RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: HUM-R02

Preventing Cyber Exposure: You Say Criminal, I Say Intractable

David Porter
Special Advisor
Digital Shadows
@digitalshadows

#RSAC

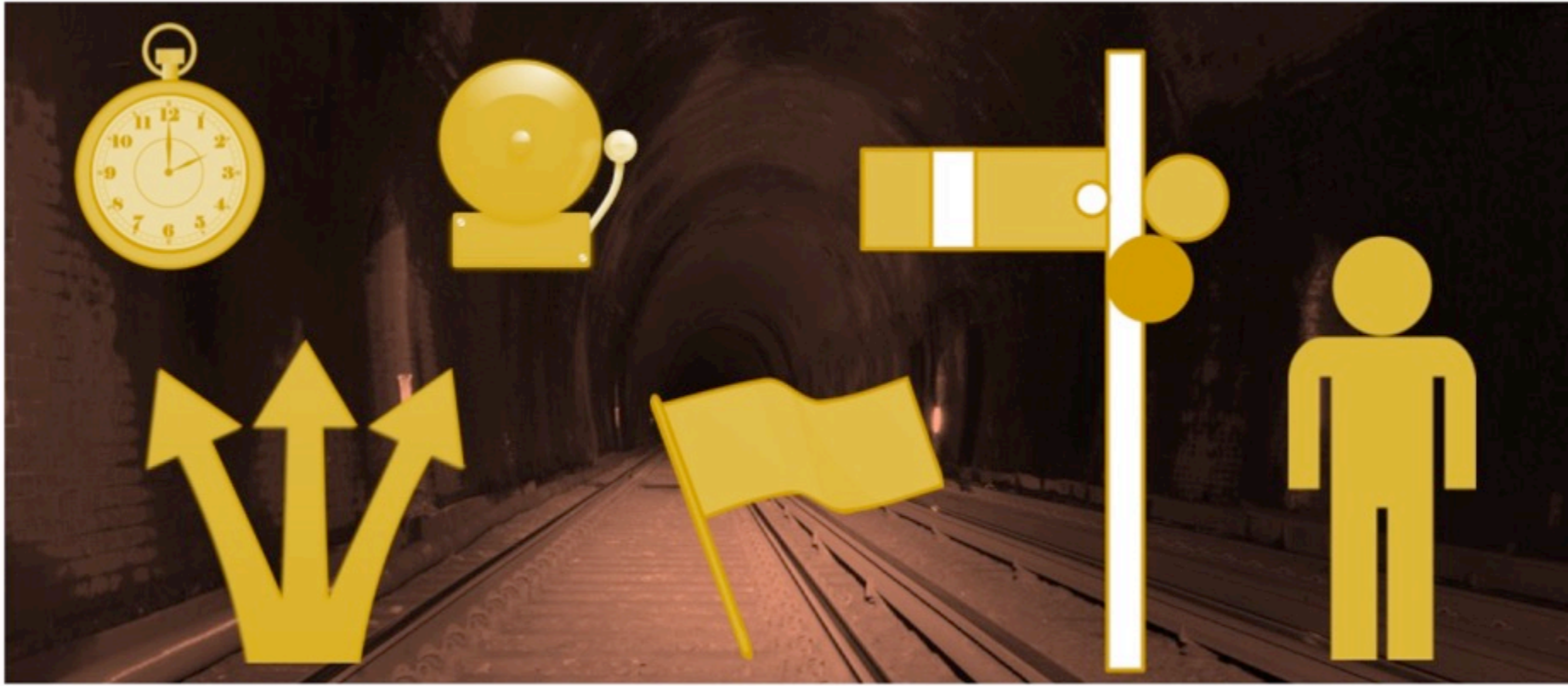
What's coming up

Threats seem to come from nowhere

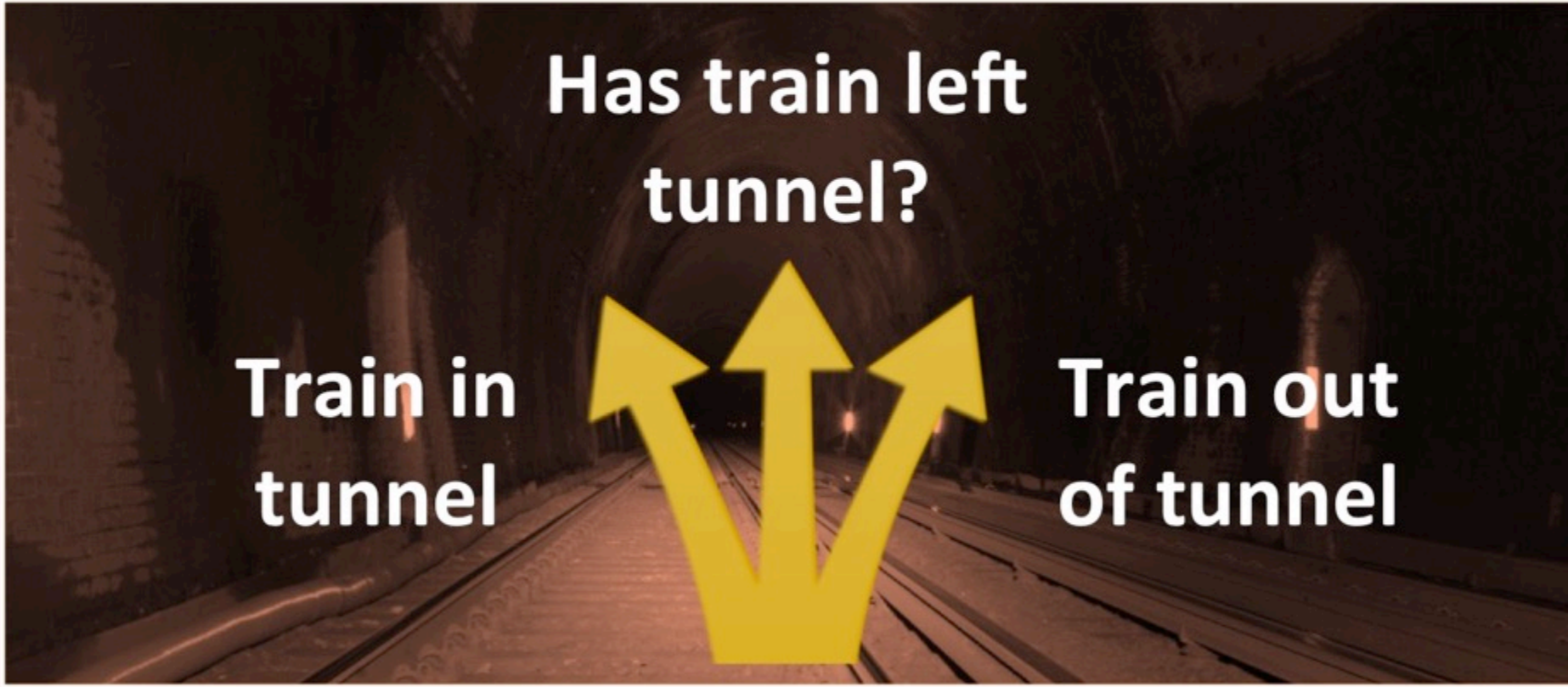
Victorian England, 1841

Clayton Tunnel: a high risk environment

Preventative safety measures employed

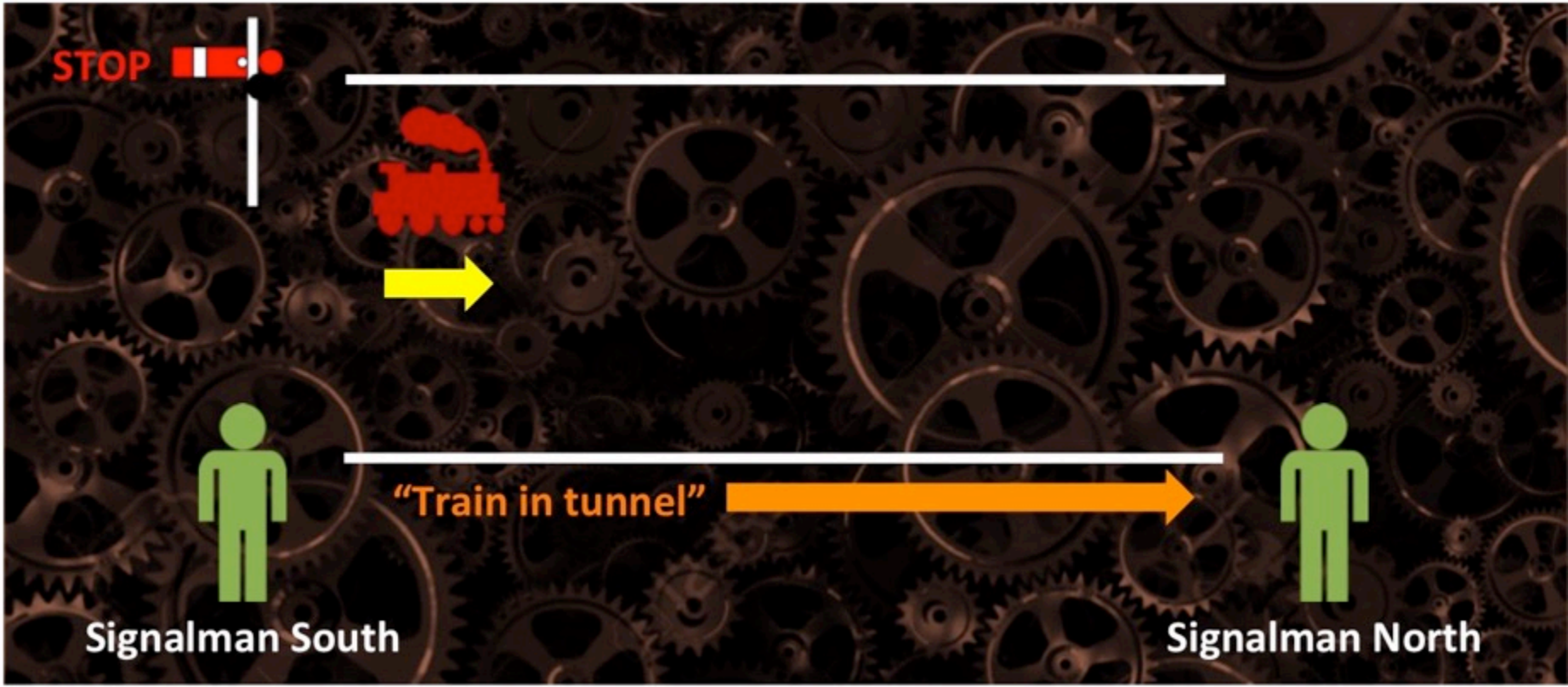


