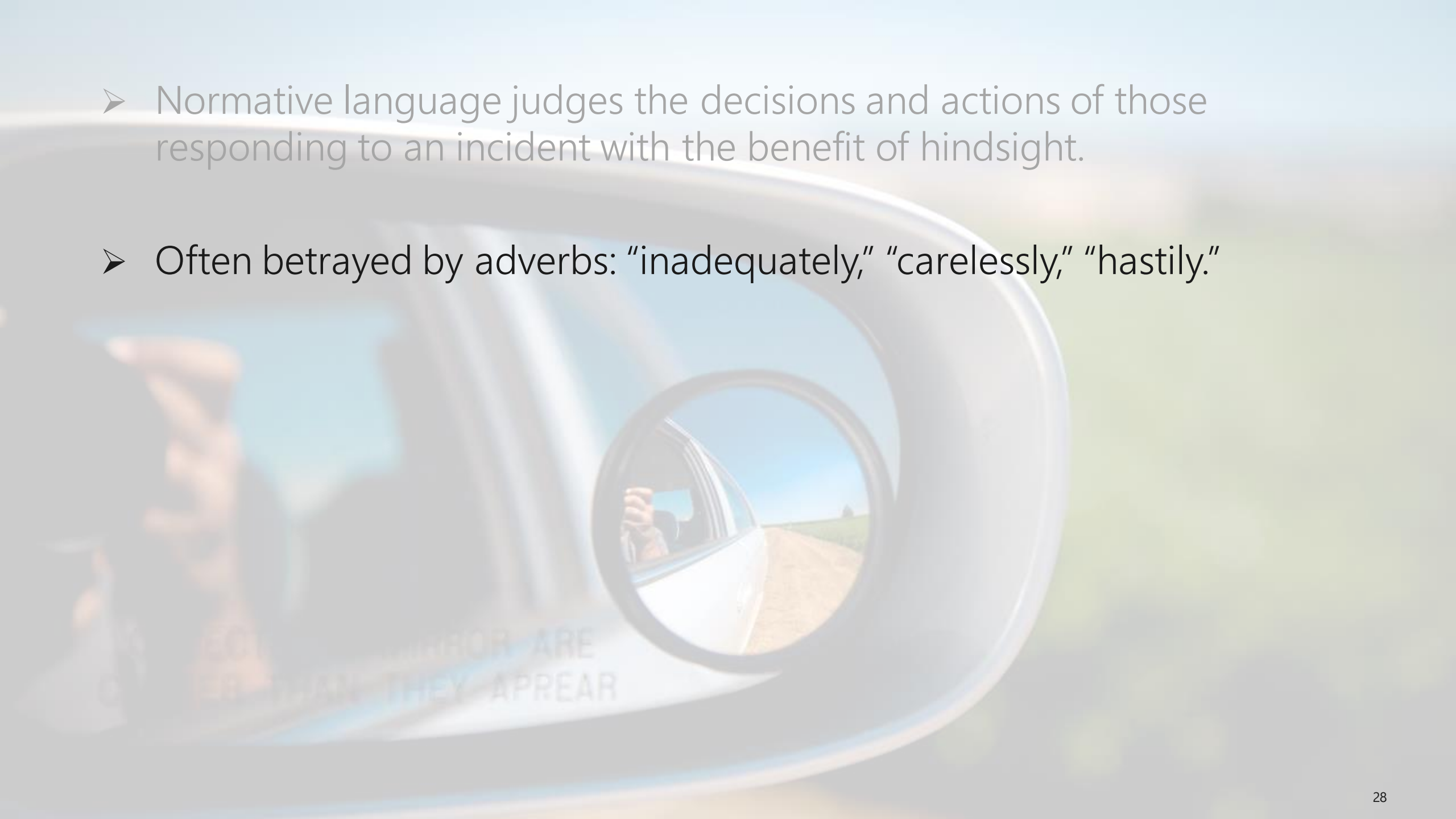
Photograph by Nimish Gogri (https://flic.kr/p/8WXy8B)

- Normative language judges the decisions and actions of those responding to an incident with the benefit of hindsight.



