Fantasy planning: the gap between systems of safety and safety of systems

The Day Book (Chicago, Ill.) ***Date:*** *April 16, 1912*
http://clickamericana.com/eras/1910s/scenes-of-horror-and-heroism-on-sinking-titanic-1912

"I can not imagine any condition which could cause this ship to founder. I can not conceive of any vital disaster happening to this vessel. Modern shipbuilding has gone beyond that."

Captain E.J. Smith, Master of SS Titanic, referring to the ship Adriatic.

Ben Hutchinson

Regional HSEQ Manager

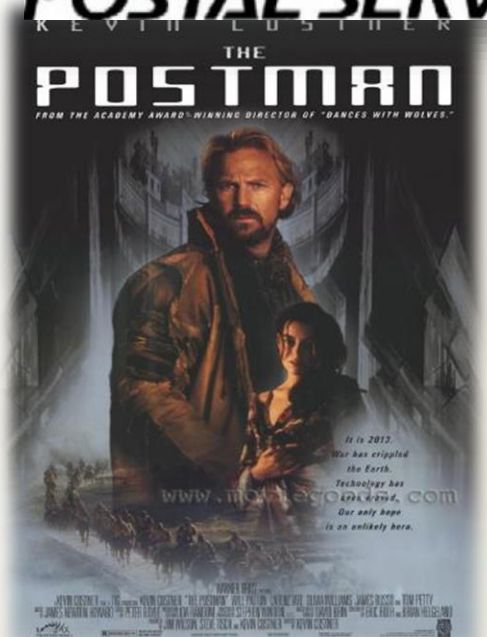
PhD Student – Safety Science

An Oil Magnate, Nuclear Engineer and Postal Worker walk into a bar…

2

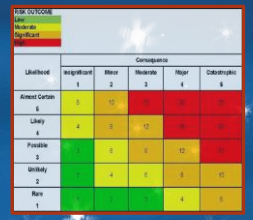
3

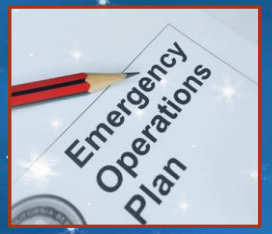
1

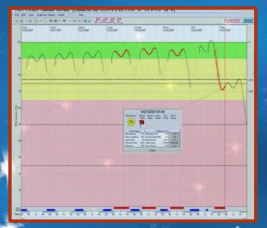


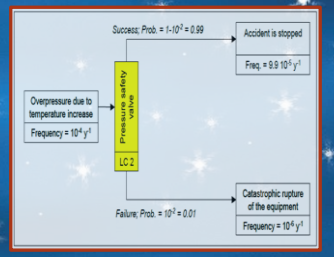
1 – Paul Searing https://www.flickr.com/photos/13995873@N05/
2 – The Atlantic https://www.theatlantic.com/photo/2014/03/the-exxon-valdez-oil-spill-25-years-ago-today/100703/
3 – Jim Brickett / Flickr https://www.flickr.com/photos/jimbrickett/