State-of-the-art telegraph technology

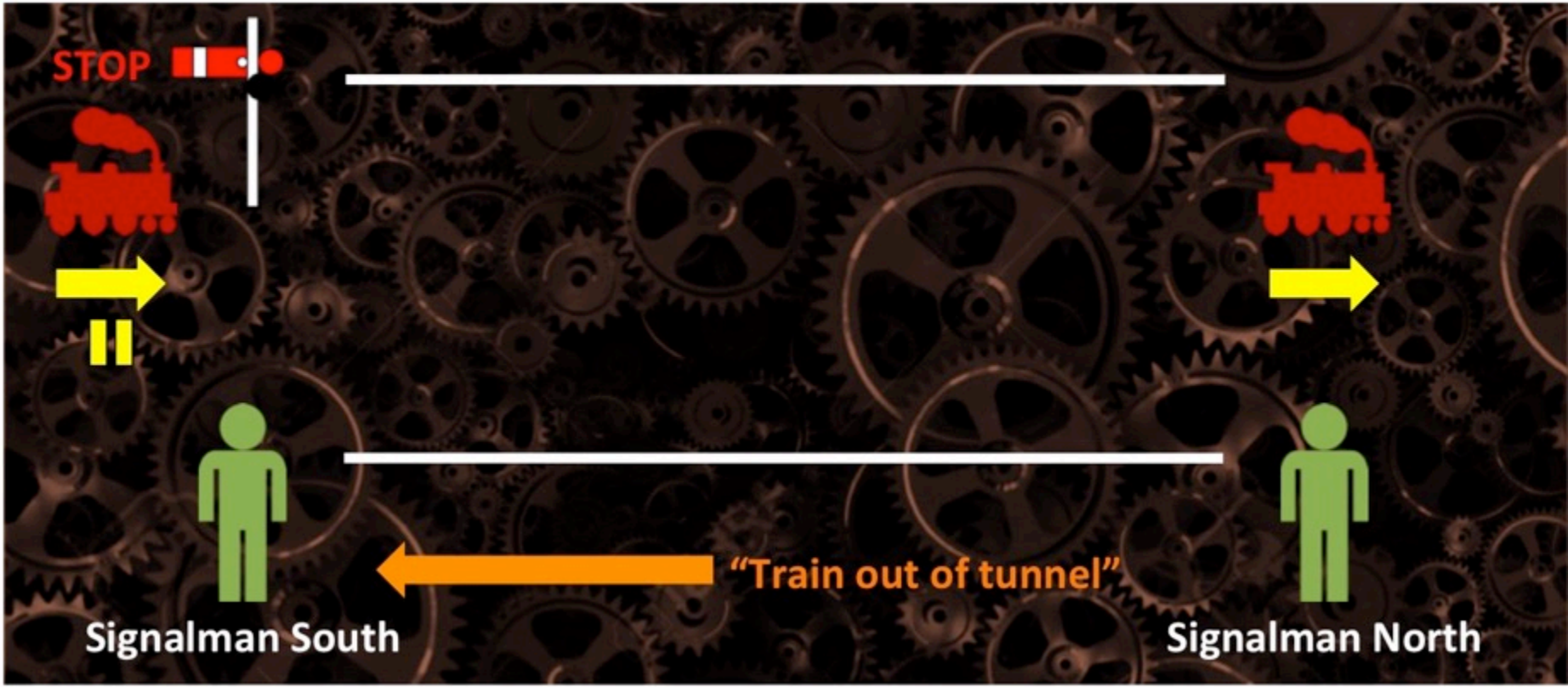


Safety system as imagined

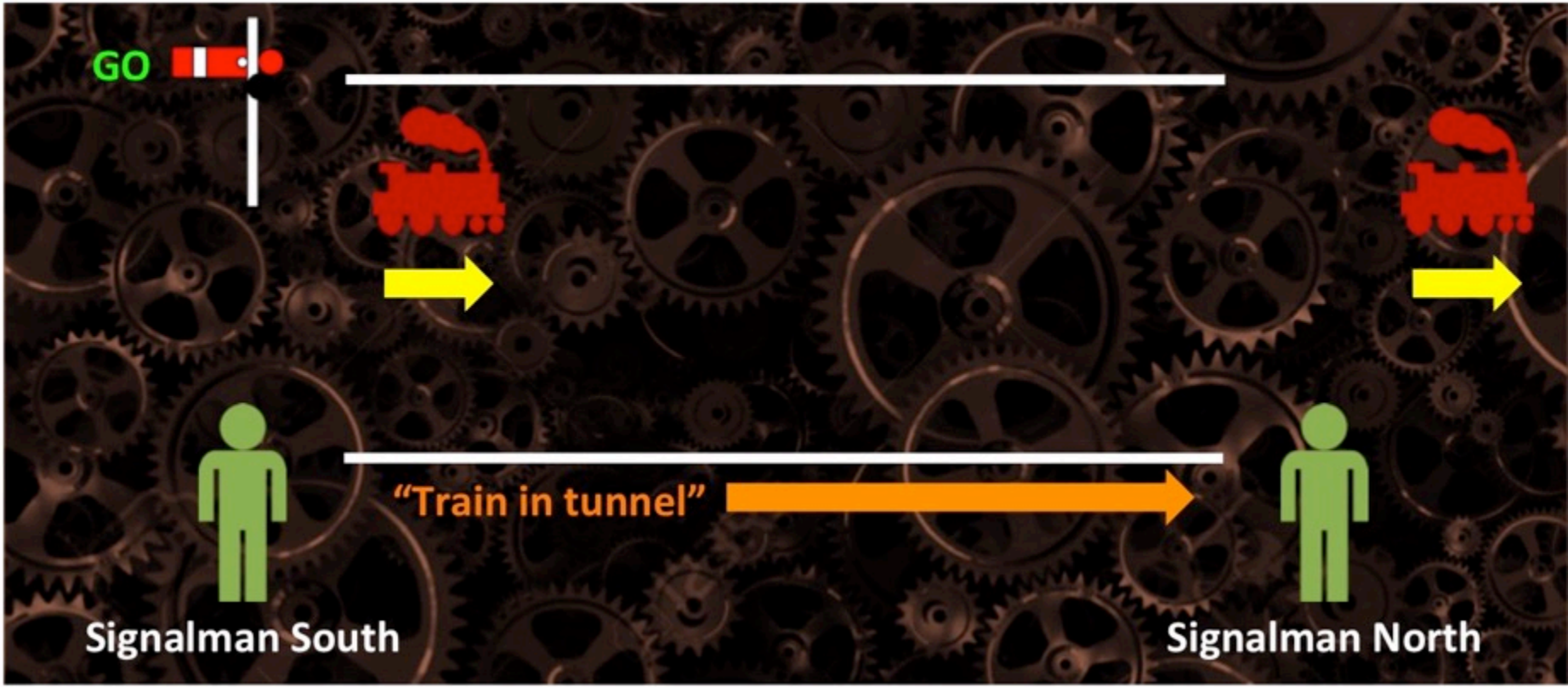
Safety system as imagined



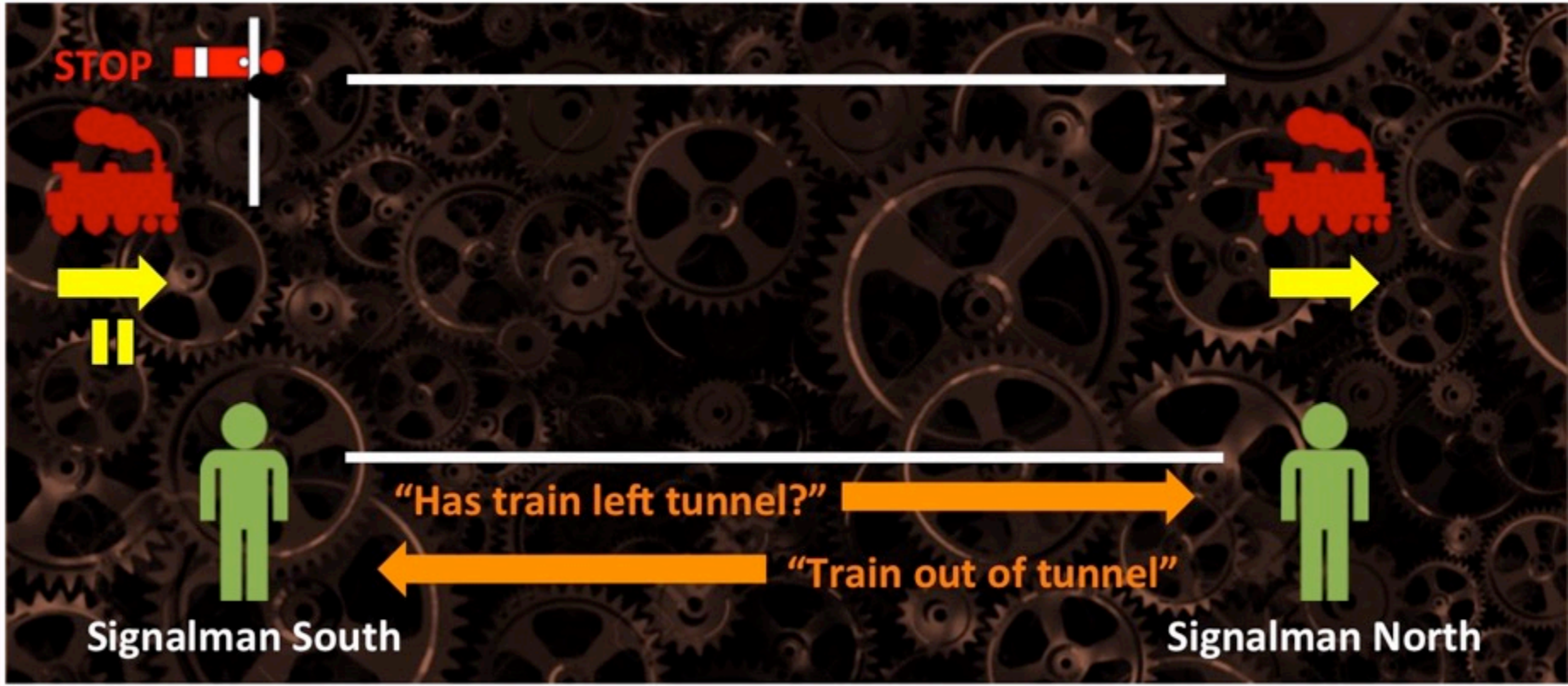
Safety system as imagined



Safety system as imagined



Safety system as imagined



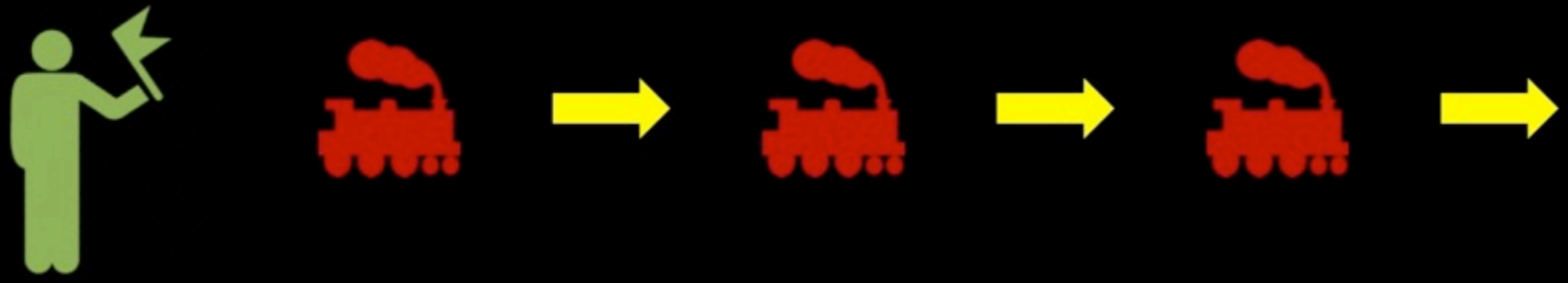
What could be safer?

Multiple protective layers
Redundant components
Well-defined protocols
State-of-the-art technology
Manual backup