- Normative language judges the decisions and actions of those responding to an incident with the benefit of hindsight.

- Often betrayed by adverbs: “inadequately,” “carelessly,” “hastily.”



- Normative language judges the decisions and actions of those responding to an incident with the benefit of hindsight.

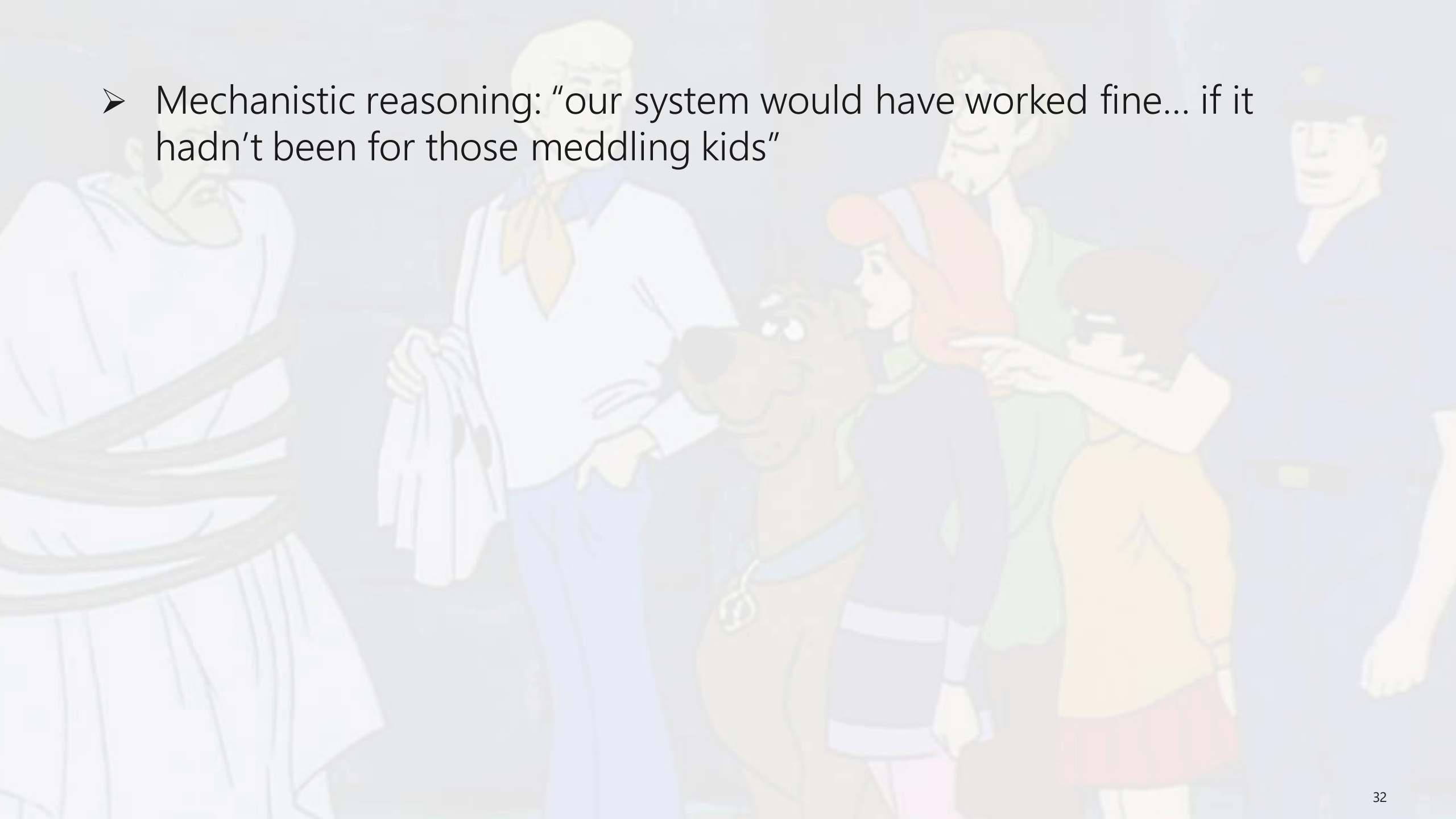
- Often betrayed by adverbs: “inadequately,” “carelessly,” “hastily.”