The Fables of Safety









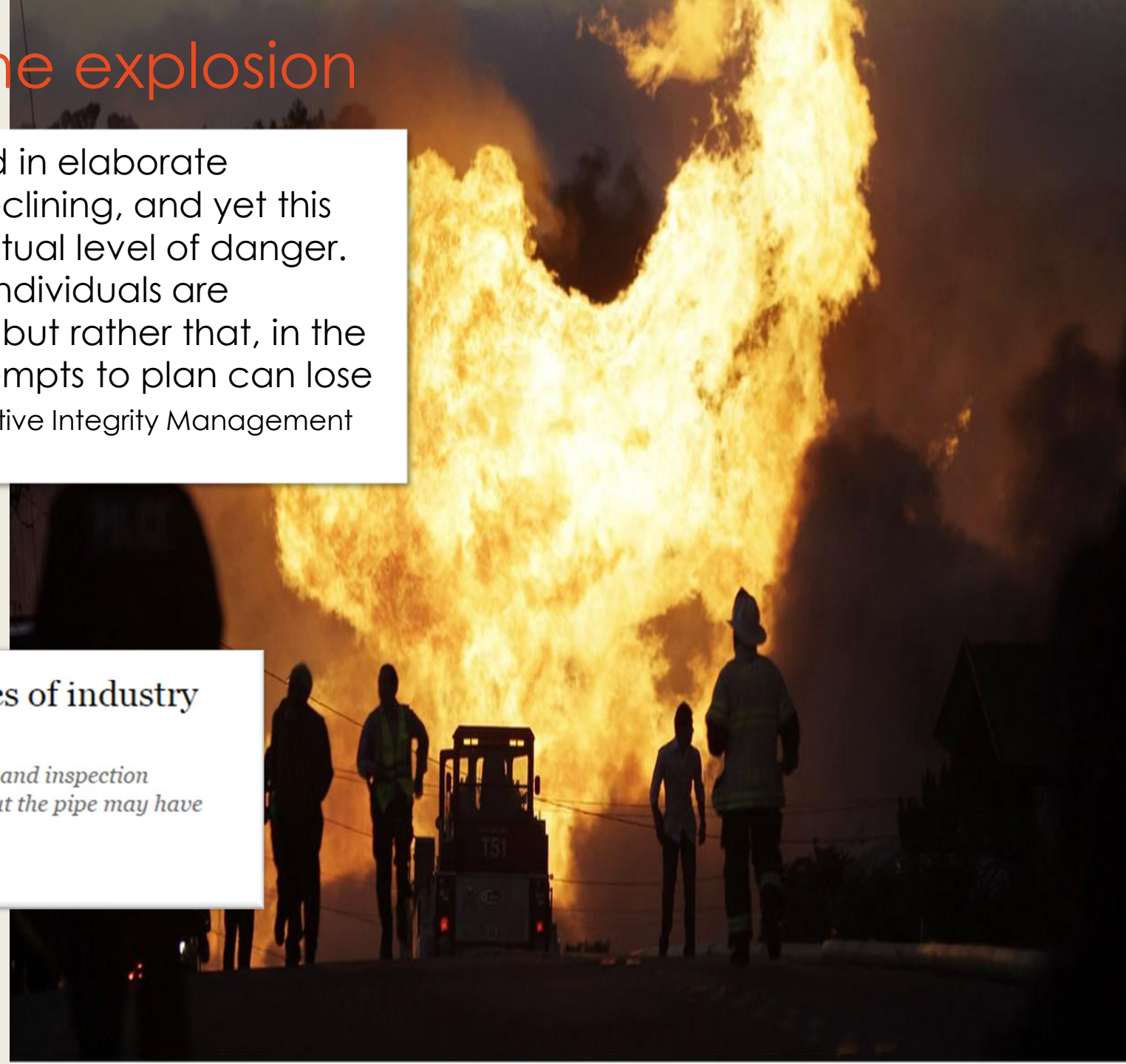
“For a successful technology, reality must take precedence over public relations, for nature cannot be fooled”

– Feynman 1986. Report of the Presidential Commission on the Space Shuttle Challenger accident.

Background: https://au.pinterest.com/pin/215258057162287016/

San Bruno pipeline explosion

"Knowing" about the system was grounded in elaborate algorithms … purported to show risk was declining, and yet this analysis was only tenuously linked to the actual level of danger. This is not to suggest that … companies or individuals are deliberately fabricating this type of plan … but rather that, in the face of significant uncertainty, earnest attempts to plan can lose touch with reality. – Hayes, 2015, 'Lessons for Effective Integrity Management from the San Bruno Pipeline Rupture', pg. 205



San Bruno gas blast gives ammunition to critics of industry risk assessment

These experts say companies have put far too much faith in technology and inspection methods. The segment wasn't one of PG&E's top 100 safety priorities but the pipe may have been brittle and corroded by water and sewage, evidence indicates.