One Sunday morning

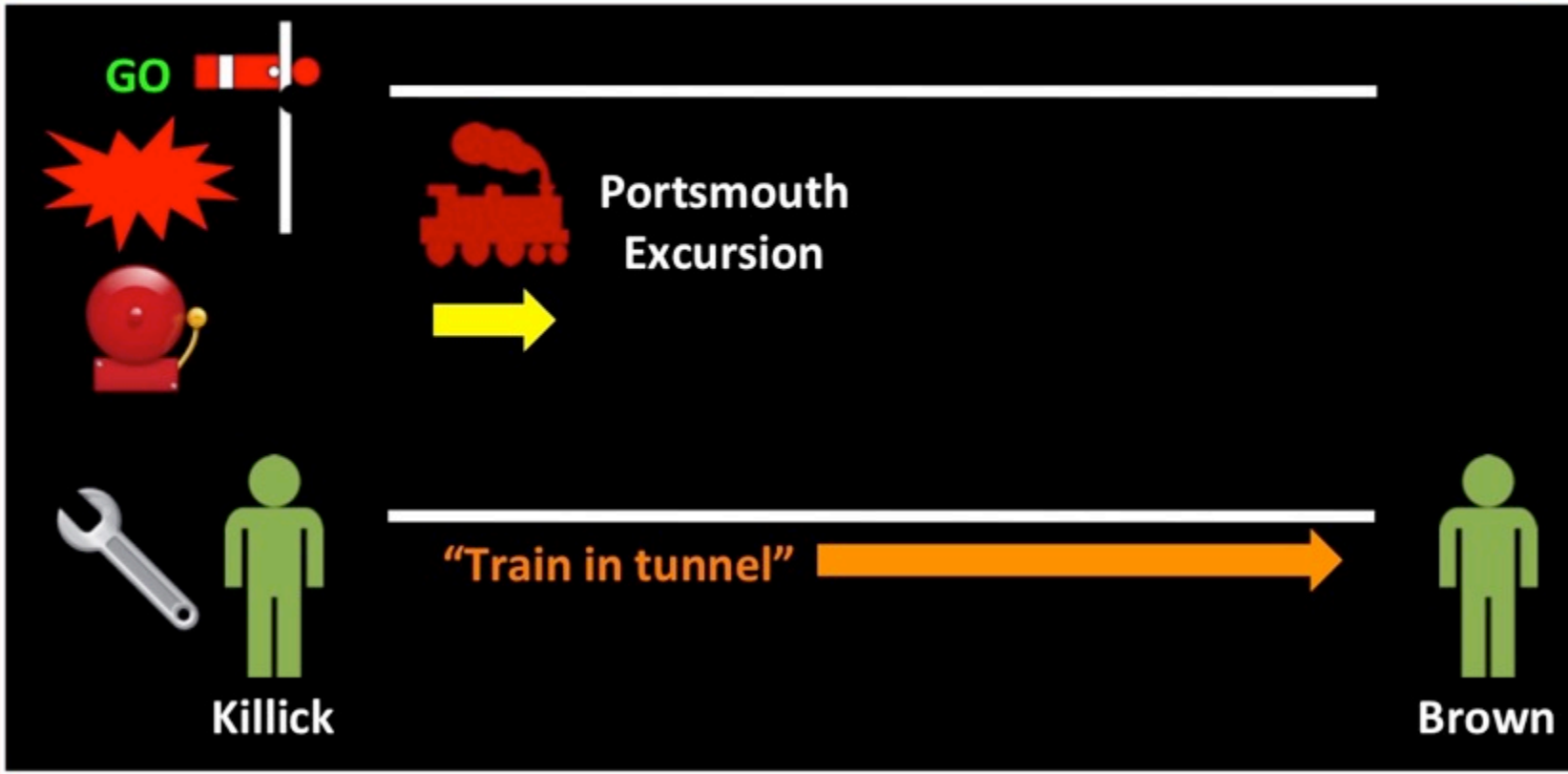
25 August 1861
08:28 GMT

25 August 1861

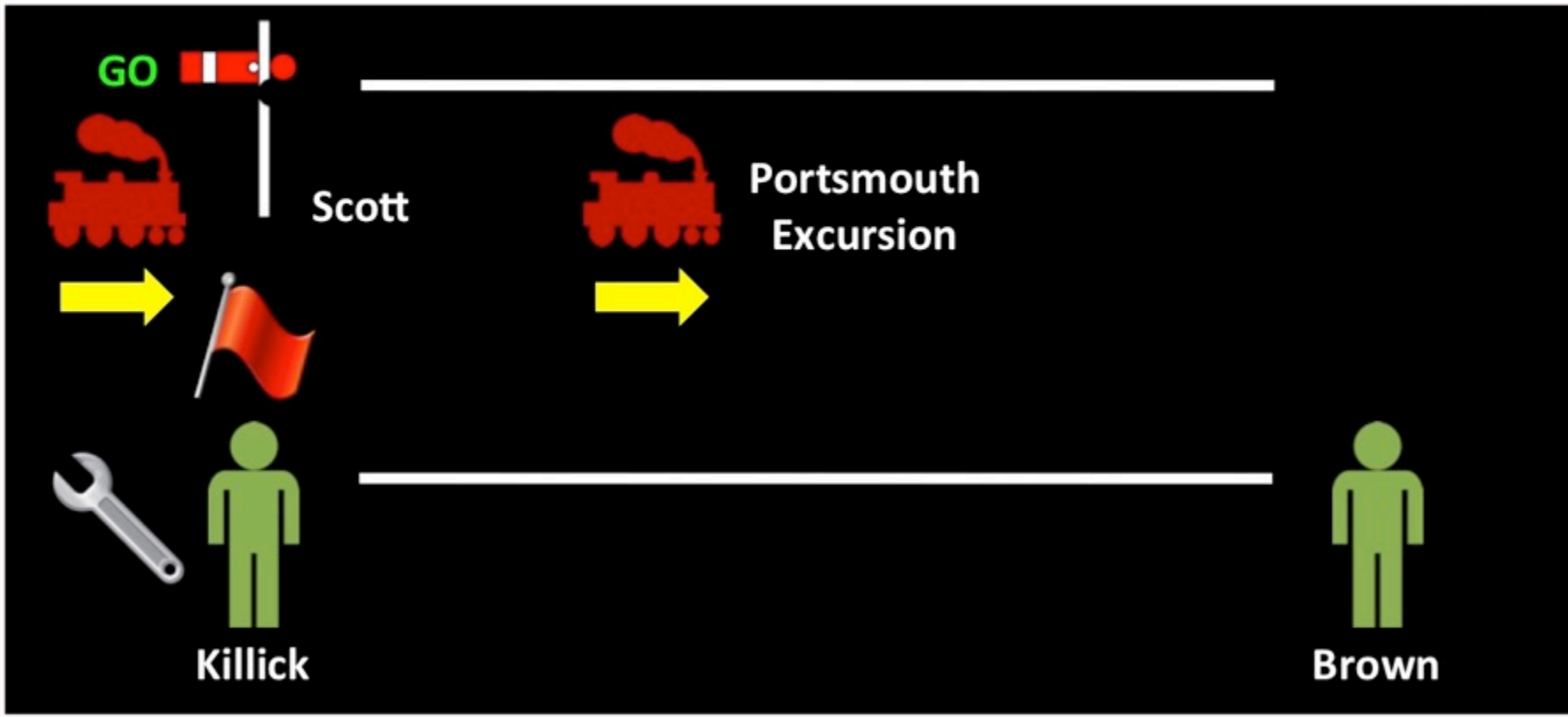


25 August 1861

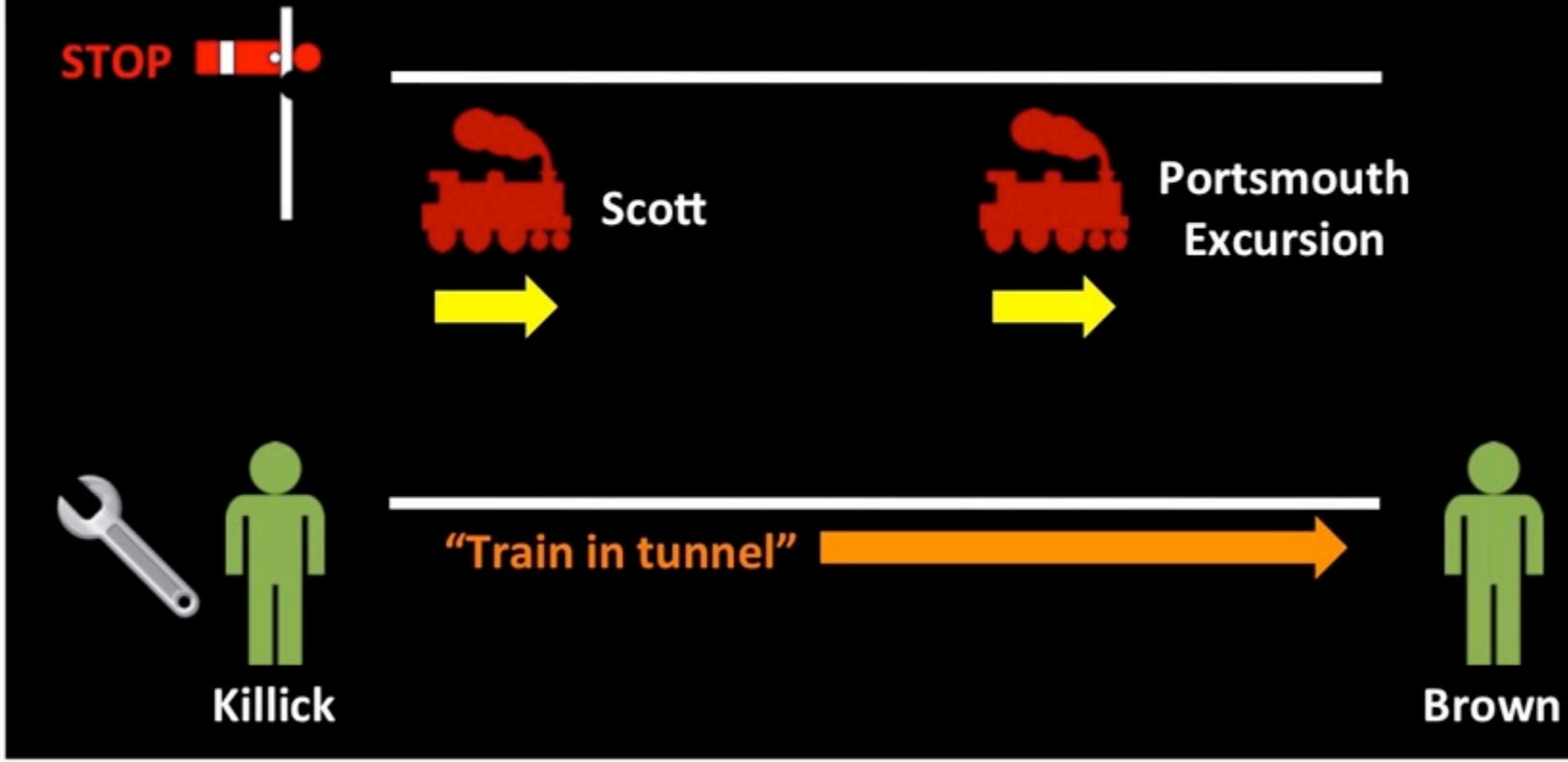
25 August 1861



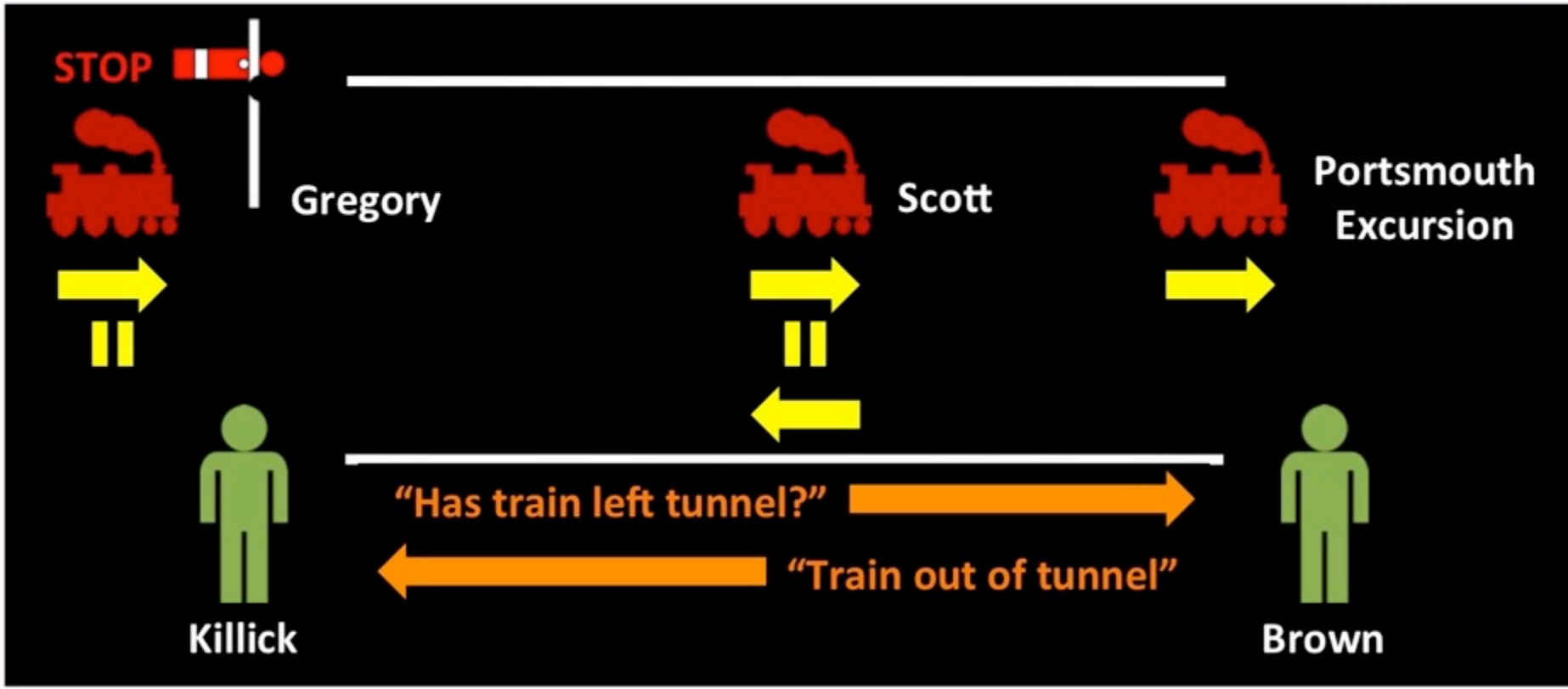
25 August 1861



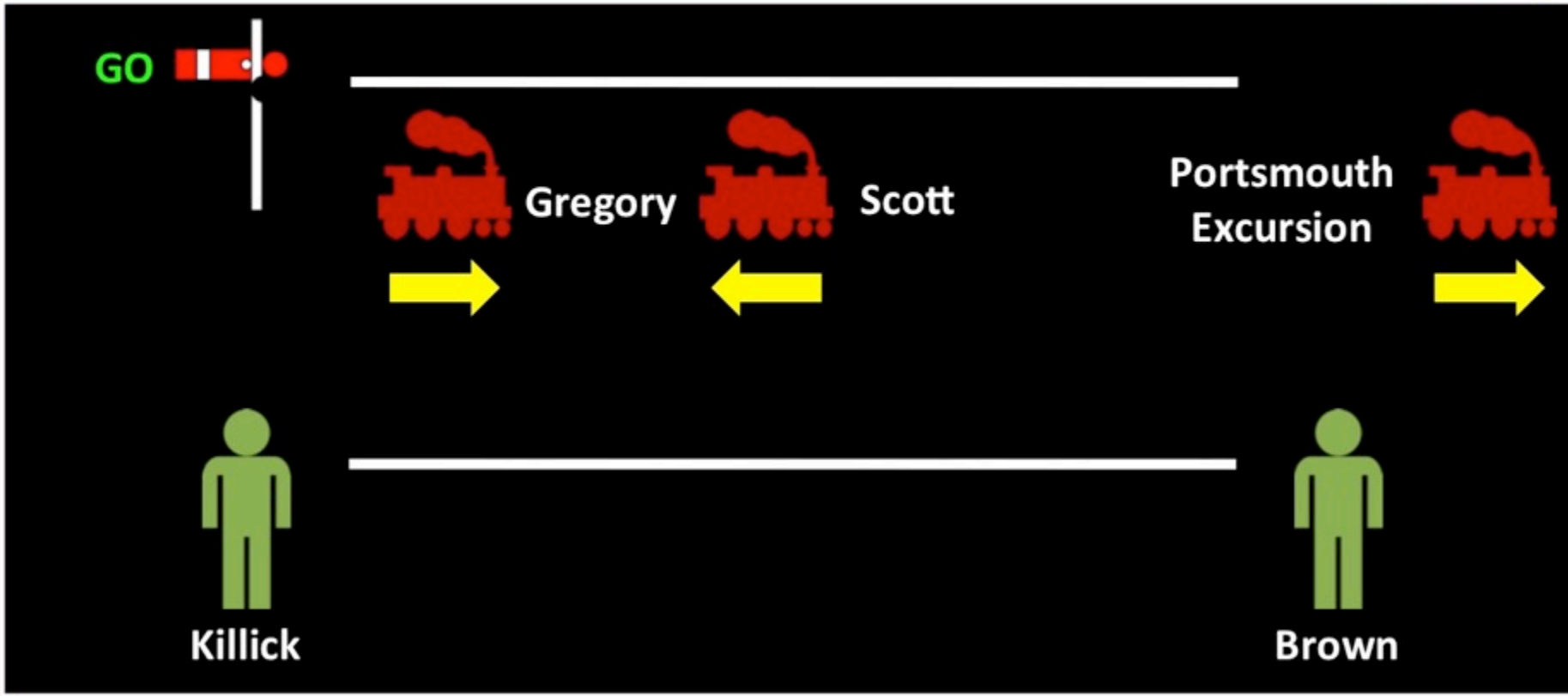
25 August 1861



25 August 1861

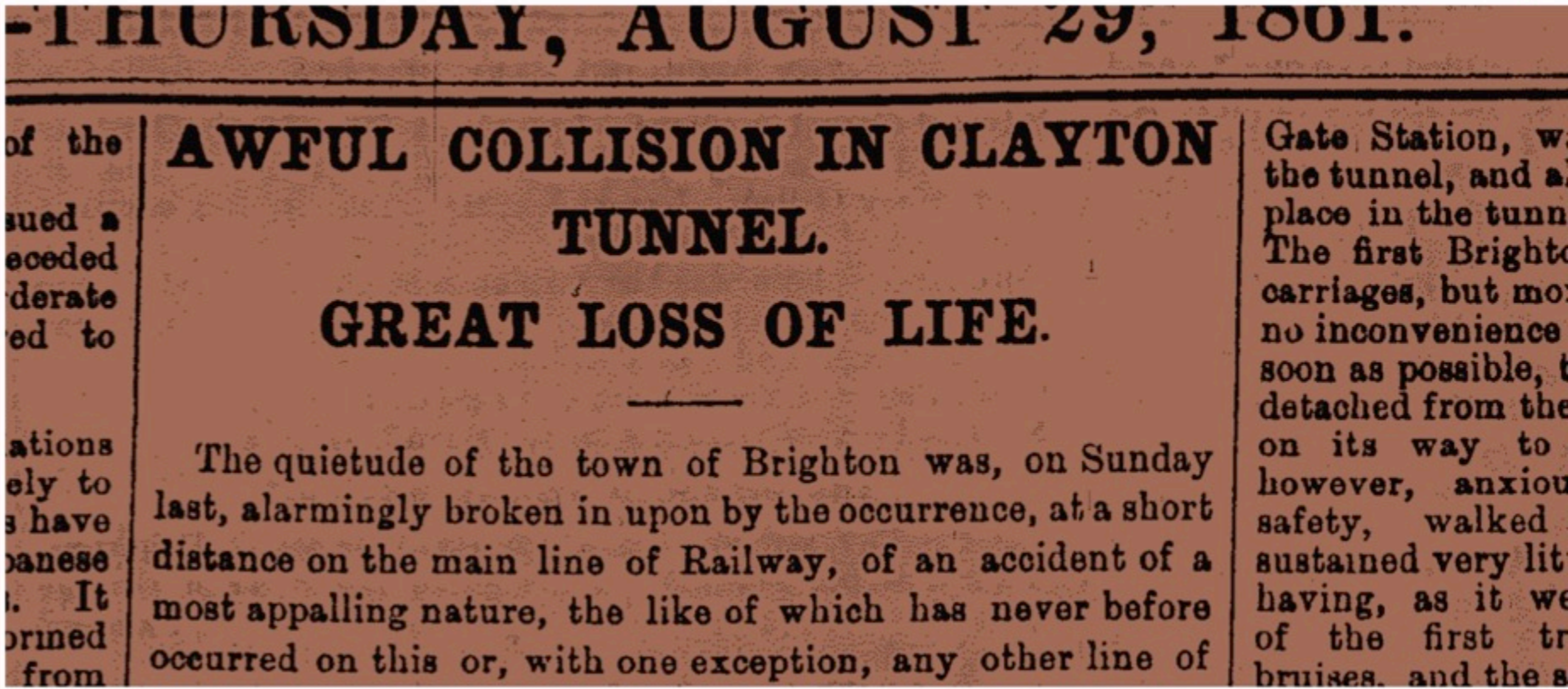


25 August 1861



25 August 1861

Despair and controversy



-THURSDAY, AUGUST 29, 1861.

of the
sued a
eceded
derate
ed to
ations
ely to
s have
panese
. It
rmed
from

AWFUL COLLISION IN CLAYTON TUNNEL.

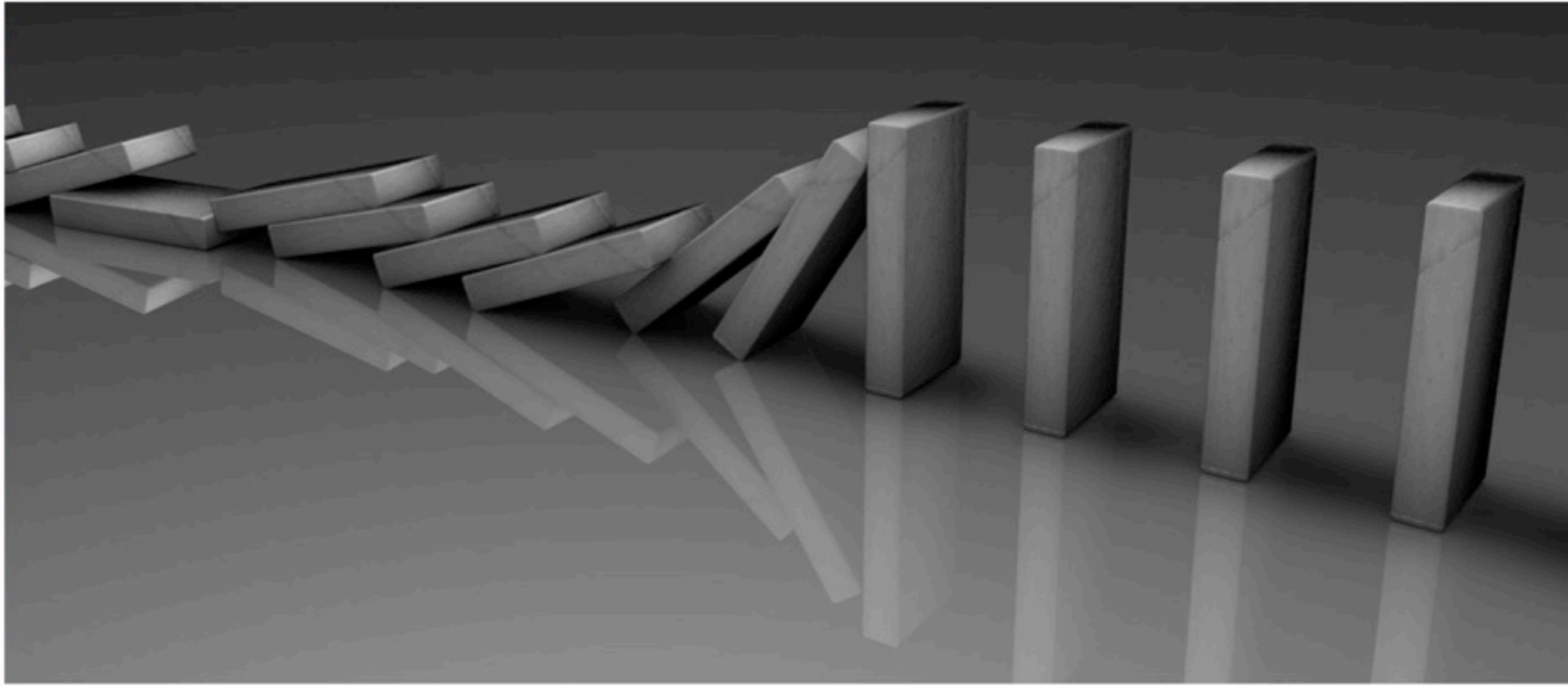
GREAT LOSS OF LIFE.

The quietude of the town of Brighton was, on Sunday last, alarmingly broken in upon by the occurrence, at a short distance on the main line of Railway, of an accident of a most appalling nature, the like of which has never before occurred on this or, with one exception, any other line of

