

# RSA Conference 2016

San Francisco | February 29–March 4 | Moscone Center

SESSION ID: HUM-R02

## Preventing Cyber Exposure: You Say Criminal, I Say Intractable



Connect   
Protect

**David Porter**

Special Advisor  
Digital Shadows  
[@digitalshadows](https://twitter.com/digitalshadows)



#RSAC



# What's coming up



***“Human error”***



# Threats seem to come from nowhere





# Victorian England, 1841





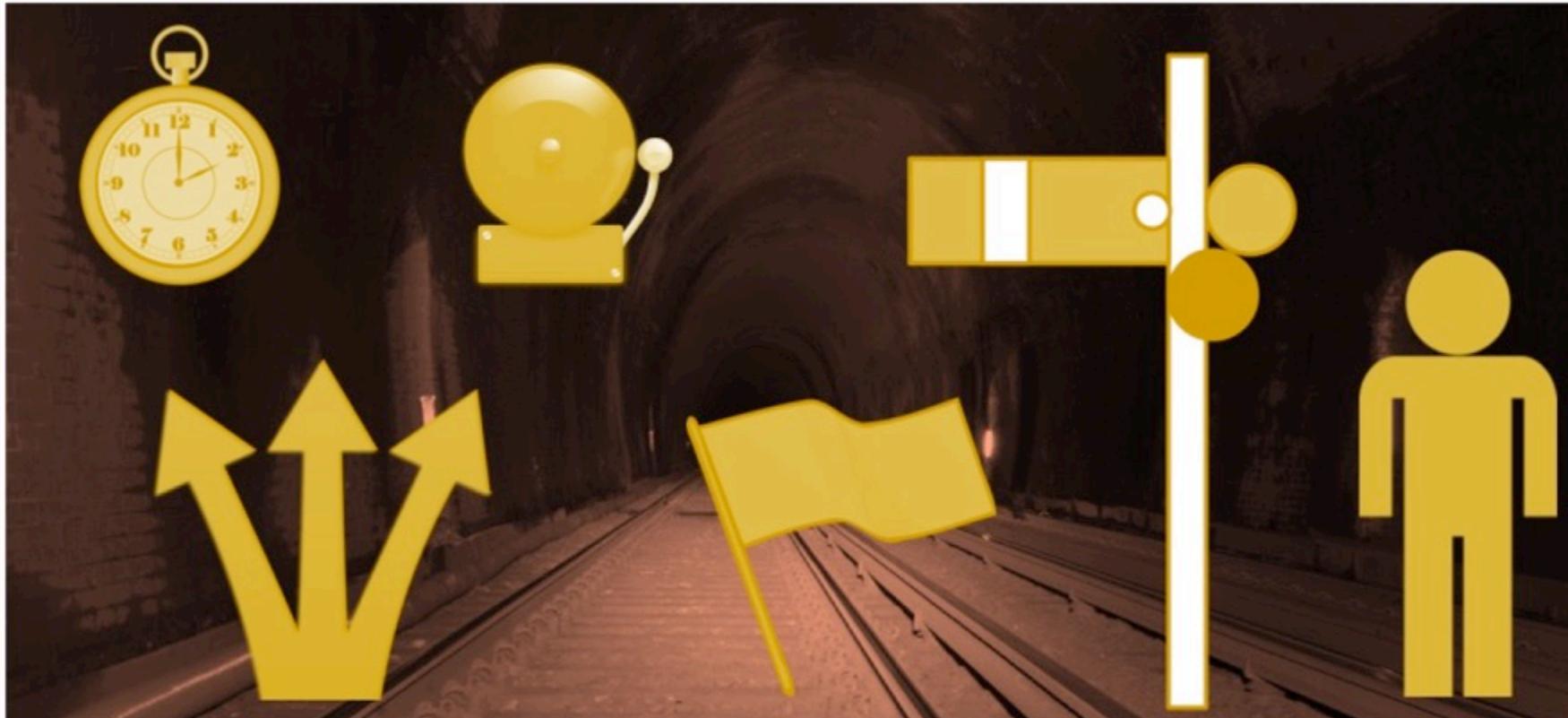
# Clayton Tunnel: a high risk environment



Only ONE train in EITHER  
direction at ANY time



# Preventative safety measures employed





# State-of-the-art telegraph technology

Has train left  
tunnel?