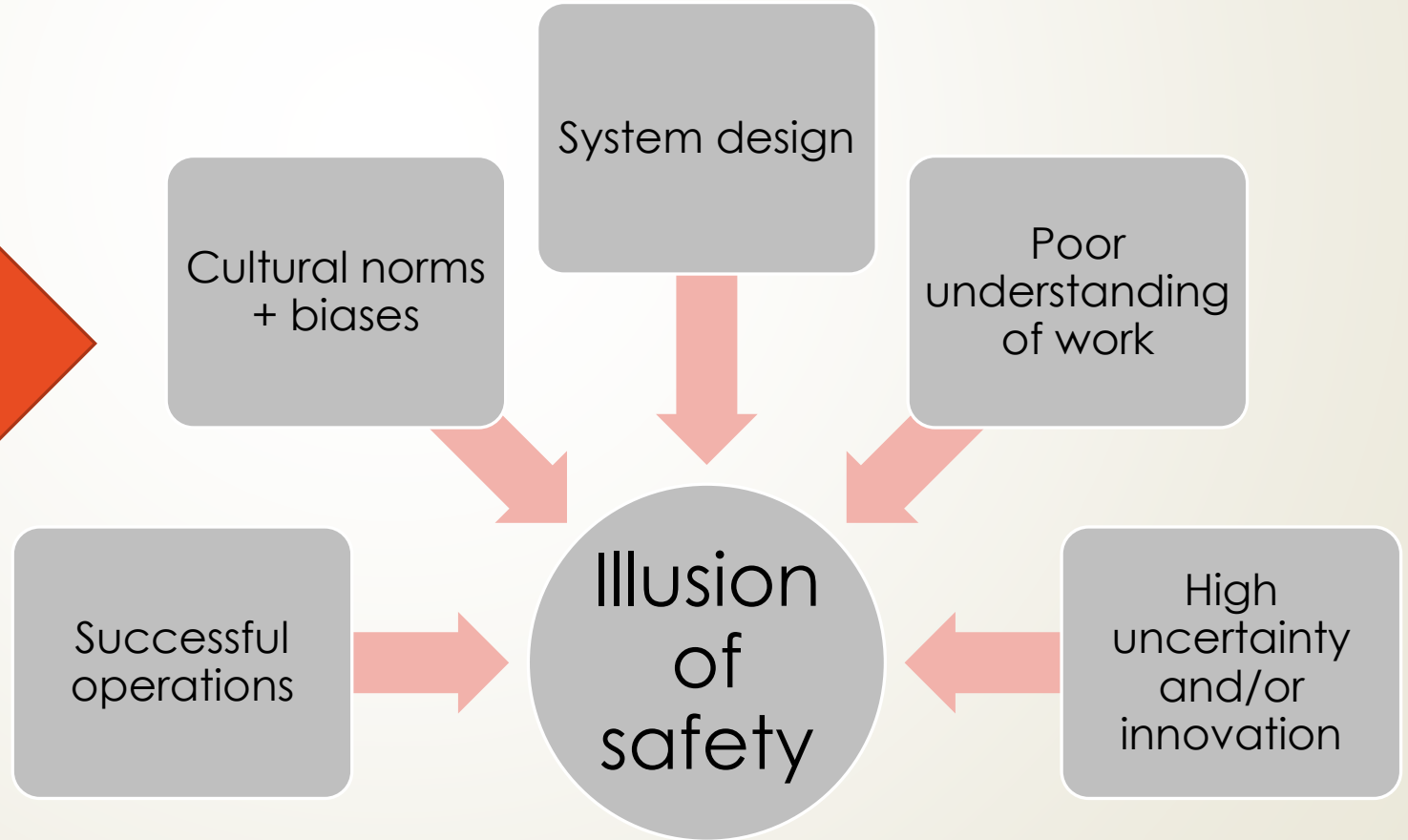
October 07, 2010 | By Ralph Vartabedian, Los Angeles Times

http://articles.latimes.com/2010/oct/07/local/la-me-brittle-pipeline-20101007

How Does an Illusion of Safety Come About?