Gate Station, w
the tunnel, and a
place in the tunn
The first Bright
carriages, but mo
no inconvenience
soon as possible, t
detached from the
on its way to
however, anxiou
safety, walked
sustained very lit
having, as it we
of the first tr
bruises, and the s

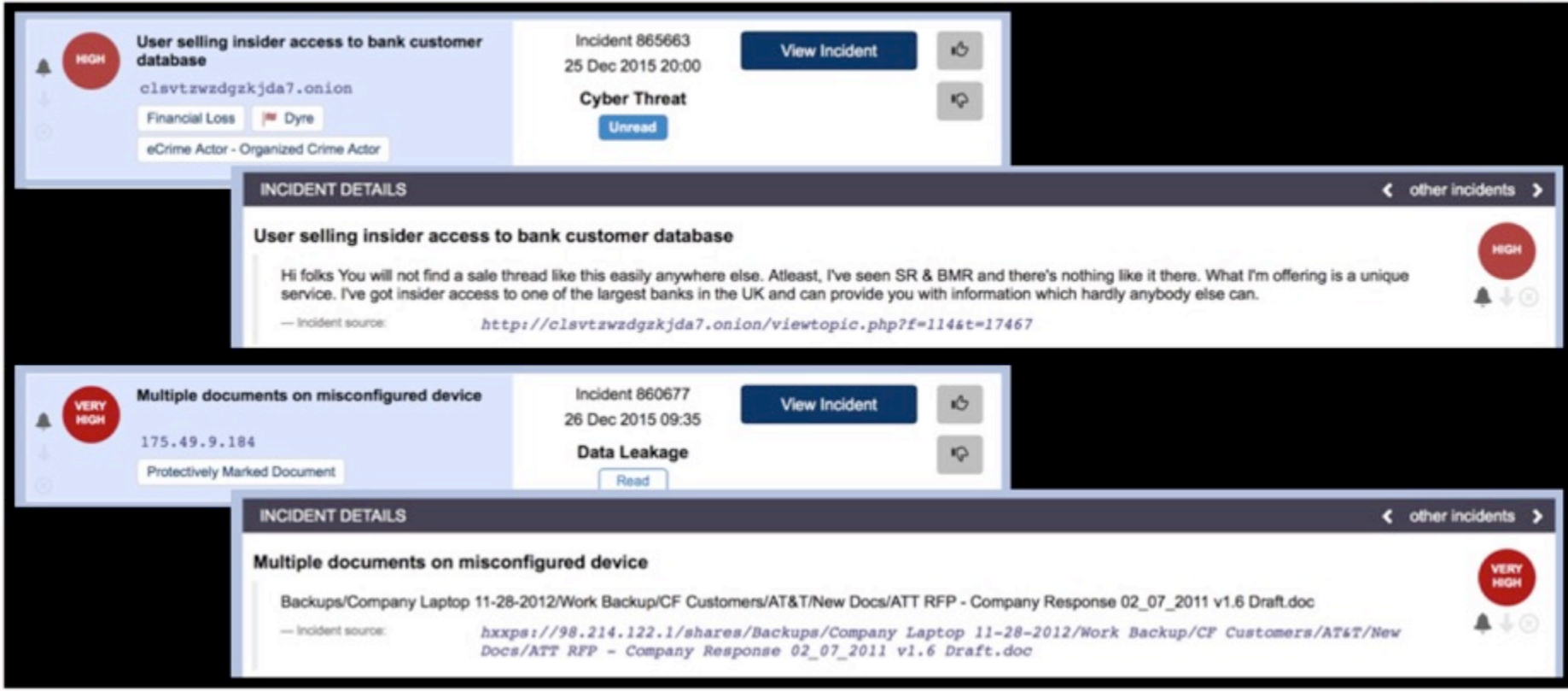
Who's to blame?

Finding the domino



Clinging to cause-effect tradition

155 years on: accidents in cyberspace



Prevention: a drunkard's search?

Security breaches study — UK

HM Government

2015 INFORMATION SECURITY BREACHES SURVEY

"50% of the worst breaches in the year were caused by inadvertent human error"

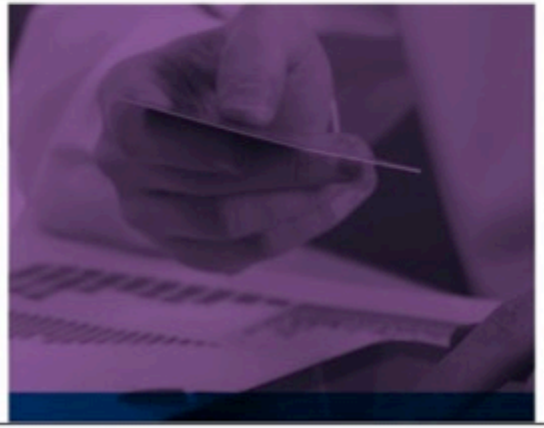
Source: *Information Security Breaches Survey 2015* HM Government