Train in  
tunnel

Train out  
of tunnel





# Safety system as imagined



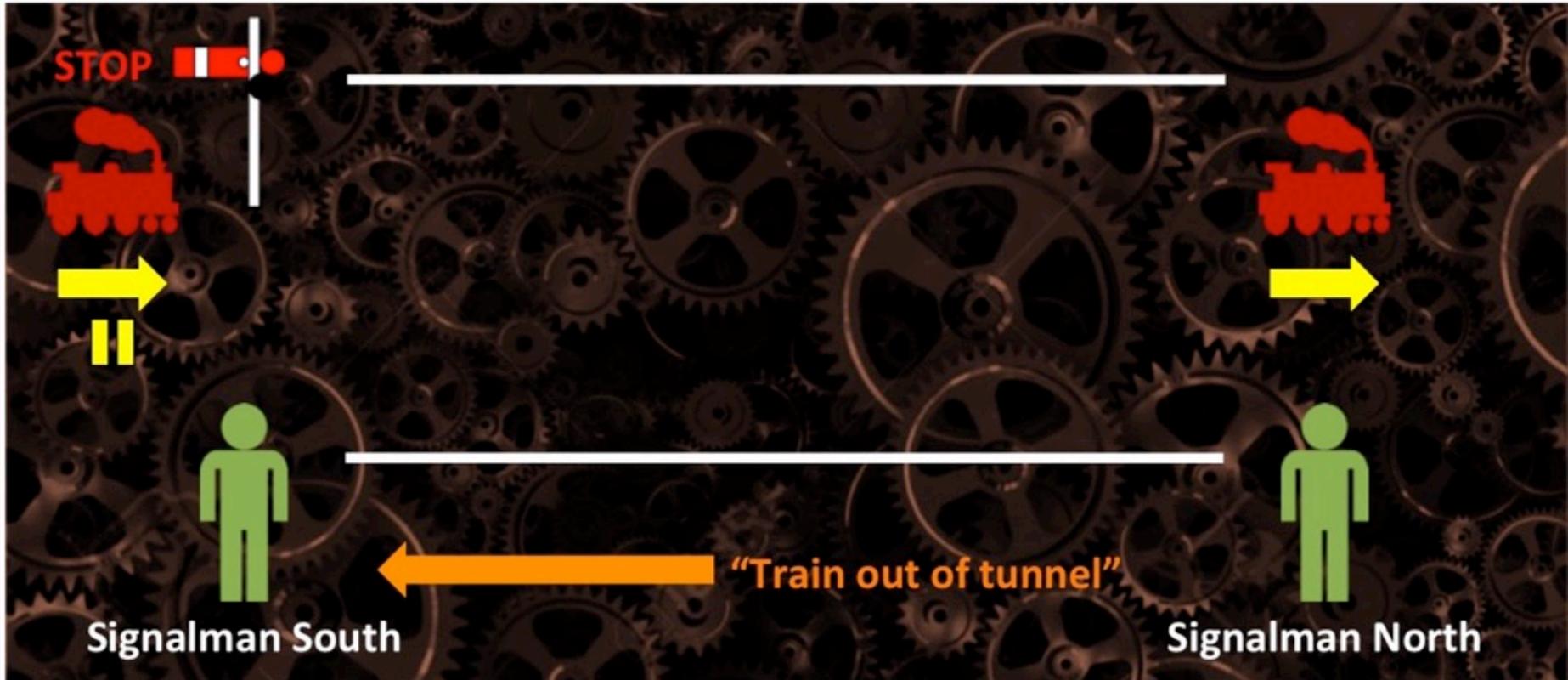


# Safety system as imagined



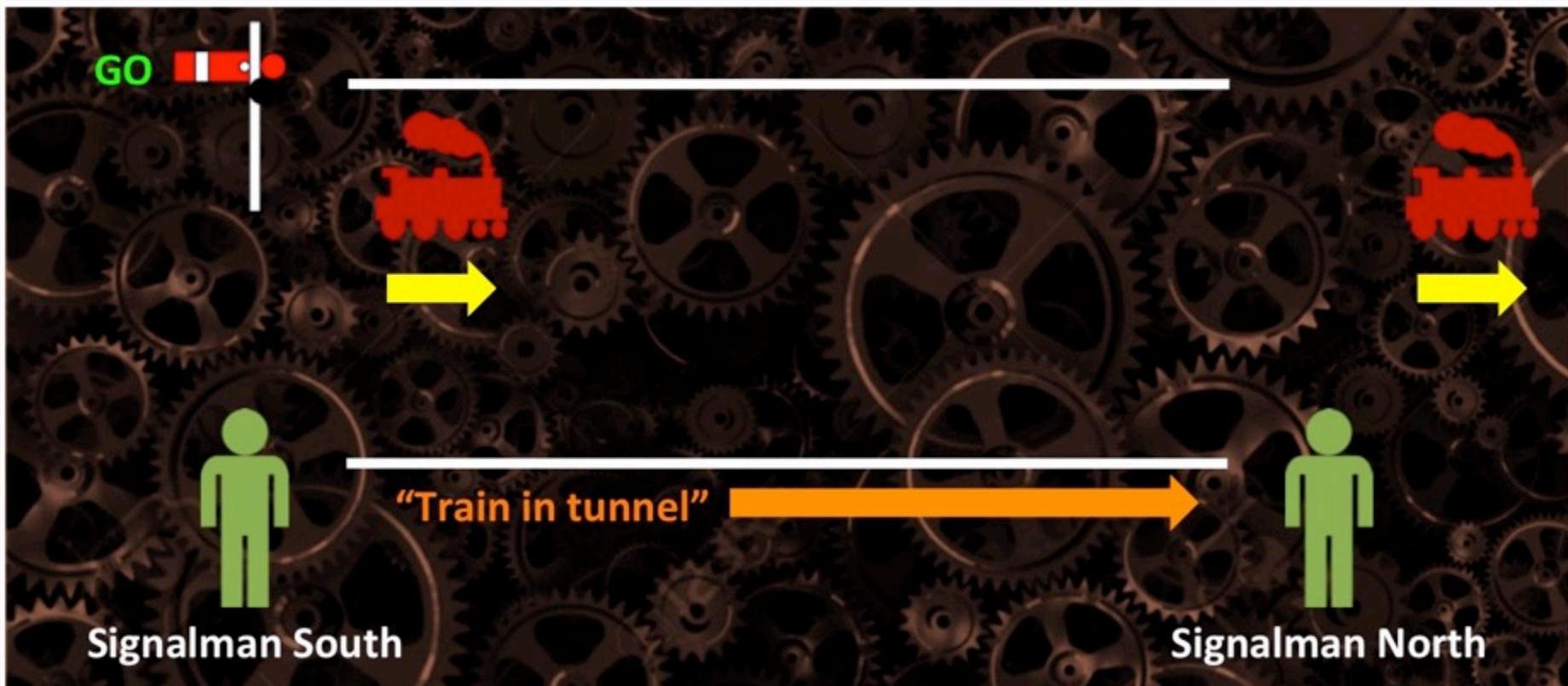


# Safety system as imagined



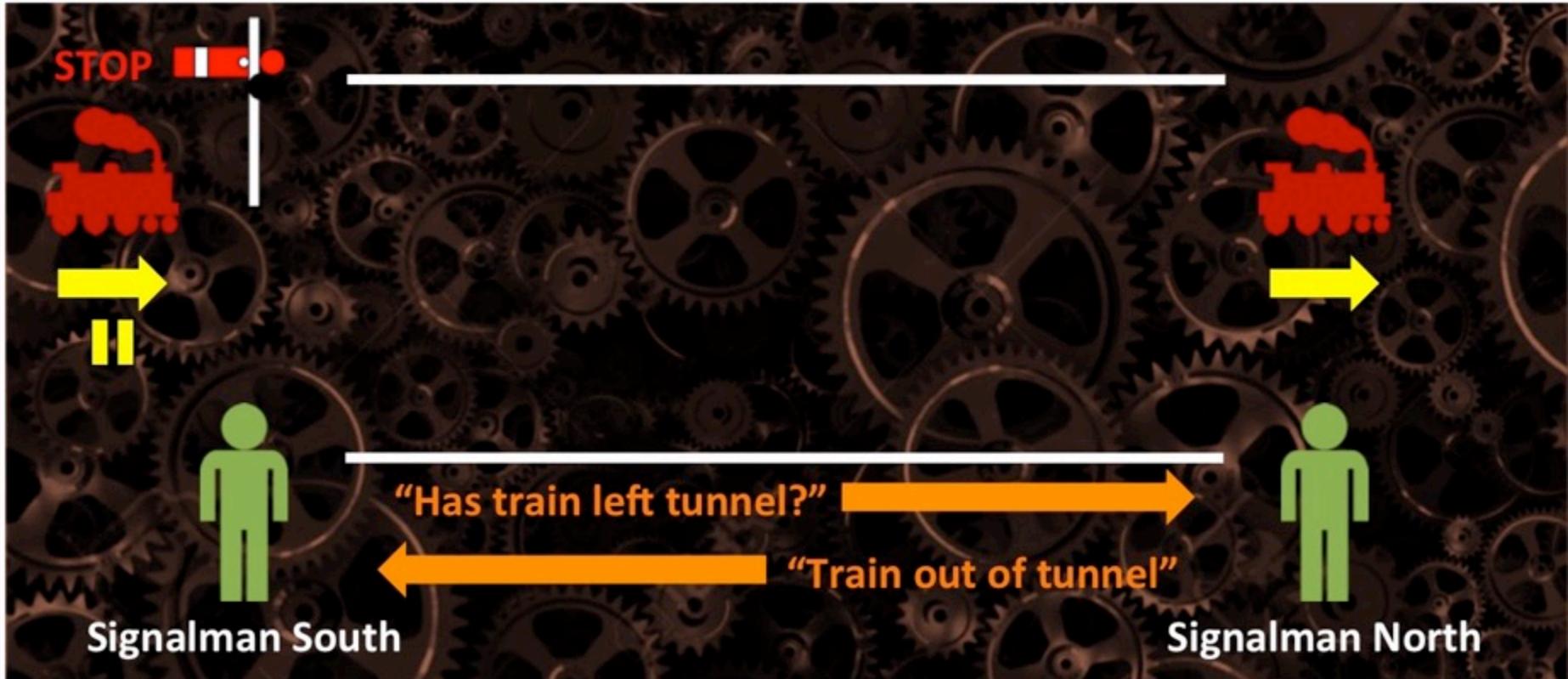


# Safety system as imagined





# 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

Gregory