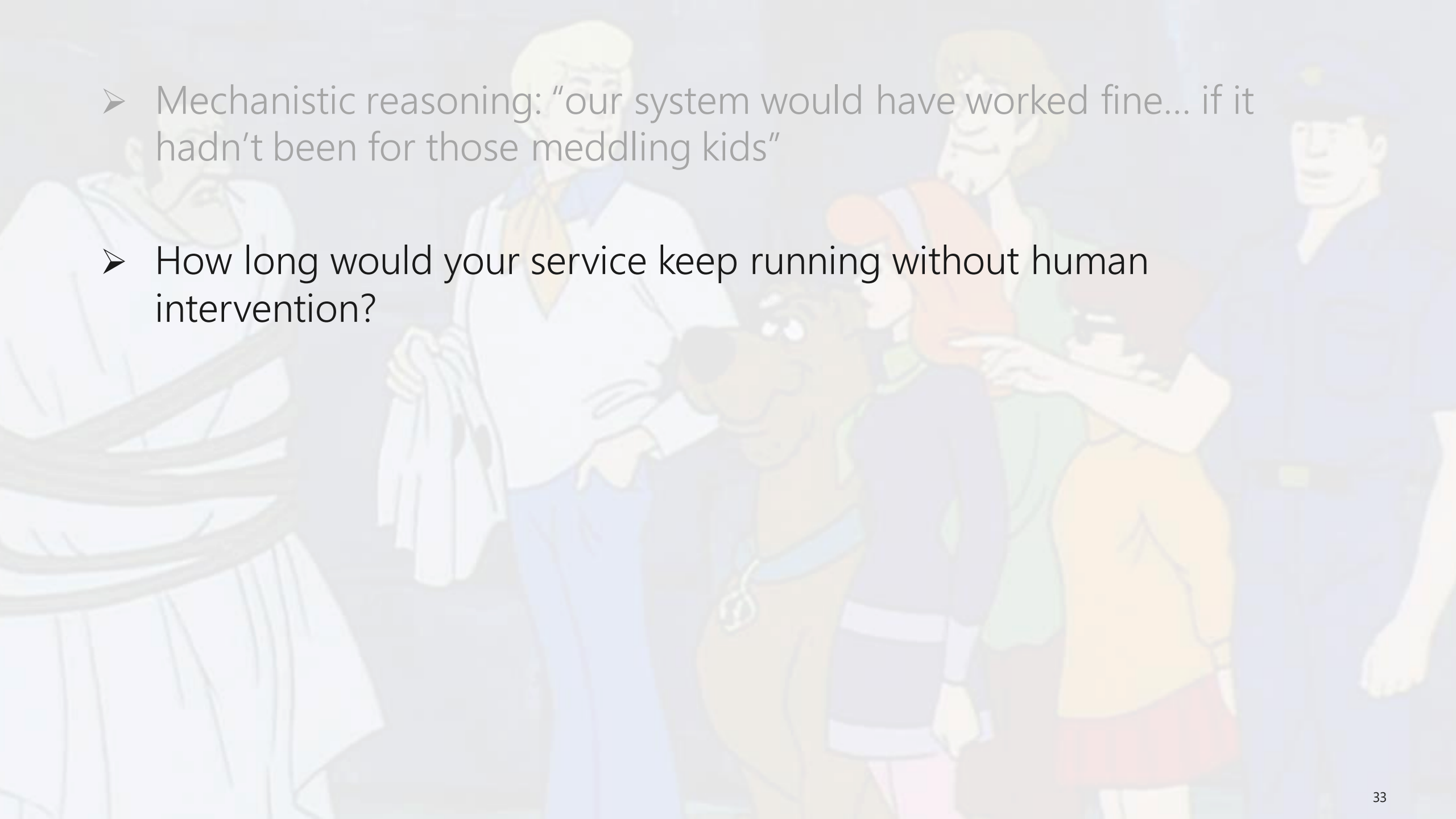
- Decisions of operators are judged on the basis of their outcomes: the one piece of information not available to the person making the decision.