Security breaches study — US

RESEARCH REPORT

MARCH 2015

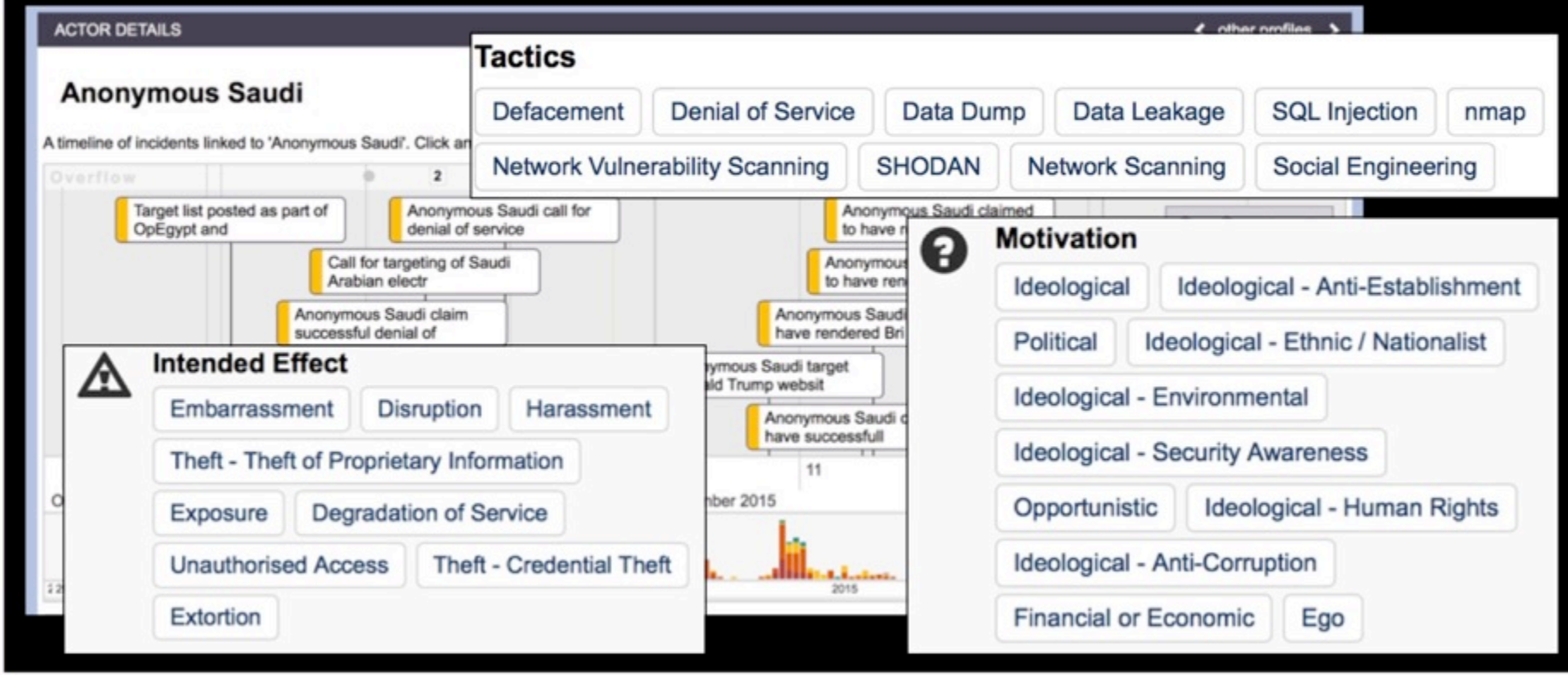
Trends in IT Security



"Human error accounts for 52% of the root cause of security breaches"

Source: *Trends in IT Security 2015*
CompTIA

Strong understanding of cyber criminality



Weak understanding of cyber accidents

"Human error"

"Glitch"

"Flub"

"General carelessness"

"Gaffe"

"Trips and spills"

"Omission"

"Misuse"

Out of scope: “error” of being deceived

People as unreliable system components

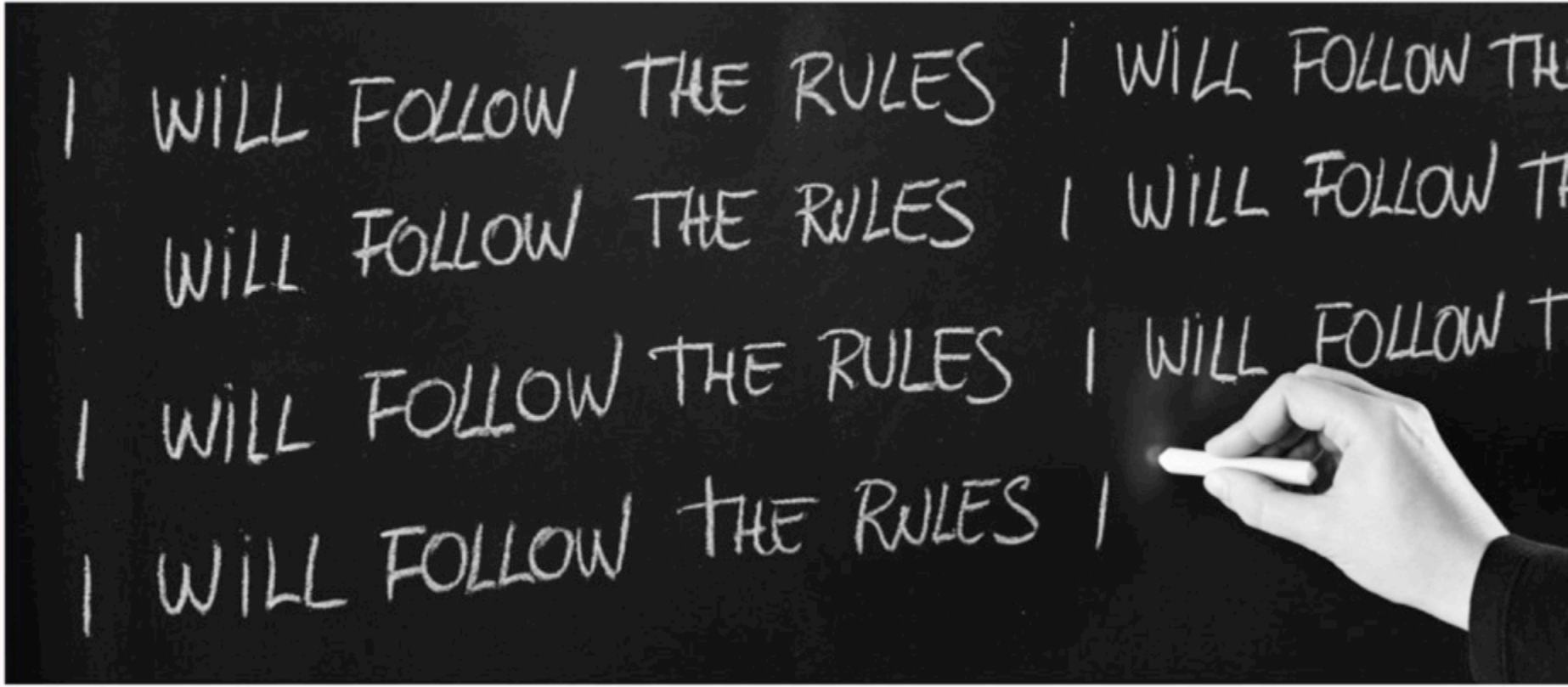
"It will be the untrained, uneducated, and just plain dumb users who put companies at risk"

"The biggest security threat will be people if they do not adhere to security policy and practice"

"The biggest security threat is the endpoint: you can't patch users"

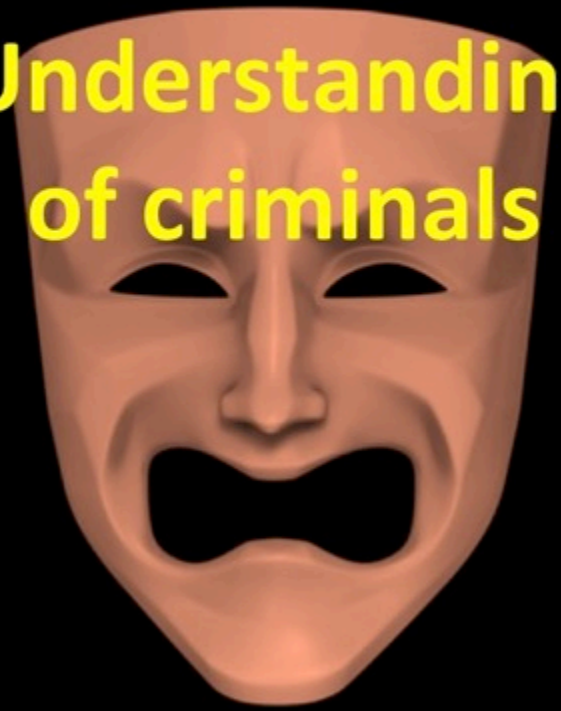
Source: *What will be the single biggest security threat of 2016?* IDG Connect 2016

Blame and train “the weakest link”



Time to redress the balance?

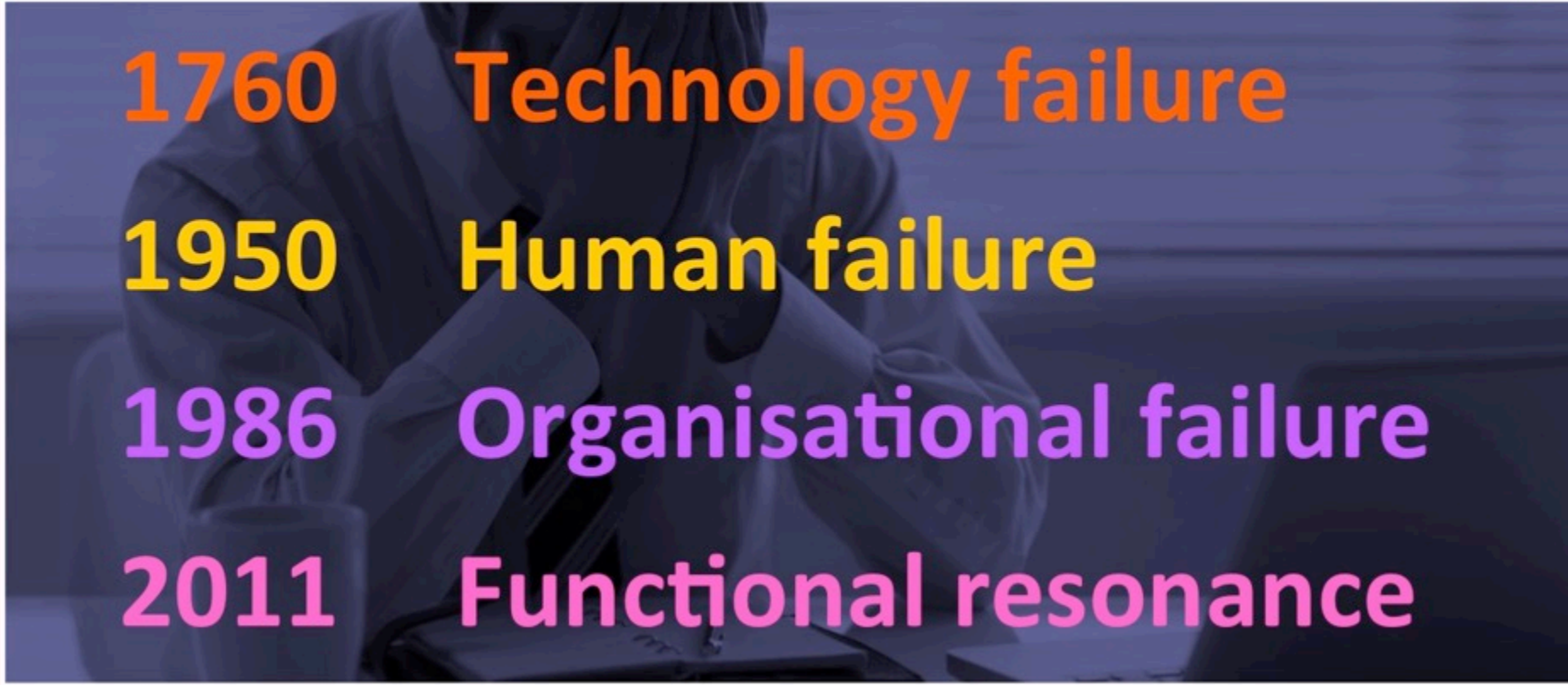
Understanding of criminals



Understanding of accidents

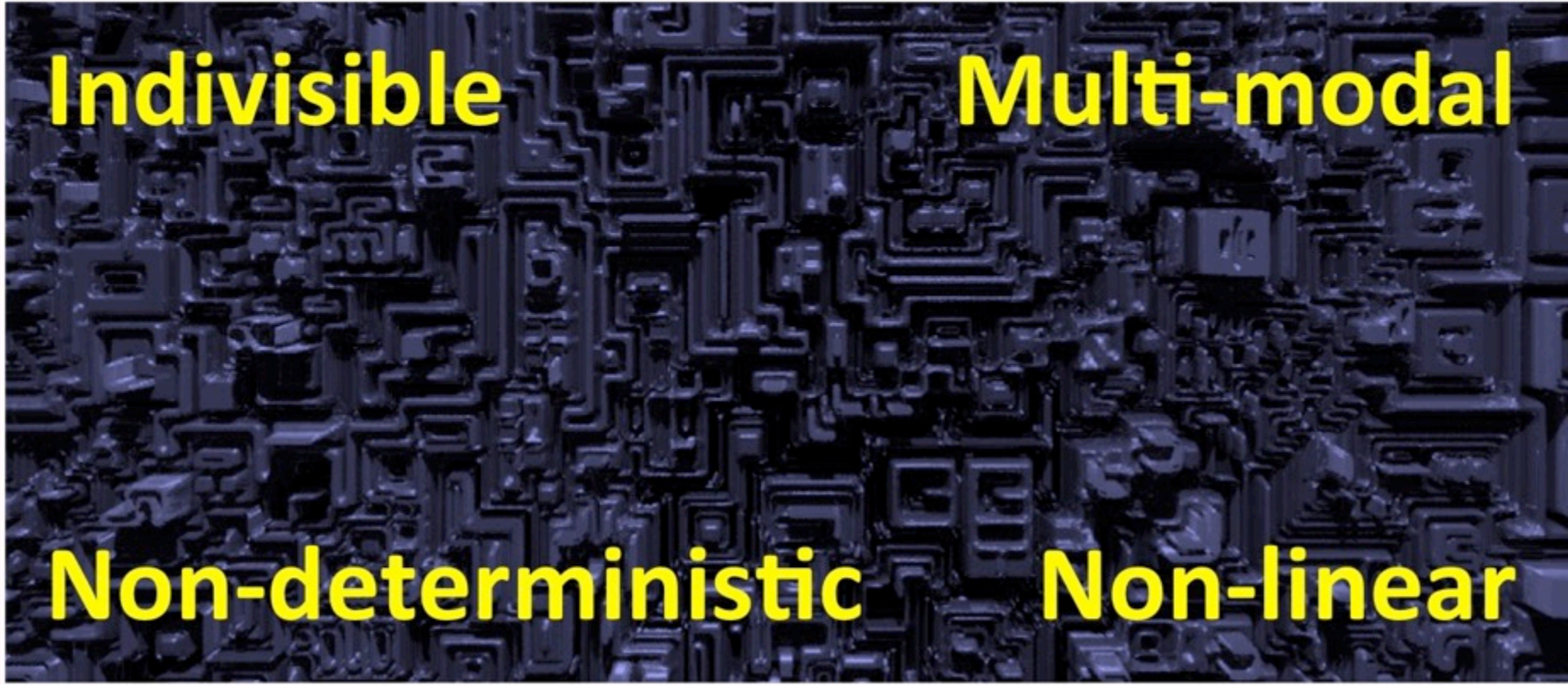
Resonance

Evolution of accident analysis



Socio-technical systems

Intractability



Tractable and intractable systems

“Find the domino” does not work

“We are too much accustomed to attribute to a single cause that which is the product of several, and the majority of our controversies come from that”