Legg



Scott



Portsmouth  
Excursion



08:35

(08:30)

08:31

(08:15)

08:28

(08:05)



# 25 August 1861



Portsmouth  
Excursion



Killick



Brown



# 25 August 1861



Portsmouth  
Excursion



Killick

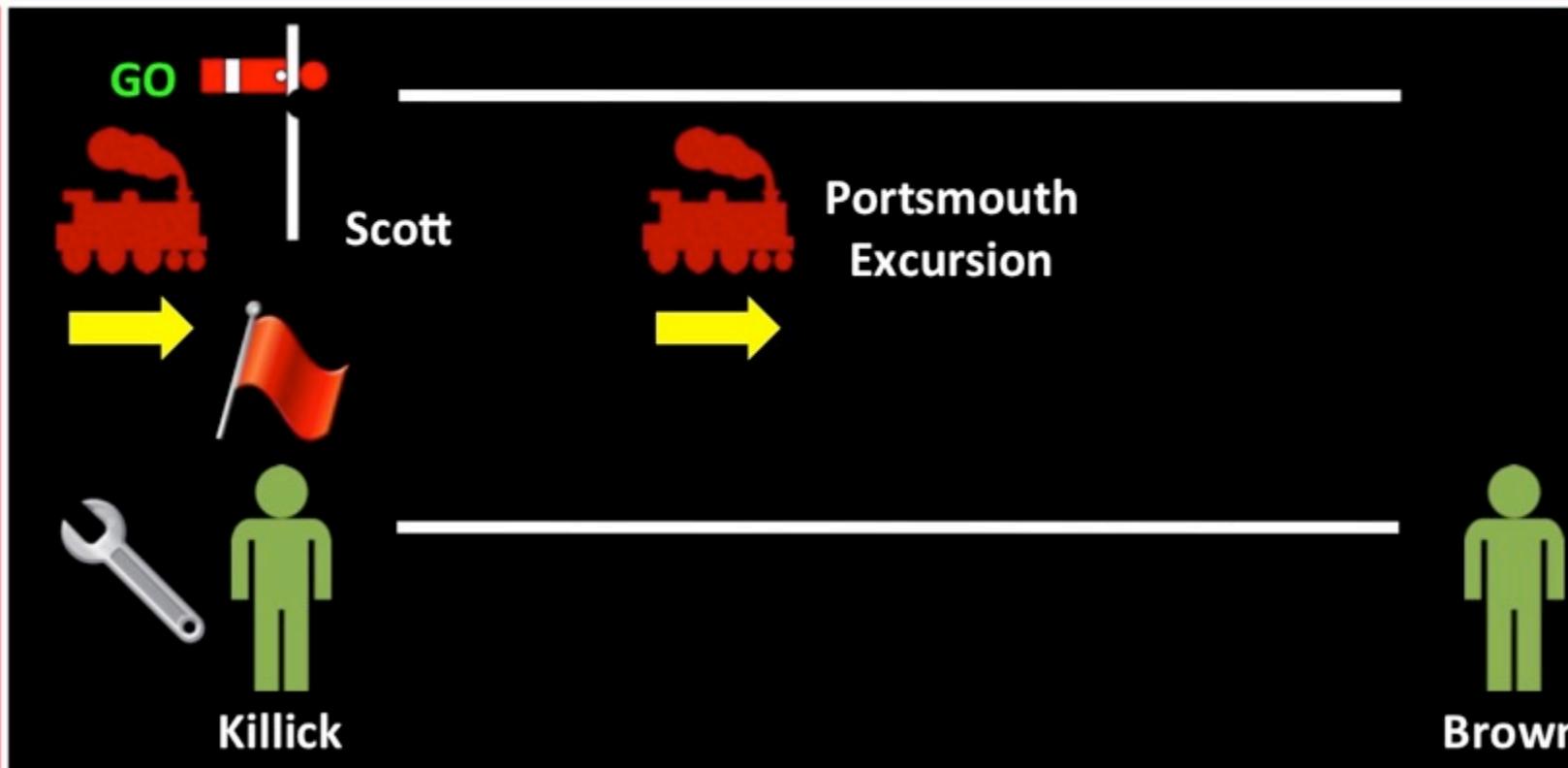
"Train in tunnel"