"[M]any of us ask for certainty from our bankers, our doctors, and our political leaders. What they deliver in response is the illusion of certainty. Many of us smile at old-fashioned fortune-tellers. But when the soothsayers work with computer algorithms rather than tarot cards, we take their predictions seriously and are prepared to pay for them" -- Gigerenzer, 2014, Risk Savvy, pg.26

Some reasons
…not exhaustive



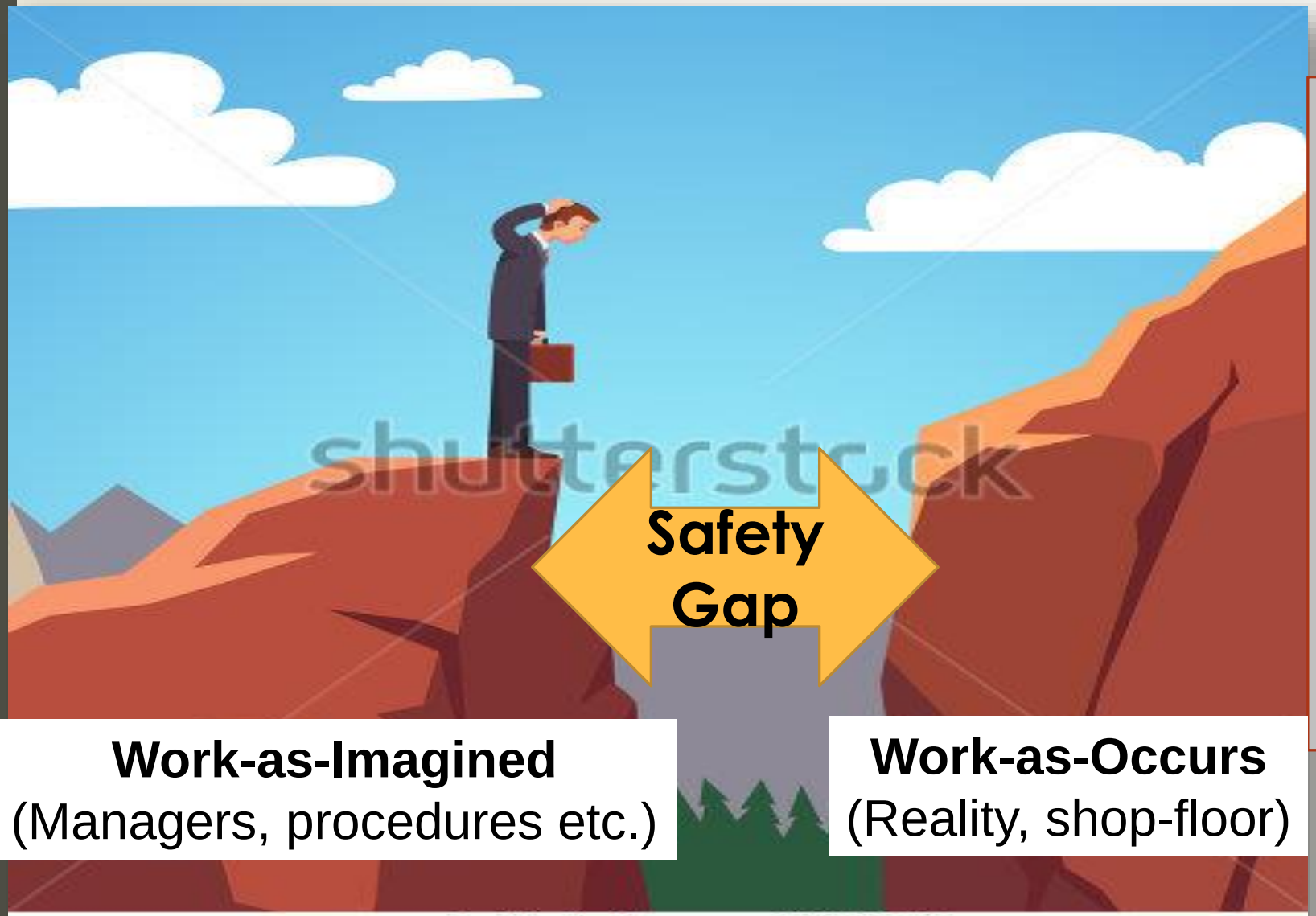
How much safety in safety management?