- Normative language judges the decisions and actions of those responding to an incident with the benefit of hindsight.
- Often betrayed by adverbs: “inadequately,” “carelessly,” “hastily.”
- Decisions of operators are judged on the basis of their outcomes: the one piece of information not available to the person making the decision.
- **The problem:** if we accept post-hoc normative judgment, we neglect to understand how the actions of operators made sense to them at the time.

Trap #4: Mechanistic reasoning

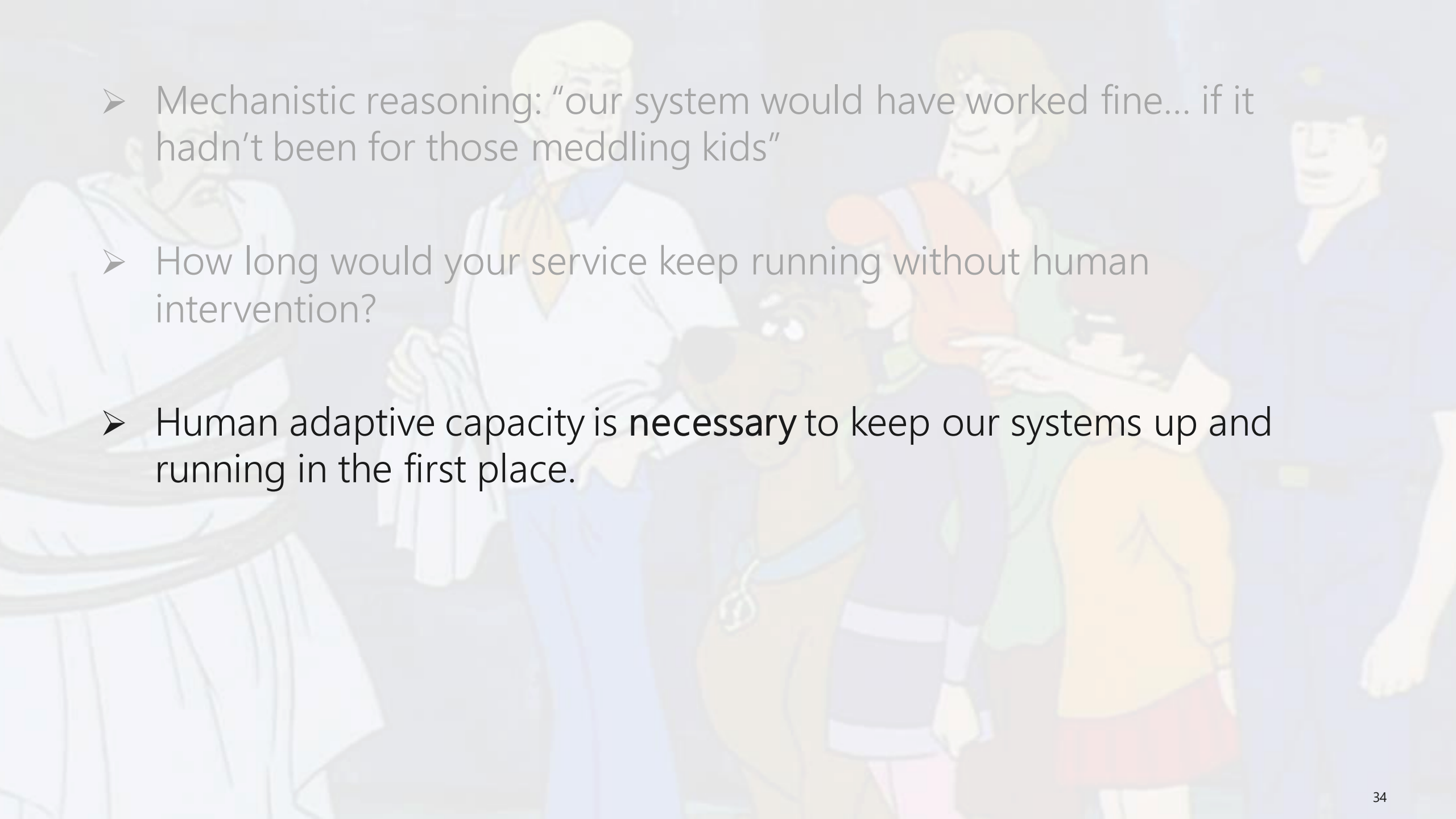
- Mechanistic reasoning: “our system would have worked fine… if it hadn’t been for those meddling kids”