Brown

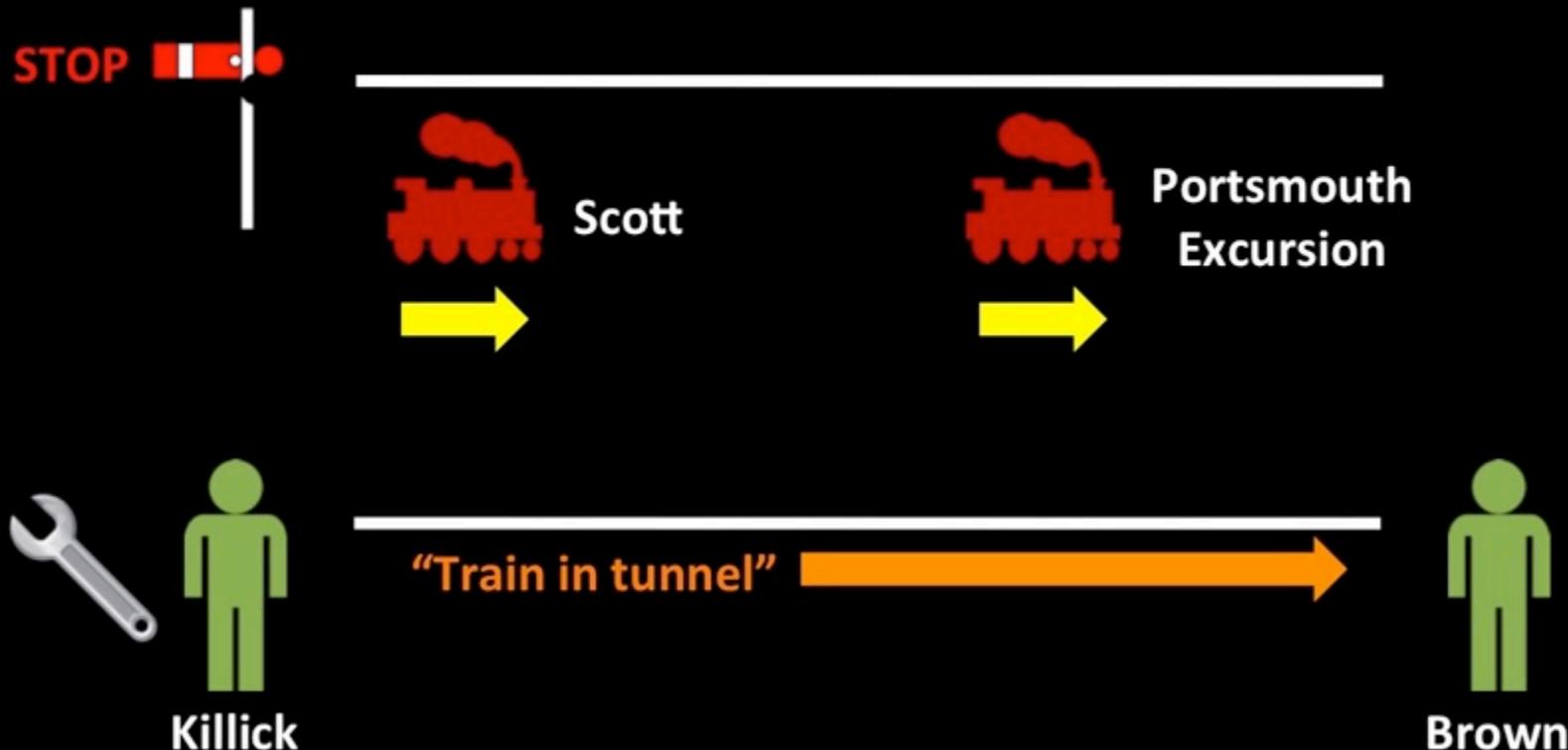


# 25 August 1861



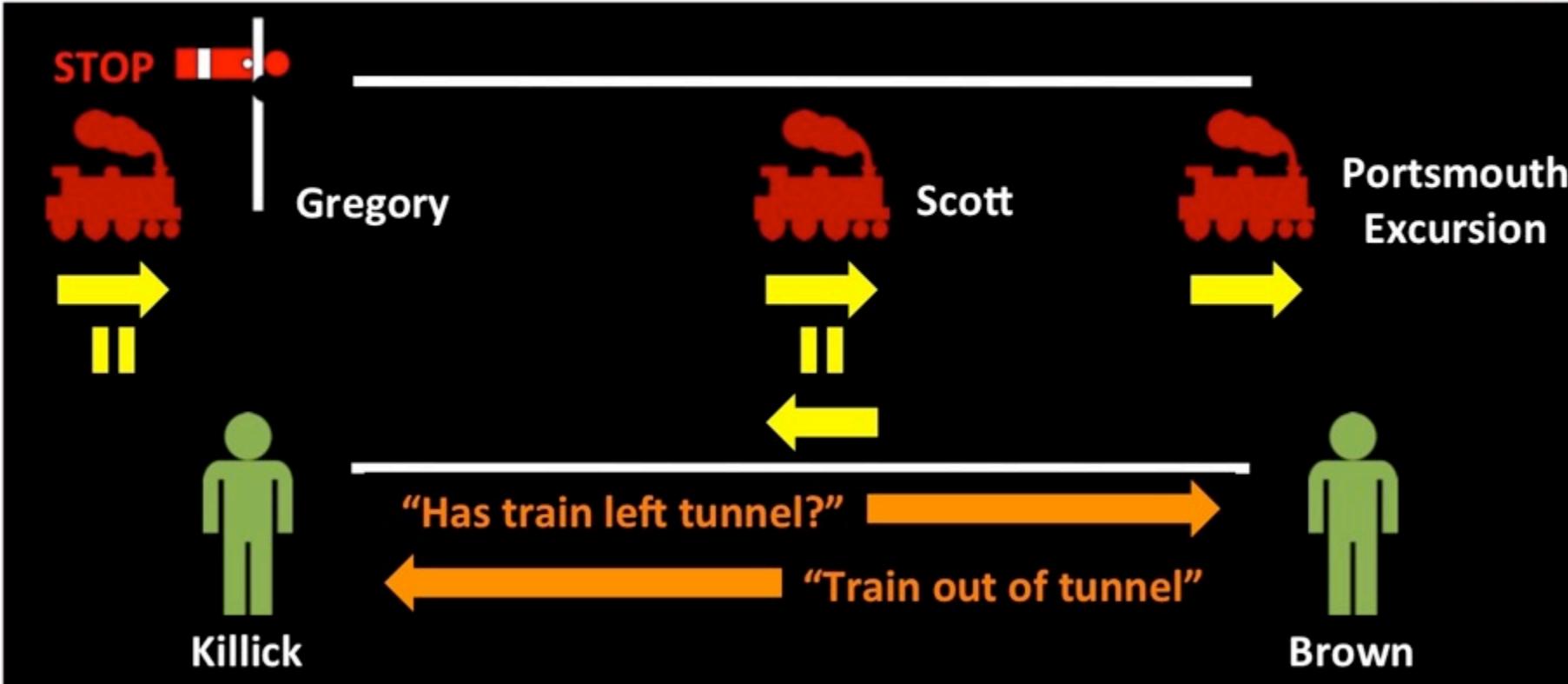


# 25 August 1861



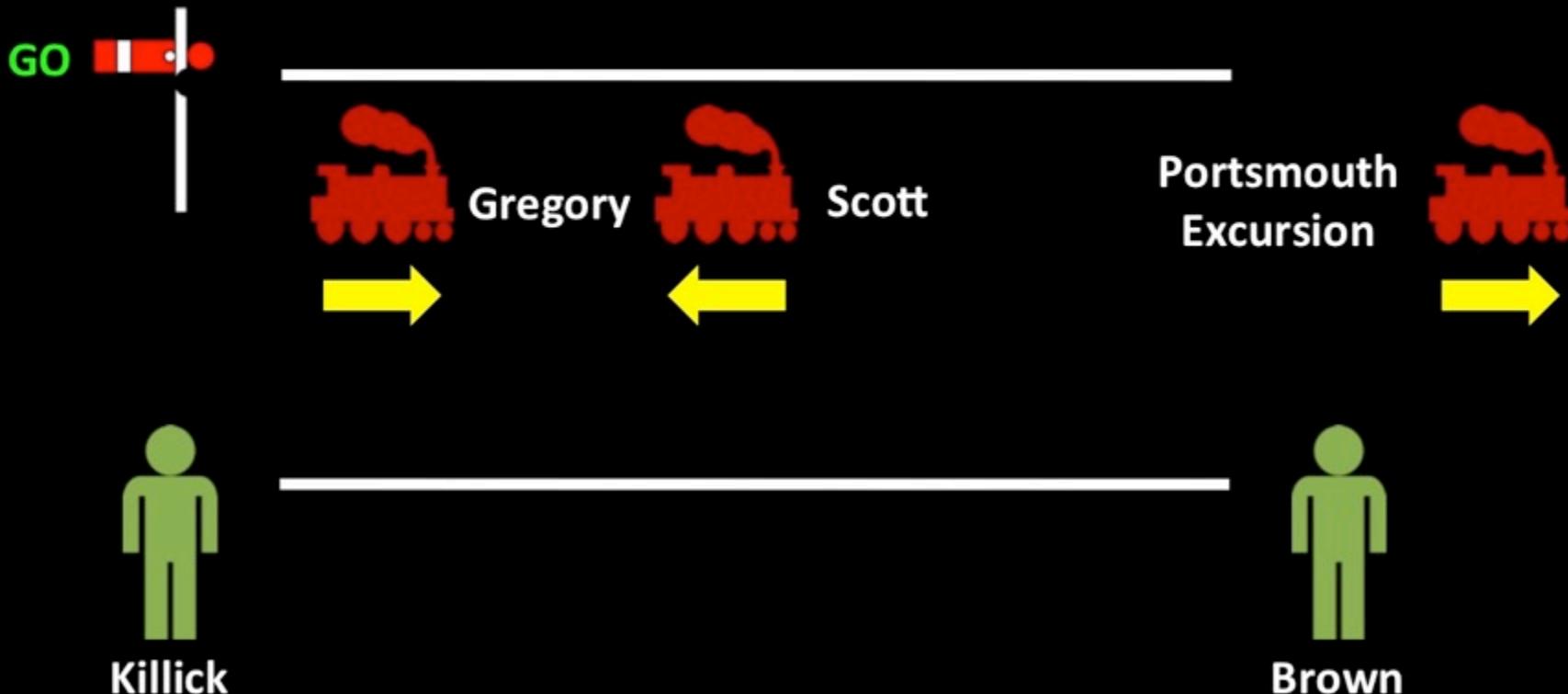


# 25 August 1861





# 25 August 1861





25 August 1861



**23 people died  
176 people severely injured**



# Despair and controversy

THURSDAY, AUGUST 29, 1801.