- "even the best management system is defective if it is not effectively implemented. The system must be capable of being understood by those expected to implement it" Dawson and Brooks, 1999, Report of the Longford Royal Commission, 200

- "Nimrod Safety Case[s] were fatally undermined by an assumption by all the organisations and individuals involved that the Nimrod was 'safe anyway', because the Nimrod fleet had successfully flown for 30 years, and they were merely documenting something which they already knew. The Nimrod Safety Case became essentially a paperwork and 'tick-box' exercise" Haddon-Cave, 2009, The Nimrod Review Report. Loss of XV230, 190

- ''Prior to Challenger, the can-do culture was a result not just of years of apparently successful launches, but of the cultural belief that the Shuttle Program's many structures, rigorous procedures, and detailed system of rules were responsible for those successes." Columbia Accident Investigation Board, 2003, 199

Oh, human error you say?

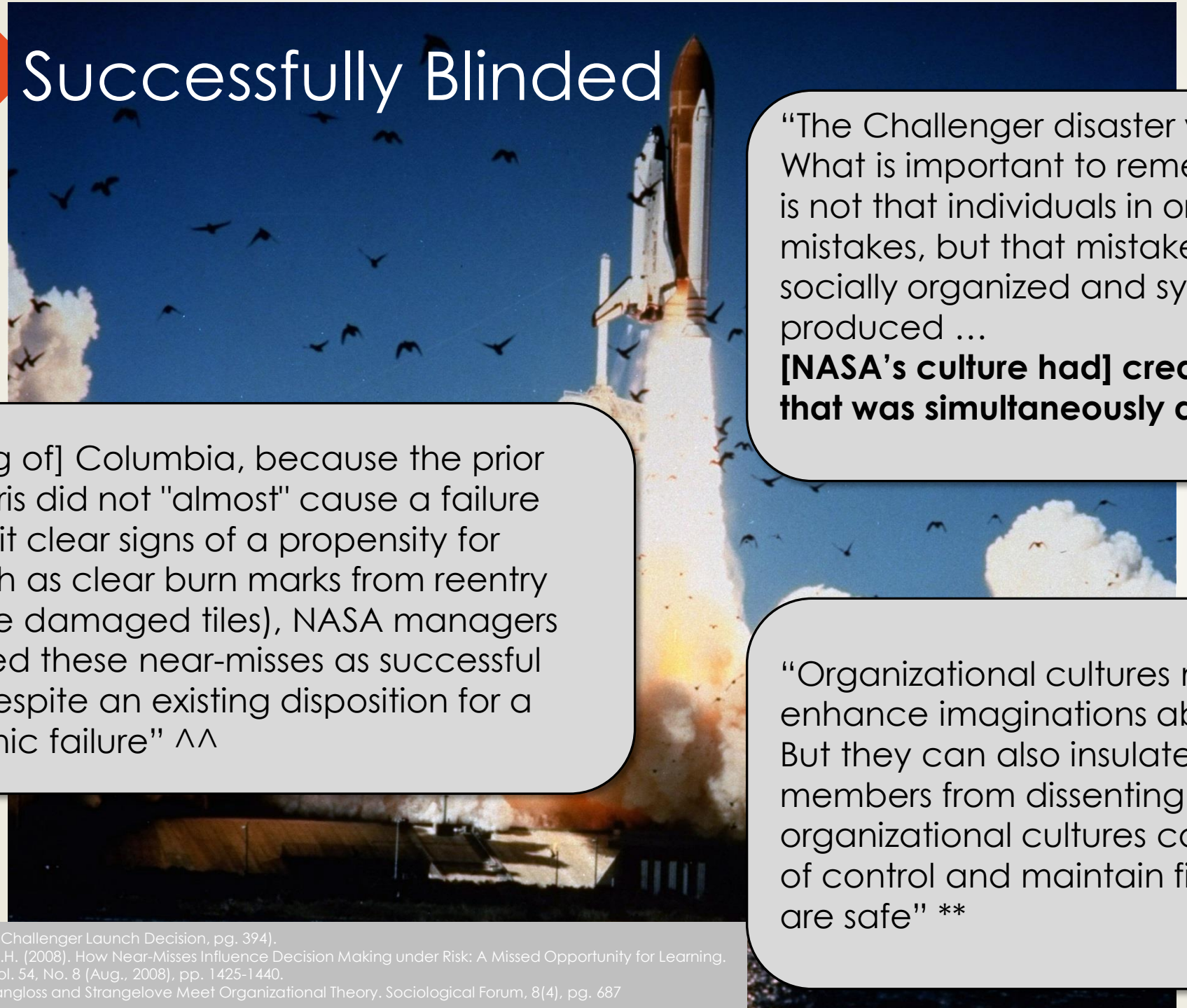


"A 'human error' problem is an organizational problem.

A 'human error' problem is at least as complex as the organization that helped create it"

- Dekker, S. (2014). Field Guide to Understanding Human Error, pg.192.

Successfully Blinded



"The Challenger disaster was an accident, … What is important to remember from this case is not that individuals in organizations make mistakes, but that mistakes themselves are socially organized and systematically produced …
[NASA's culture had] created a way of seeing that was simultaneously a way of not seeing." ǂ

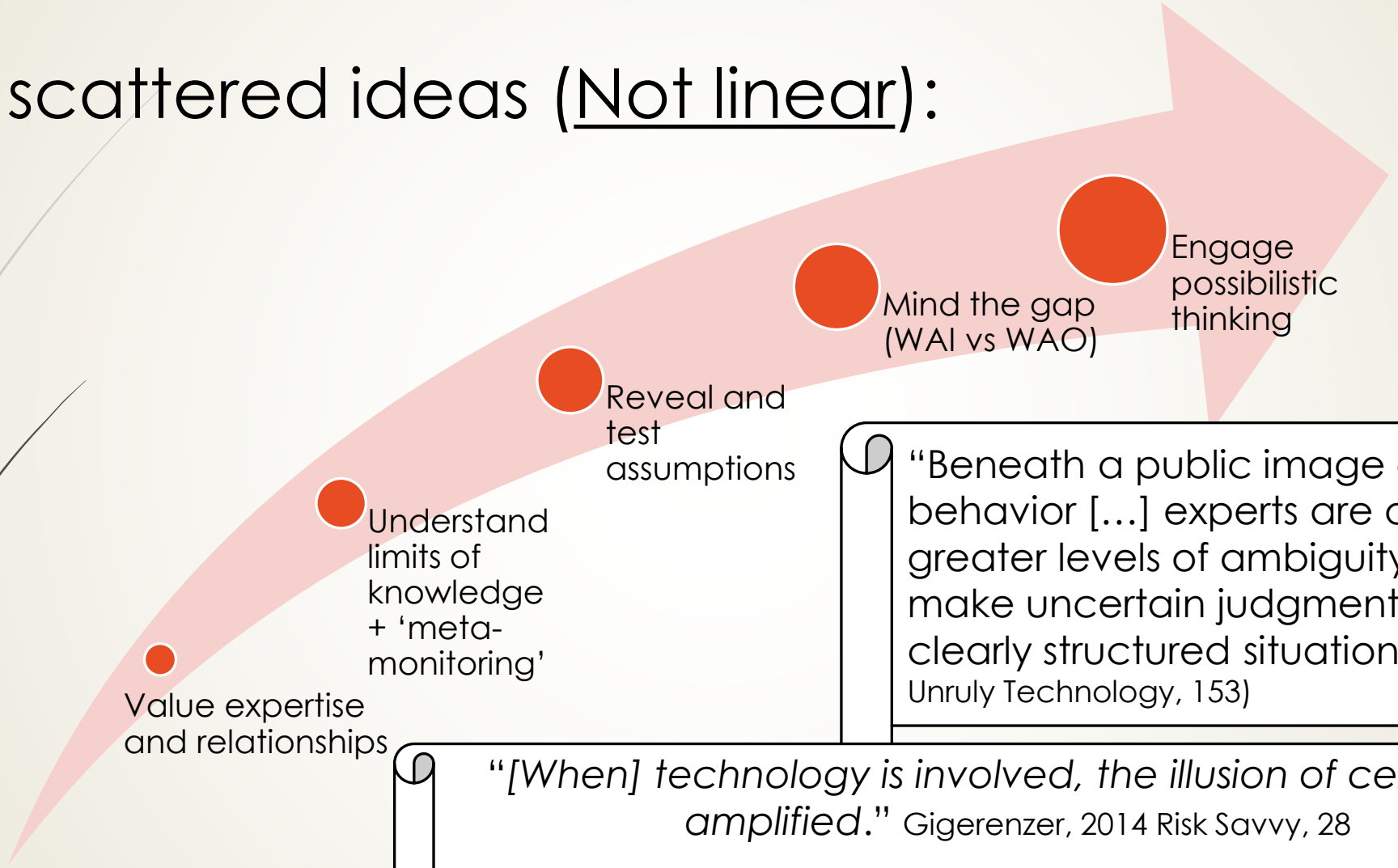
"[Speaking of] Columbia, because the prior foam debris did not "almost" cause a failure (i.e., exhibit clear signs of a propensity for failure such as clear burn marks from reentry around the damaged tiles), NASA managers categorized these near-misses as successful missions despite an existing disposition for a catastrophic failure" ^^