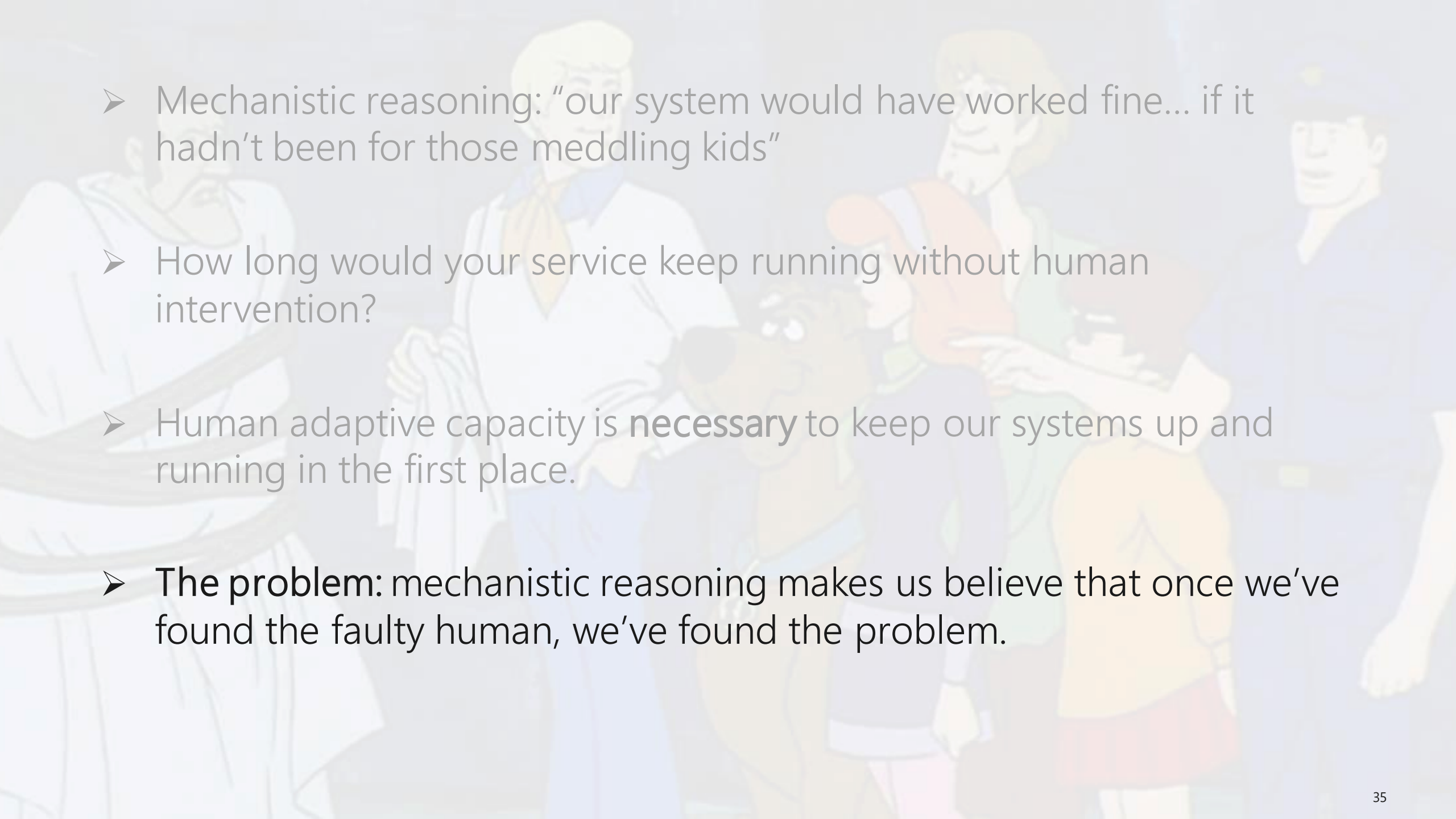


- Mechanistic reasoning: “our system would have worked fine… if it hadn’t been for those meddling kids”

- How long would your service keep running without human intervention?



- Mechanistic reasoning: “our system would have worked fine… if it hadn’t been for those meddling kids”
- How long would your service keep running without human intervention?
- Human adaptive capacity is **necessary** to keep our systems up and running in the first place.



- Mechanistic reasoning: “our system would have worked fine… if it hadn’t been for those meddling kids”
- How long would your service keep running without human intervention?
- Human adaptive capacity is **necessary** to keep our systems up and running in the first place.
- **The problem:** mechanistic reasoning makes us believe that once we’ve found the faulty human, we’ve found the problem.

Agenda

1. Why learn from incidents?
2. Four common traps.
3. Four helpful practices.

1. Run a facilitated post-incident review

Photograph by Melody Ayres-Griffiths (https://flic.kr/p/bnT21X)

1. Run a facilitated post-incident review

- A meeting with incident participants.
- ~60-90m maximum.
- Neutral facilitator (not actively involved in the incident).
- Prepare with one-to-one interviews.
- Lots of incidents? Don’t try and do this for all of them right away.

2. Ask better questions

Photograph by Barney Moss (https://flic.kr/p/gmMJ4K)

2. Ask better questions

- Language matters: prefer “how?” over “why?”
- Each participant has a different viewpoint: ask about that!
- Ask about what normally happens, too.
- Read Etsy’s Debriefing Facilitation Guide: https://aka.ms/etsydebriefing

3. Ask how things went *right*

Photograph by Dave Bleasdale (https://flic.kr/p/H9ZgUq)

3. Ask how things went *right*

- Ask about how we recovered the system.
- What insights/tools/skills/people were involved?
- How do people know what they know? Decide what they decide?
- Remember: we care about response as well as prevention.

4. Keep review and planning meetings separate

Photograph by Ian D Keating (https://flic.kr/p/2c9scLA)