of the  
sued a  
eceeded  
derate  
ed to

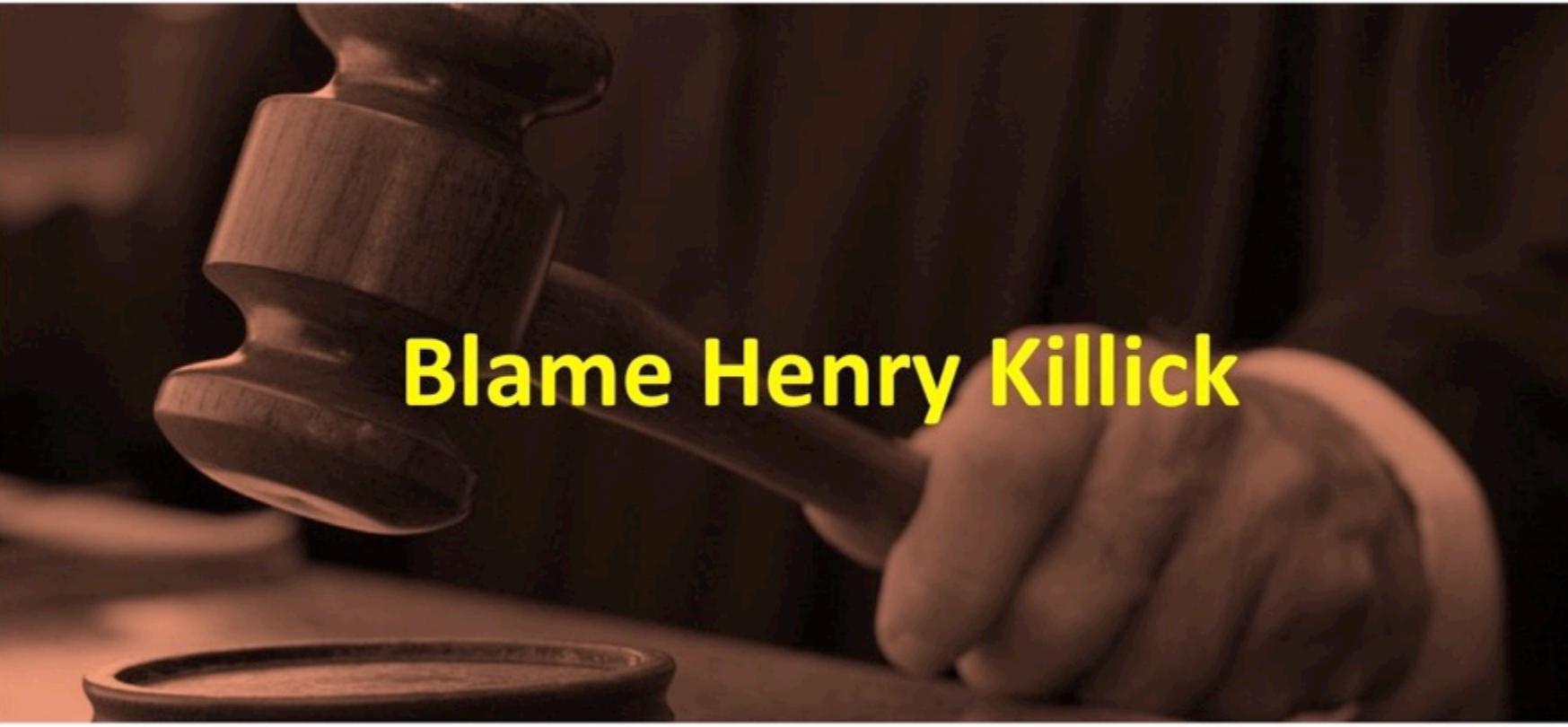
## **AWFUL COLLISION IN CLAYTON TUNNEL. GREAT LOSS OF LIFE.**

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 Brighto  
carriages, but mo  
no inconvenience  
soon as possible, t  
detached from the  
on its way to  
however, anxious  
safety, walked  
sustained very lit  
having, as it we  
of the first tr  
bruises, and the s