"Organizational cultures may be organized to enhance imaginations about risk and safety. But they can also insulate organizational members from dissenting points of view. And organizational cultures can perpetuate myths of control and maintain fictions that systems are safe" **

ǂ Vaughan, D. (1996). The Challenger Launch Decision, pg. 394).
^^ Dillon, R.L., & Tinsley, C.H. (2008). How Near-Misses Influence Decision Making under Risk: A Missed Opportunity for Learning. Management Science, Vol. 54, No. 8 (Aug., 2008), pp. 1425-1440.
** Clarke, L. (1993). Drs. Pangloss and Strangelove Meet Organizational Theory. Sociological Forum, 8(4), pg. 687

A Firm Grip on Reality (…whatever that is)

Some scattered ideas (Not linear):



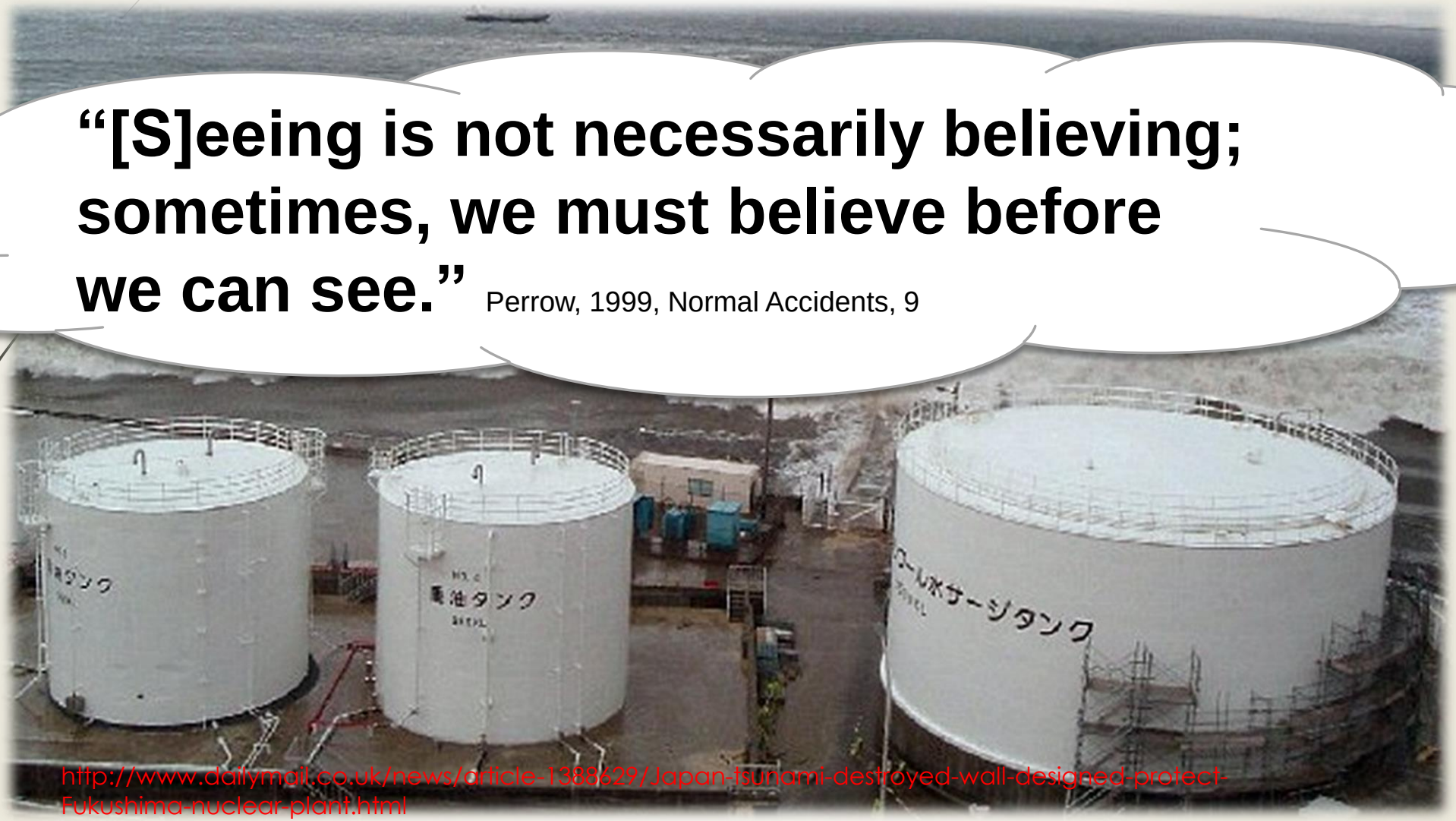
"Beneath a public image of rule-following behavior […] experts are opening with far greater levels of ambiguity, needing to make uncertain judgments in less than clearly structured situations" Wynne (1988, Unruly Technology, 153)

"*[When] technology is involved, the illusion of certainty is amplified.*" Gigerenzer, 2014 Risk Savvy, 28

"[We have a] tendency to look at what confirms our knowledge, not our ignorance" Taleb, 2007 The black swan, 30

Probabilistic vs Possibilistic thinking. Or: "**things that have never happened before happen all the time.**" (Sagan, 1993, The Limits of Safety,12)

“[S]eeing is not necessarily believing; sometimes, we must believe before we can see.” Perrow, 1999, Normal Accidents, 9



http://www.dailymail.co.uk/news/article-1388629/Japan-tsunami-destroyed-wall-designed-protect-Fukushima-nuclear-plant.html

Questions?

"Where technological domains trade in 'hard data' and 'solid technical conclusions' their discourse is masking the ambiguities and social processes behind these data."

- Downer, 2009, Watching the Watchmaker, 9

"The Safety Case regime has lost its way. It has led to a culture of 'paper safety' at the expense of *real* safety."

- Haddon-Cave, 2009, The Nimrod Review Report. Loss of XV230, 533