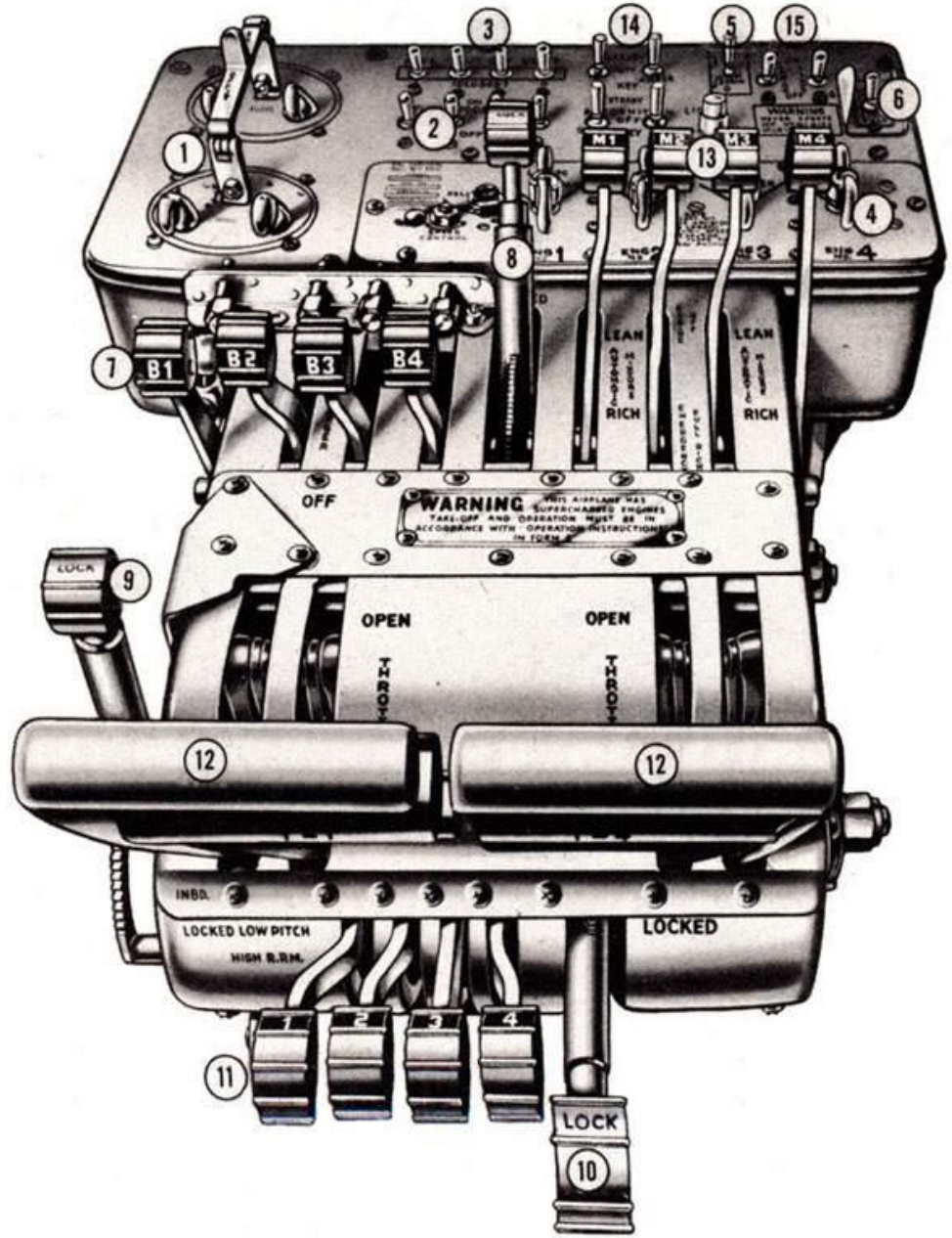
4. Keep review and planning meetings separate