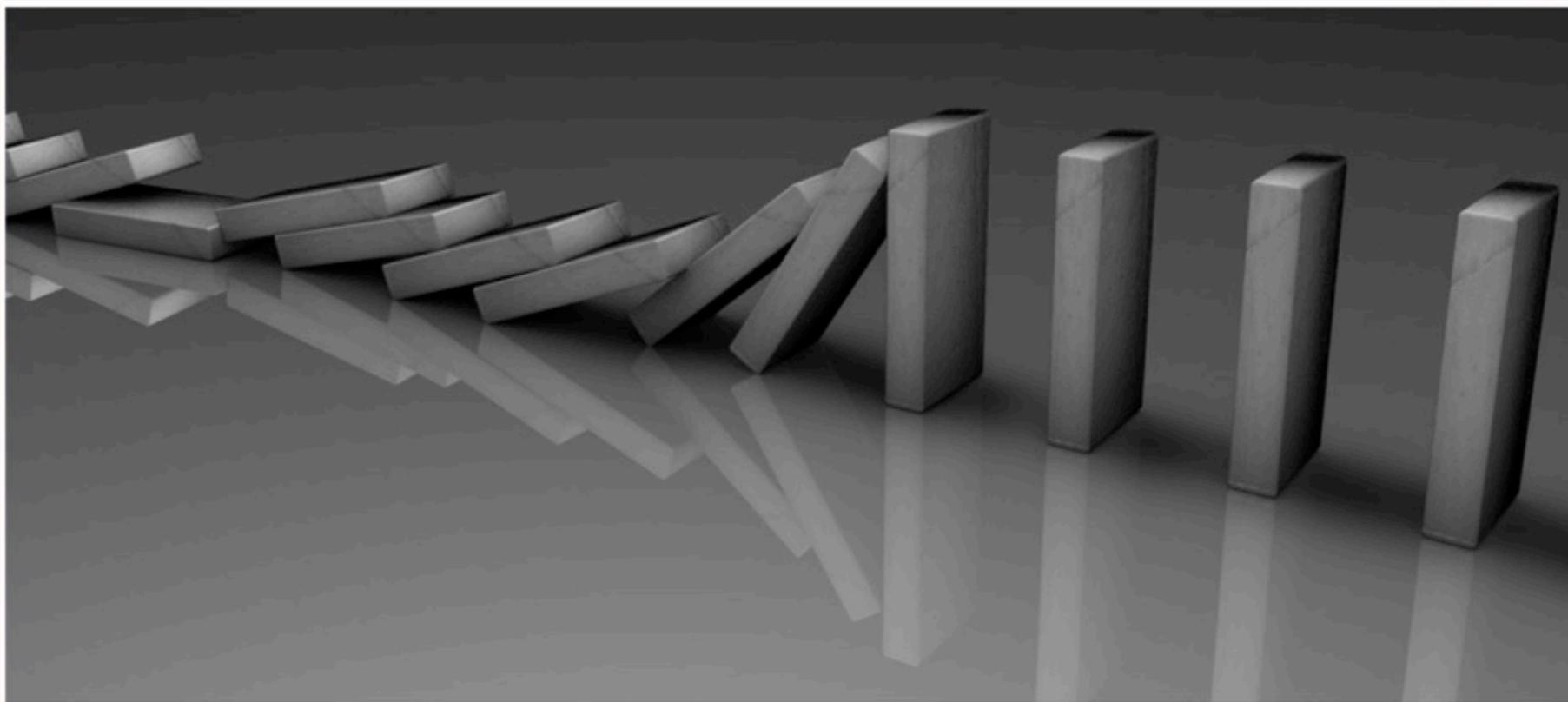
# Who's to blame?



Blame Henry Killick



# Finding the domino





# Clinging to cause-effect tradition

INCIDENTS



RISKS



# 155 years on: accidents in cyberspace

**User selling insider access to bank customer database**

Incident 865663  
25 Dec 2015 20:00

Cyber Threat

View Incident

Unread

INCIDENT DETAILS

**User selling insider access to bank customer database**

Hi folks You will not find a sale thread like this easily anywhere else. Atleast, I've seen SR & BMR and there's nothing like it there. What I'm offering is a unique service. I've got insider access to one of the largest banks in the UK and can provide you with information which hardly anybody else can.

— Incident source: <http://clsvtzwzdgzkjda7.onion/viewtopic.php?f=114&t=17467>

**Multiple documents on misconfigured device**

Incident 860677  
26 Dec 2015 09:35

Data Leakage

View Incident

Read

INCIDENT DETAILS

**Multiple documents on misconfigured device**

Backups/Company Laptop 11-28-2012/Work Backup/CF Customers/AT&T/New Docs/ATT RFP - Company Response 02\_07\_2011 v1.6 Draft.doc

— Incident source: [http://98.214.122.1/shares/Backups/Company Laptop 11-28-2012/Work Backup/CF Customers/AT&T/New Docs/ATT RFP - Company Response 02\\_07\\_2011 v1.6 Draft.doc](http://98.214.122.1/shares/Backups/Company Laptop 11-28-2012/Work Backup/CF Customers/AT&T/New Docs/ATT RFP - Company Response 02_07_2011 v1.6 Draft.doc)



# Prevention: a drunkard's search?





# Security breaches study — UK



HM Government



2015 INFORMATION SECURITY  
BREACHES SURVEY



digital shadows\_

***"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**



**ACTOR DETAILS**

## Tactics

Anonymous Saudi

A timeline of incidents linked to 'Anonymous Saudi'. Click an incident to view more details.

Overflow 2

Target list posted as part of OpEgypt and

Anonymous Saudi call for denial of service

Call for targeting of Saudi Arabian electr

Anonymous Saudi claim successful denial of

Anonymous Saudi claimed to have ren

Anonymous Saudi have rendered Bri

Anonymous Saudi target old Trump websit

Anonymous Saudi c have successfull

Intended Effect

Embarrassment Disruption Harassment

Theft - Theft of Proprietary Information

Exposure Degradation of Service

Unauthorised Access Theft - Credential Theft

Extortion

?

## Motivation

Ideological Ideological - Anti-Establishment

Political Ideological - Ethnic / Nationalist

Ideological - Environmental

Ideological - Security Awareness

Opportunistic Ideological - Human Rights

Ideological - Anti-Corruption

Financial or Economic Ego

The timeline visualization shows a sequence of incidents from 2015. The incidents are represented by yellow boxes with text descriptions, arranged horizontally. A vertical timeline bar on the left indicates the progression of time, with labels for 'Overflow' at the top and '2' indicating the number of incidents. Below the timeline, there is a small chart with a red bar representing data for the year 2015.