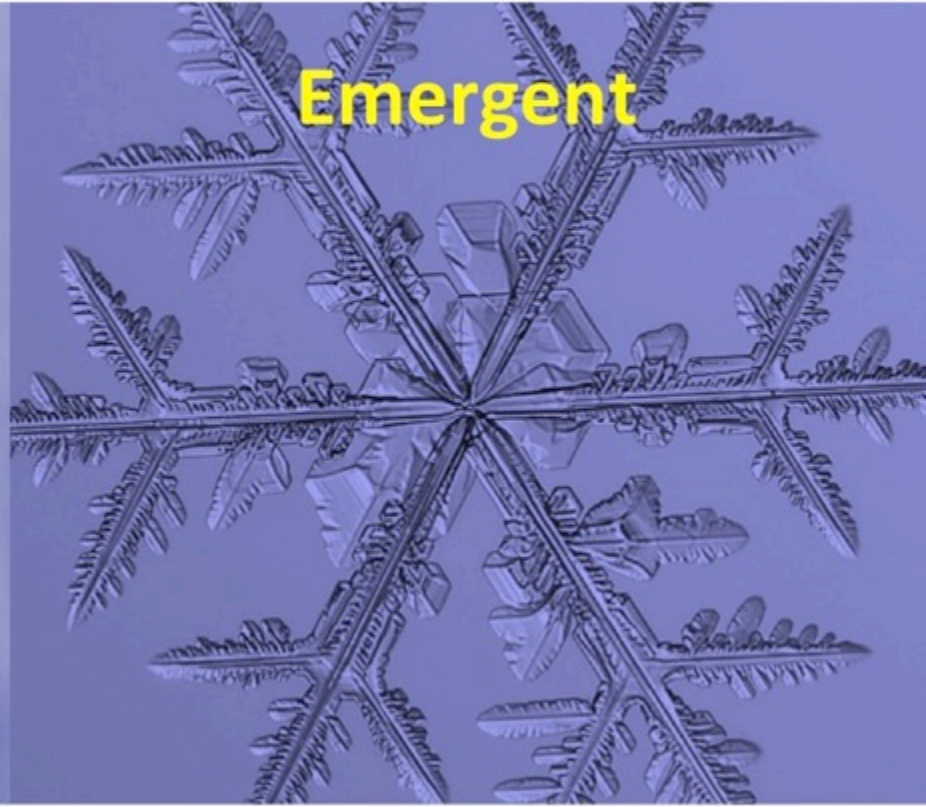
Marcus Aurelius, Roman Emperor, 161-180 AD

A new perspective

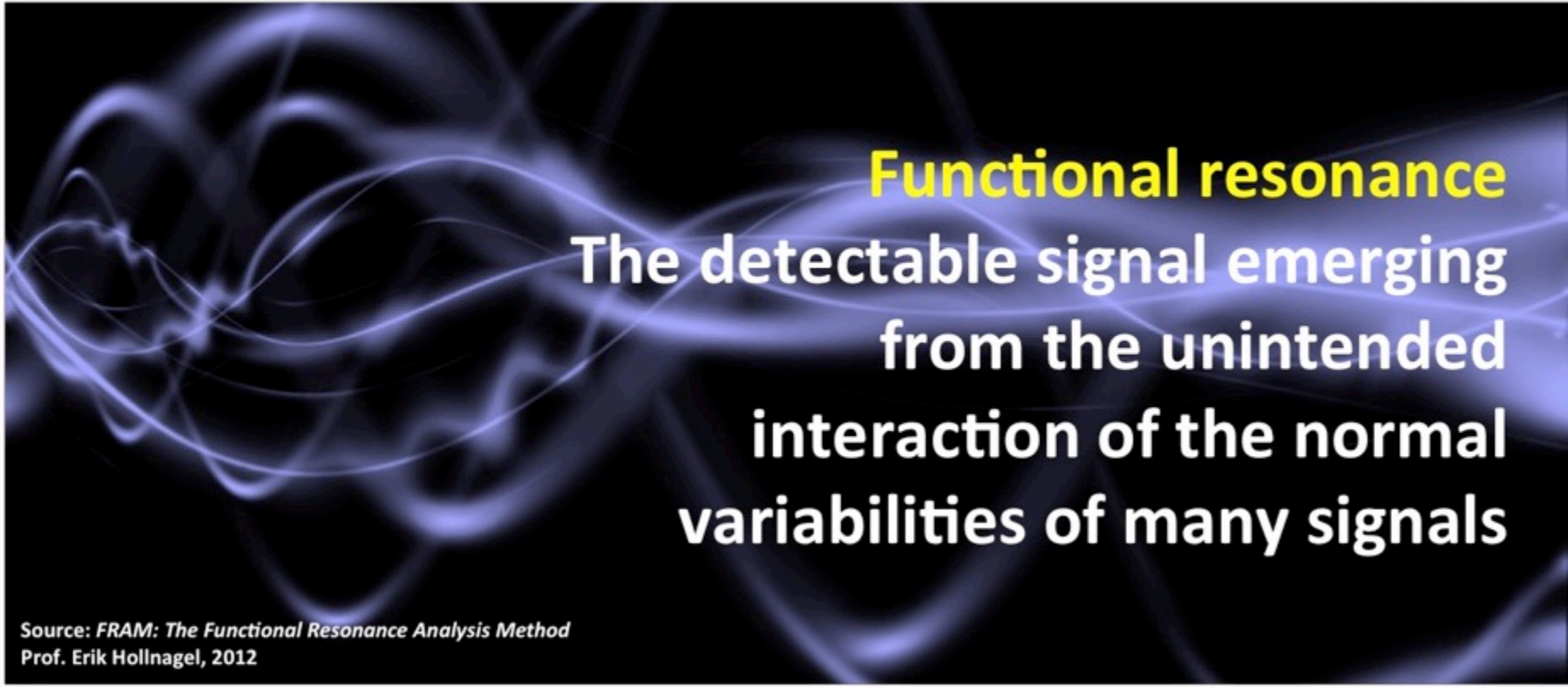
Successes and failures are equivalent

People make approximate adjustments

Bad and good outcomes are emergent



Variabilities can unintentionally resonate



Source: *FRAM: The Functional Resonance Analysis Method*
Prof. Erik Hollnagel, 2012

Modeling

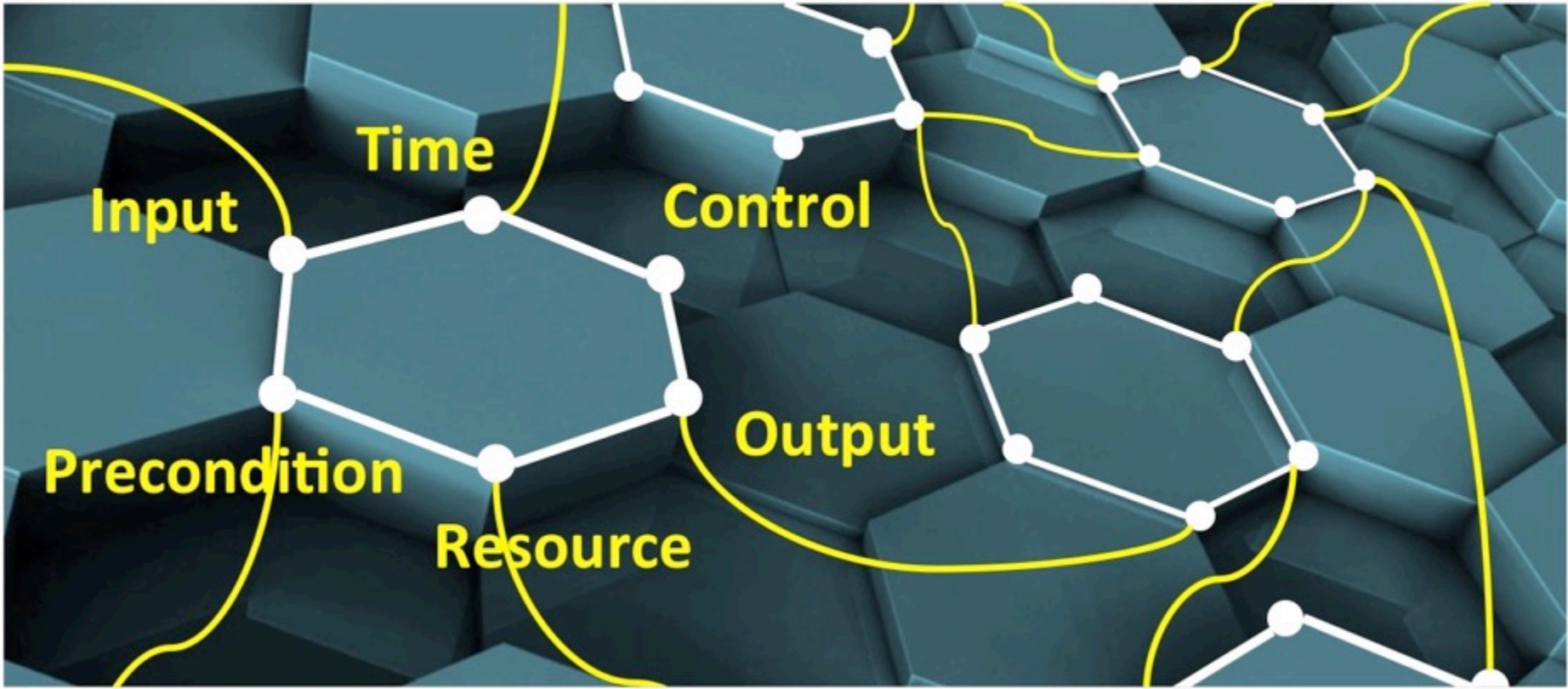
Time for a new approach

"When the interactions among factors become more important than the factors themselves then we need to revise our approach"