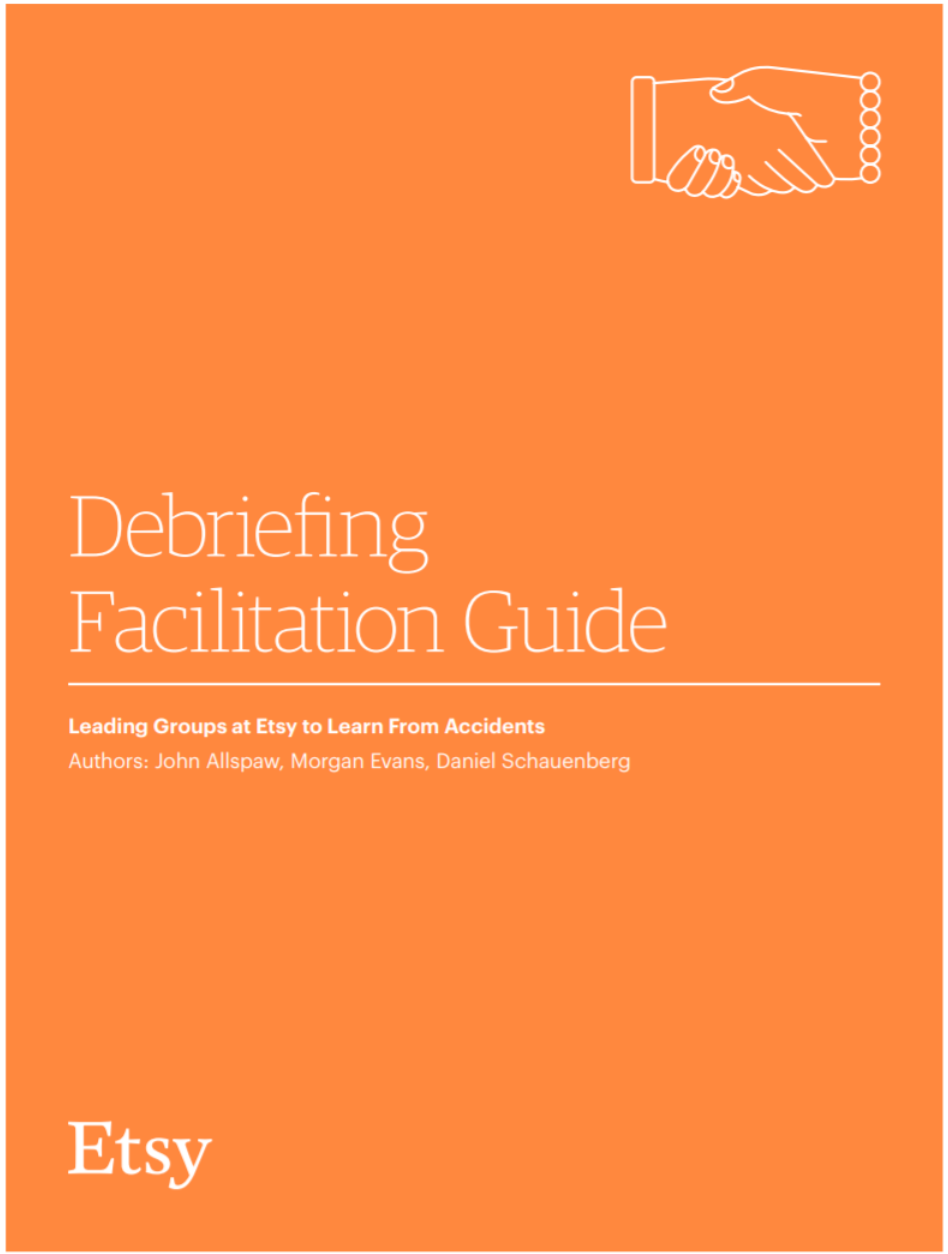
- Keep discussion of future mitigation out of the post-incident review.
- Hold a separate, smaller, planning meeting 24-48h later.
- Helps keep the focus on what actually happened.
- Allows “soak time” which will result in better repair items.

100%

⇒

WEST MOUNT
FIRE DEPT.
ENGINE
4


1
2
3
4
5
6
7
8
9
10
11
12
12
13
14
15
B1
B2
B3
B4
M1
M2
M3
M4
LEAN
RICH
LEAN
RICH
OFF
WARNING
OPEN
OPEN
LOCK
INBD.
LOCKED LOW PITCH
HIGH R.P.M.
LOCKED
1
2
3
4
LOCK


Debriefing
Facilitation Guide
Leading Groups at Etsy to Learn From Accidents
Authors: John Allspaw, Morgan Evans, Daniel Schauenberg
Etsy

Thank you

https://aka.ms/srecon19emea/lfi

Nick Stenning (@nickstenning)

Jessica DeVita (@ubergeekgirl)