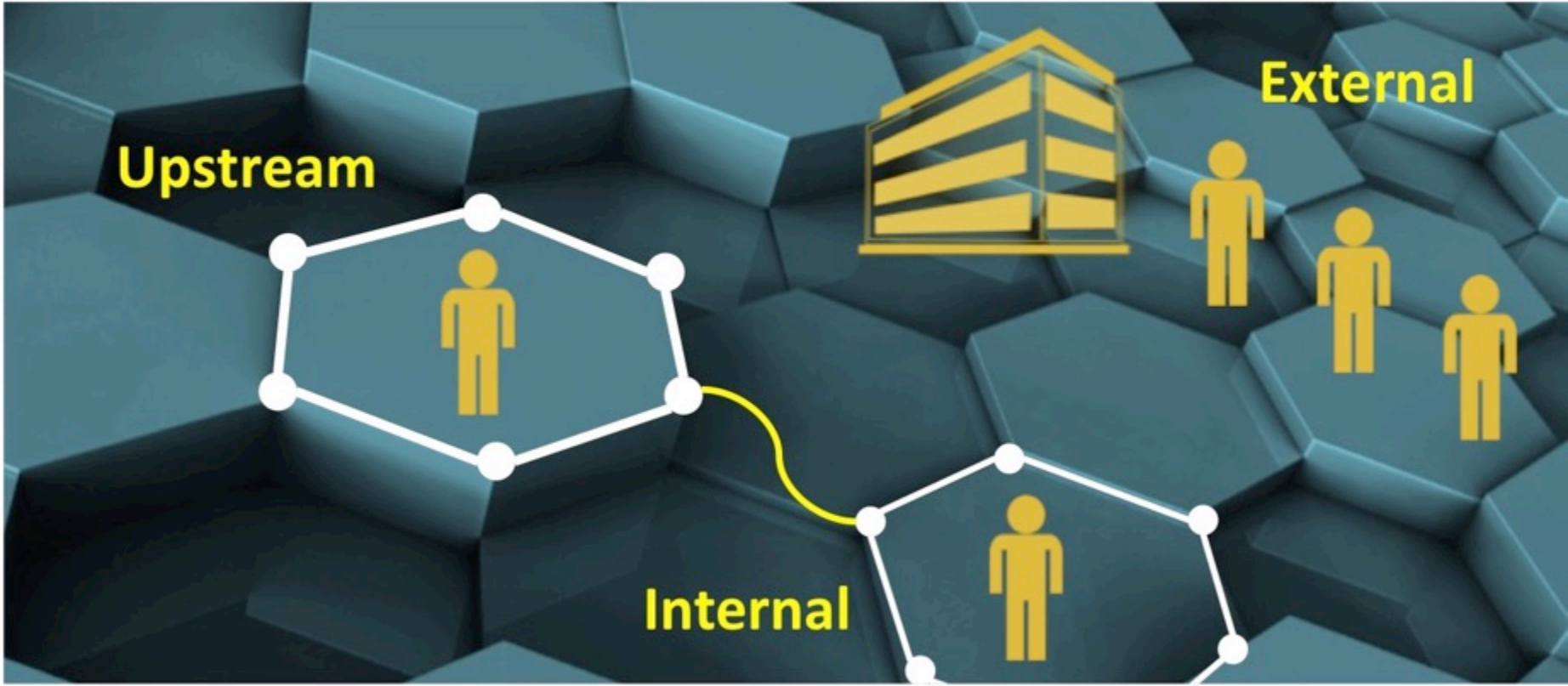
Prof. Erik Hollnagel

European Safety and Reliability Conference, 2011

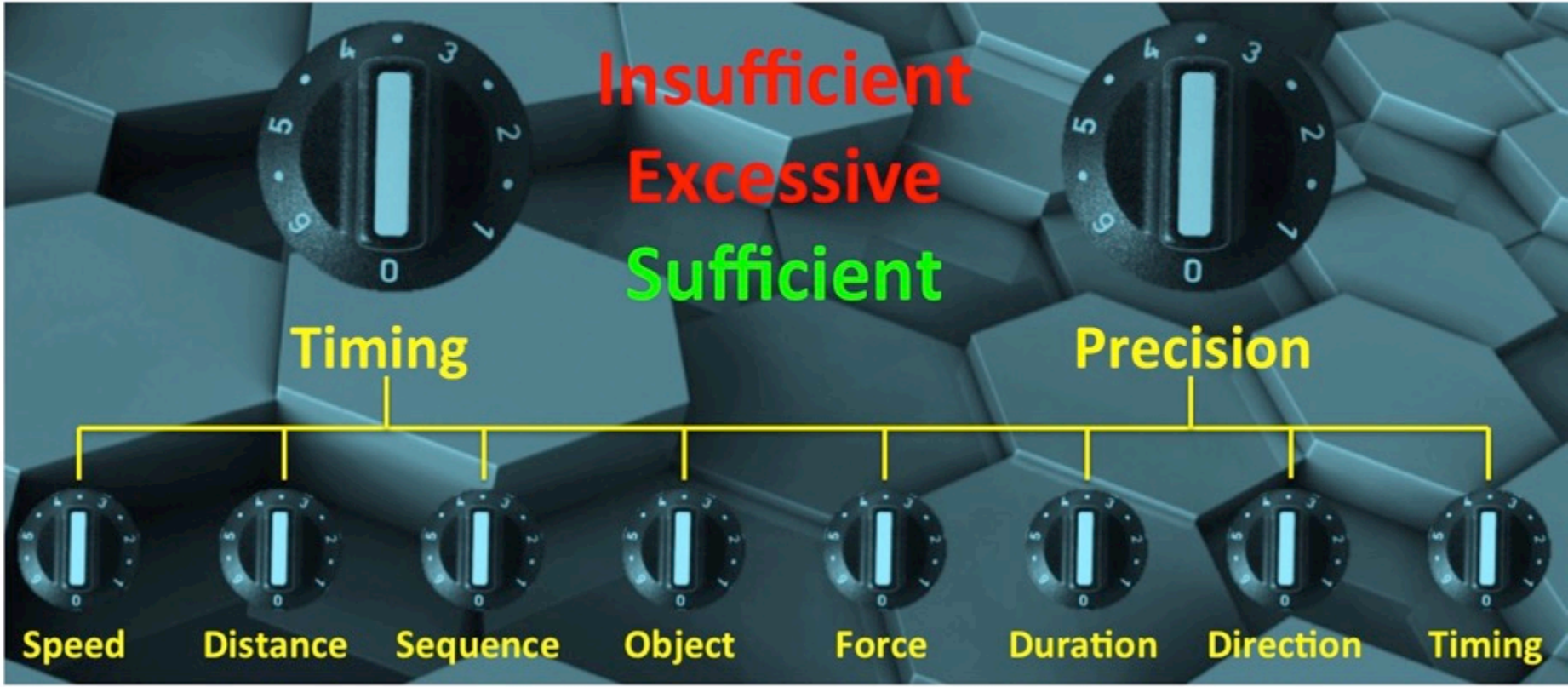
Focus on function not architecture



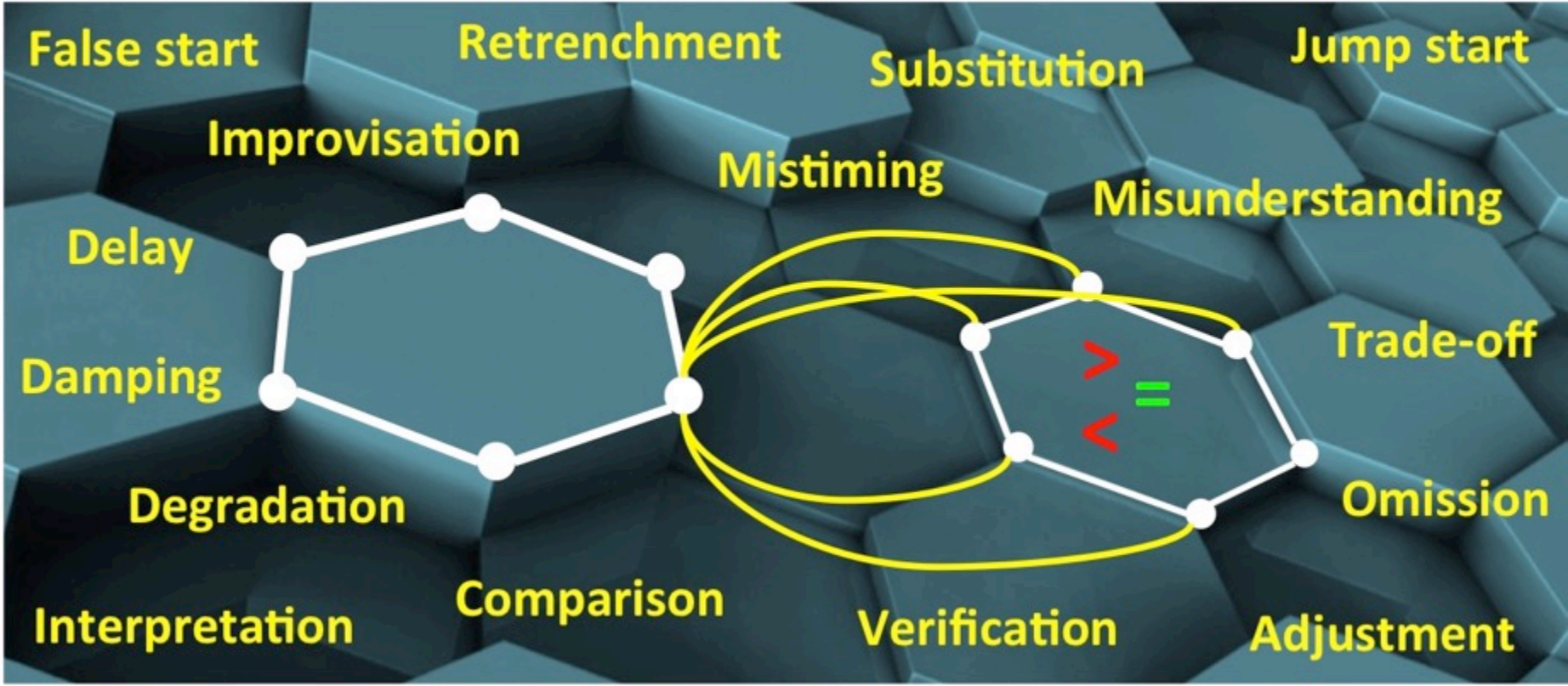
Understand sources of variability



Understand types of variability



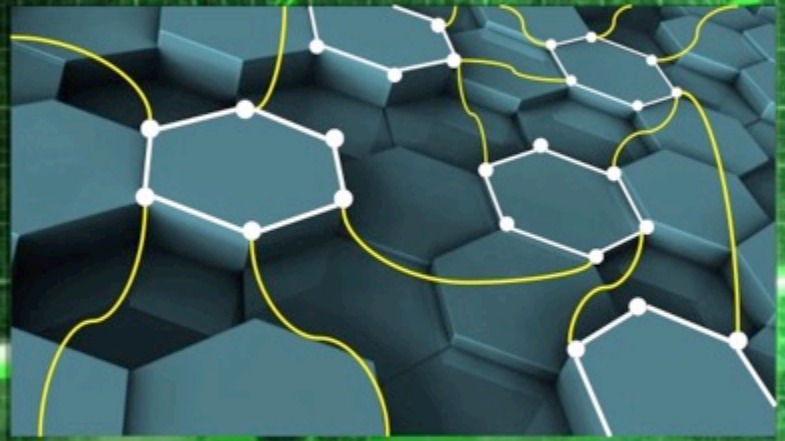
Identify potential functional resonance

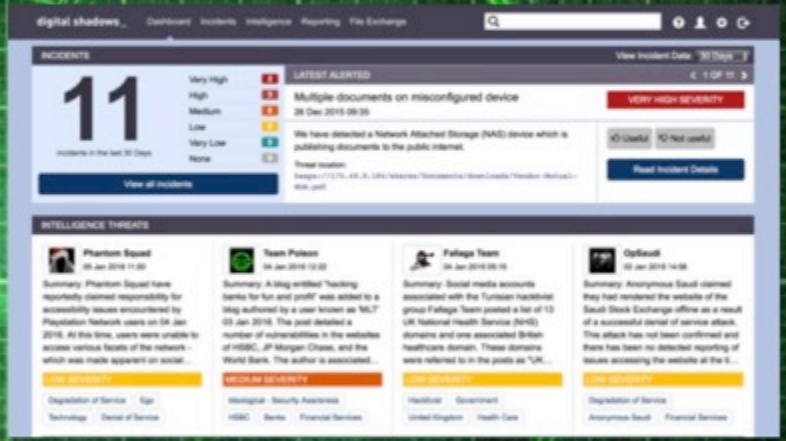


Monitor and influence variabilities

Insights

Situational awareness inside and beyond

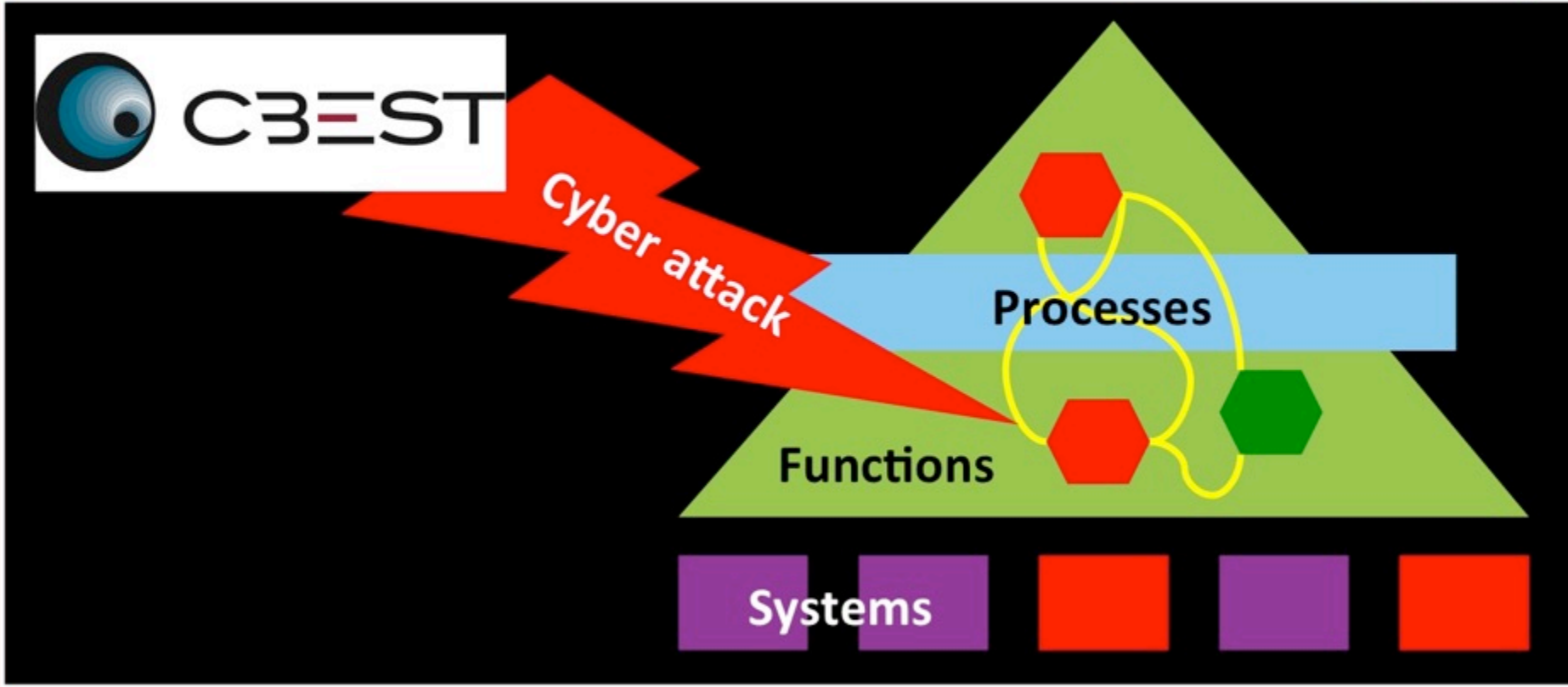




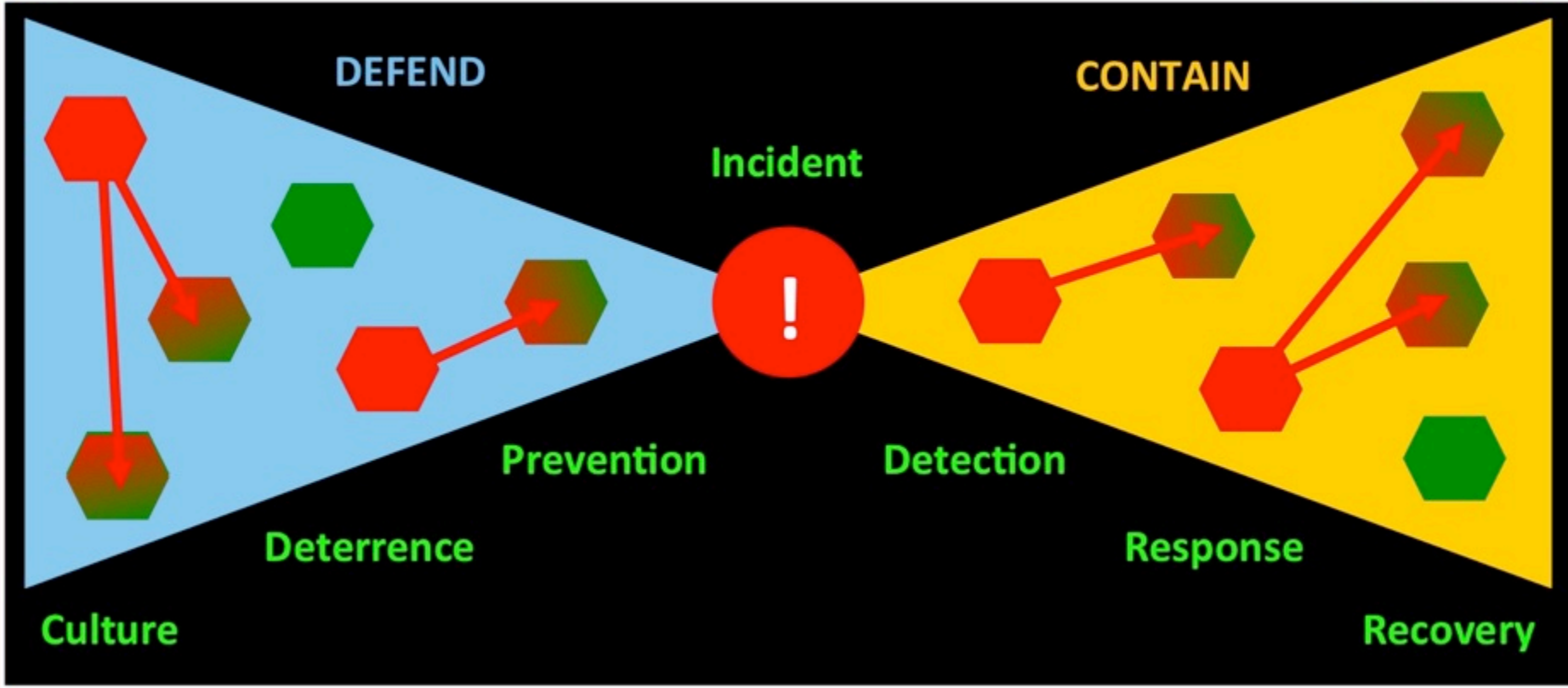
Internal accident

External criminal

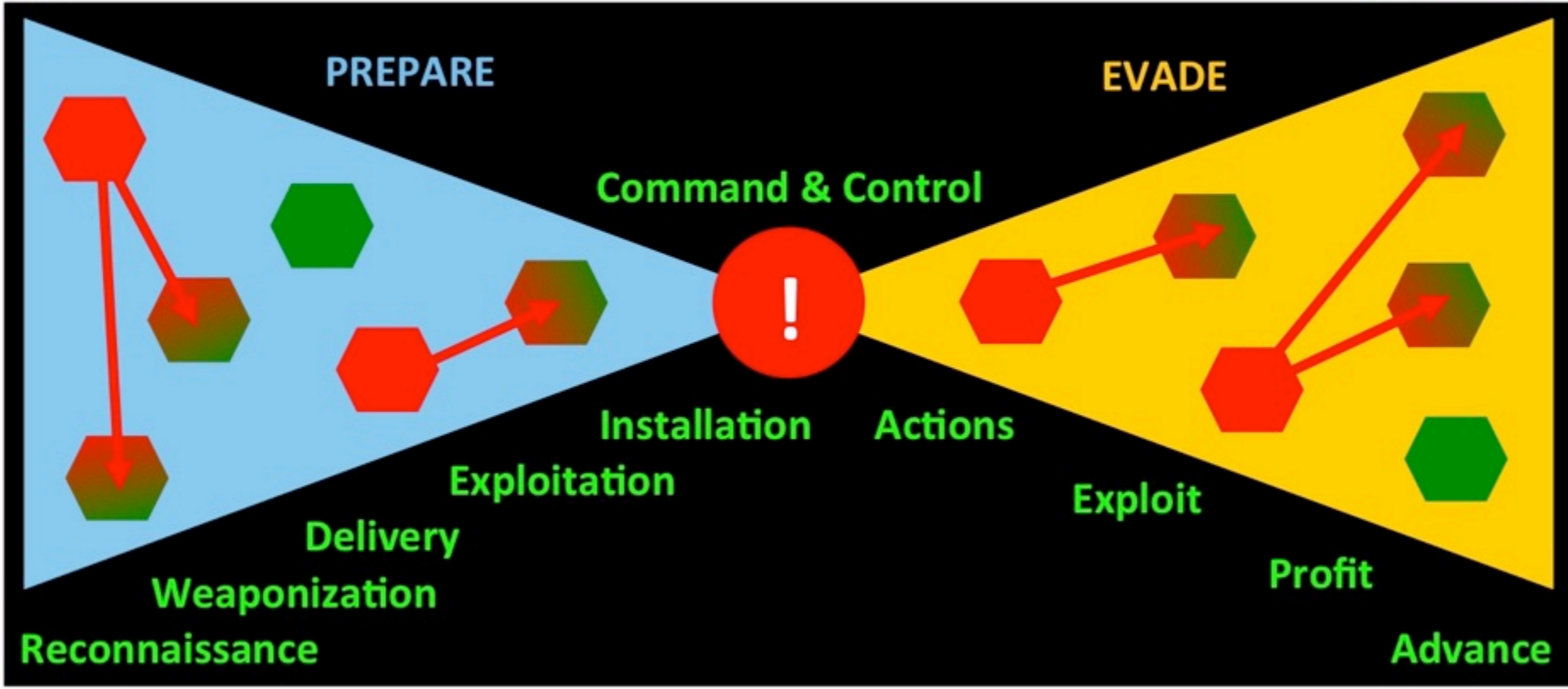
Facilitating intelligence-led testing



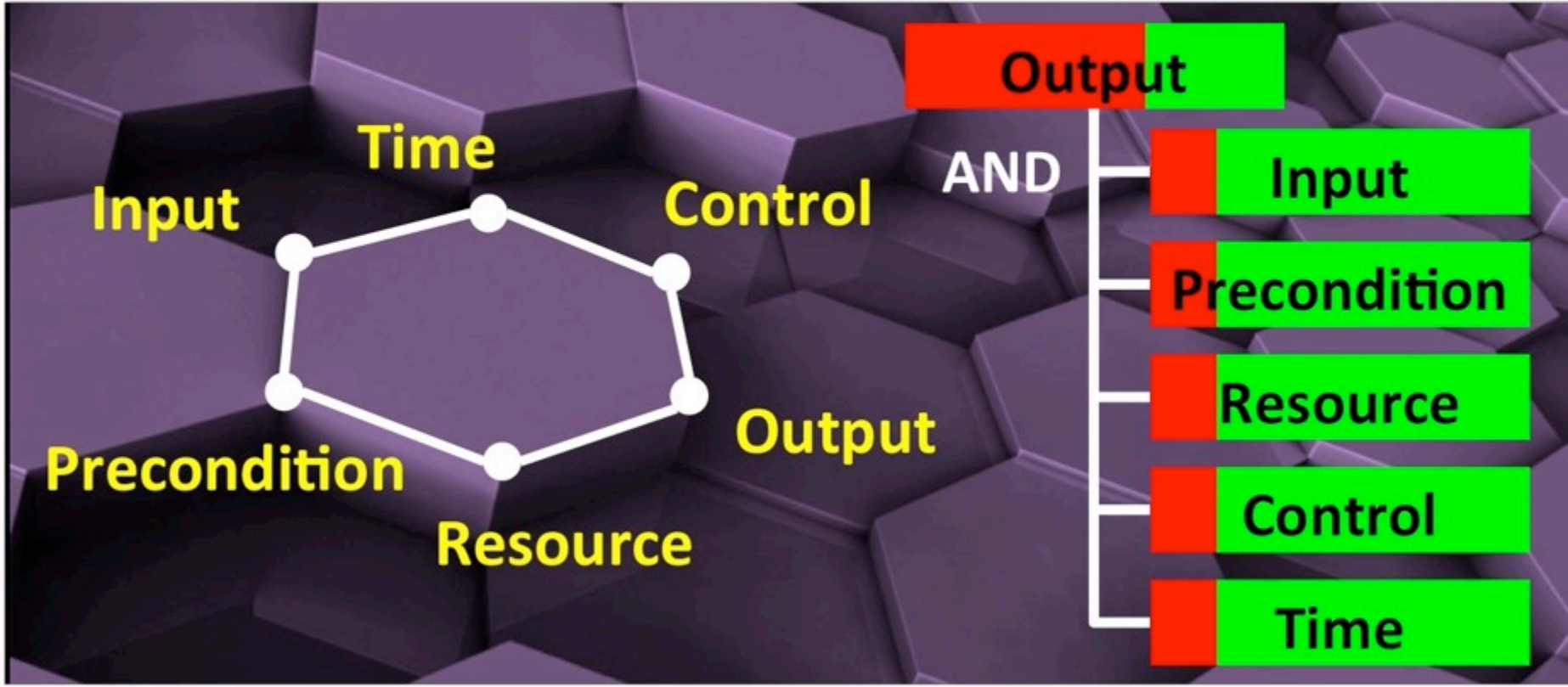
Testing our cyber defenses



Disrupting the kill chain



Quantification using Bayesian networks



Navigating the darkness of risk

Uncertainty

Situational awareness

A new perspective on risk

Risk

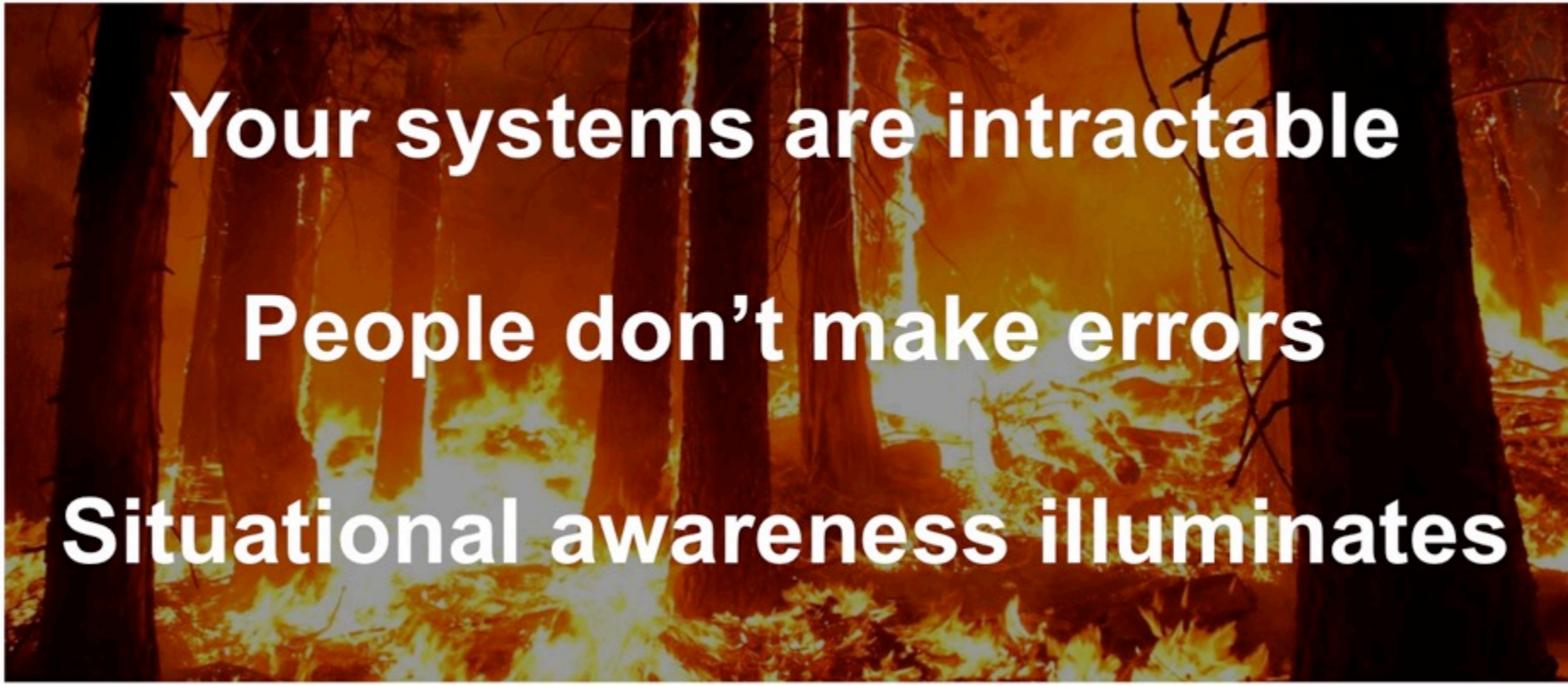
The degree to which the chances of achieving our goals are affected by things we cannot control, predict or understand

Source *Dependency modelling and understanding risks to the infrastructure*
Prof. John Gordon, 2011

Who's to blame?

Complex, non-linear, socio-technical

Key messages



Applying today's lessons

Re-evaluate and tune your external data leakage intelligence capability

Analyse historical intelligence detailing your criminal and accidental cyber security exposure

Identify critical business functions and manage potential performance variabilities

Thank you

digital shadows_