# Weak understanding of cyber accidents

***“Human error”***

***“Glitch”***

***“Flub”***

***“General carelessness”***

***“Trips and spills”***

***“Omission”***

***“Gaffe”***

***“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 is the endpoint: you can't patch users"*

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

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



## Blame and train “the weakest link”

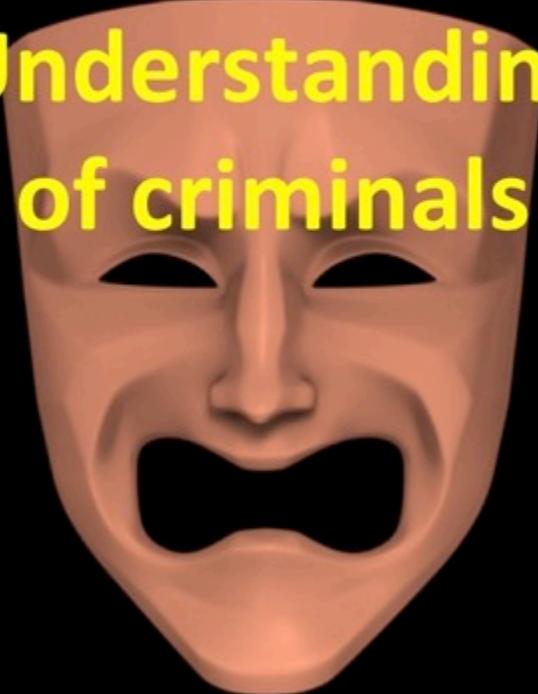
I WILL FOLLOW THE RULES I WILL FOLLOW THE RULES  
I WILL FOLLOW THE RULES I WILL FOLLOW THE RULES  
I WILL FOLLOW THE RULES I WILL FOLLOW THE RULES  
I WILL FOLLOW THE RULES I WILL FOLLOW THE RULES  
I WILL FOLLOW THE RULES I



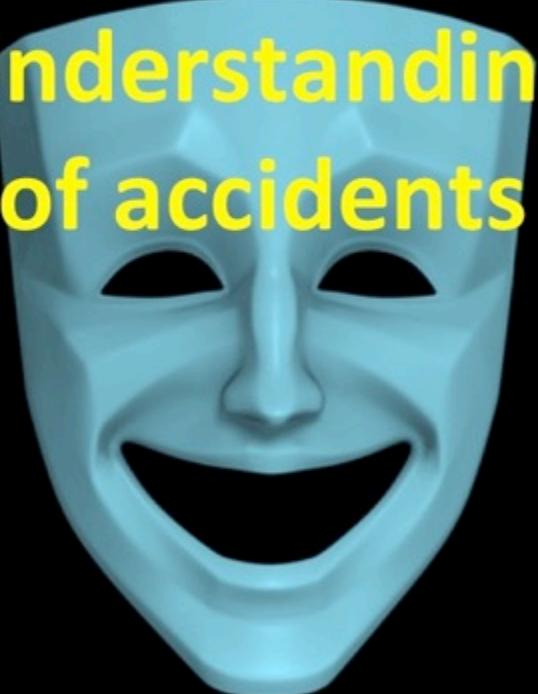


# Time to redress the balance?

Understanding  
of criminals



Understanding  
of accidents





## Resonance





# Evolution of accident analysis

1760 Technology failure

1950 Human failure

1986 Organisational failure

2011 Functional resonance



# Socio-technical systems

**Efficiency-Thoroughness  
Trade Off  
(expectation vs. hindsight)**





# Intractability

**Indivisible**

**Multi-modal**

**Non-deterministic**

**Non-linear**



# Tractable and intractable systems

Tractable



Intractable





# "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

+

Expected  
outcome  
“Correct”

Unintentional

Action  
“Correct”  
action

-

Unexpected  
outcome  
“Error”  
Intentional



# People make approximate adjustments



Why things usually go right but can go wrong

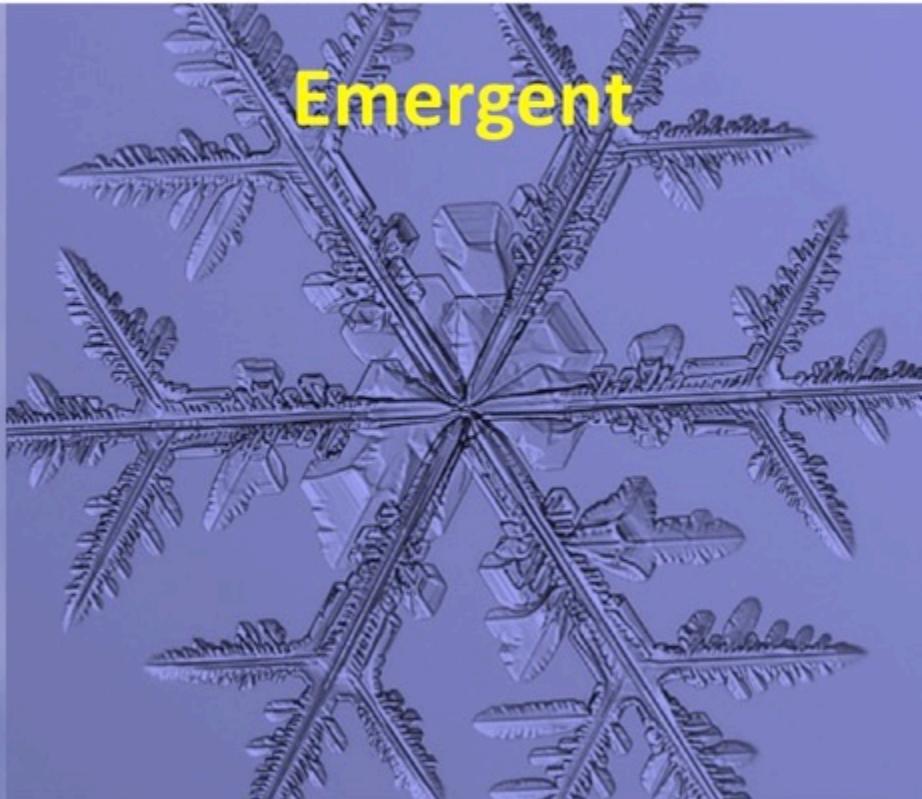


# Bad and good outcomes are emergent

Resultant



Emergent





# Variabilities can unintentionally resonate

**Functional resonance**  
The detectable signal emerging  
from the unintended  
interaction of the normal  
variabilities of many signals

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



## Modeling





# Time for a new approach

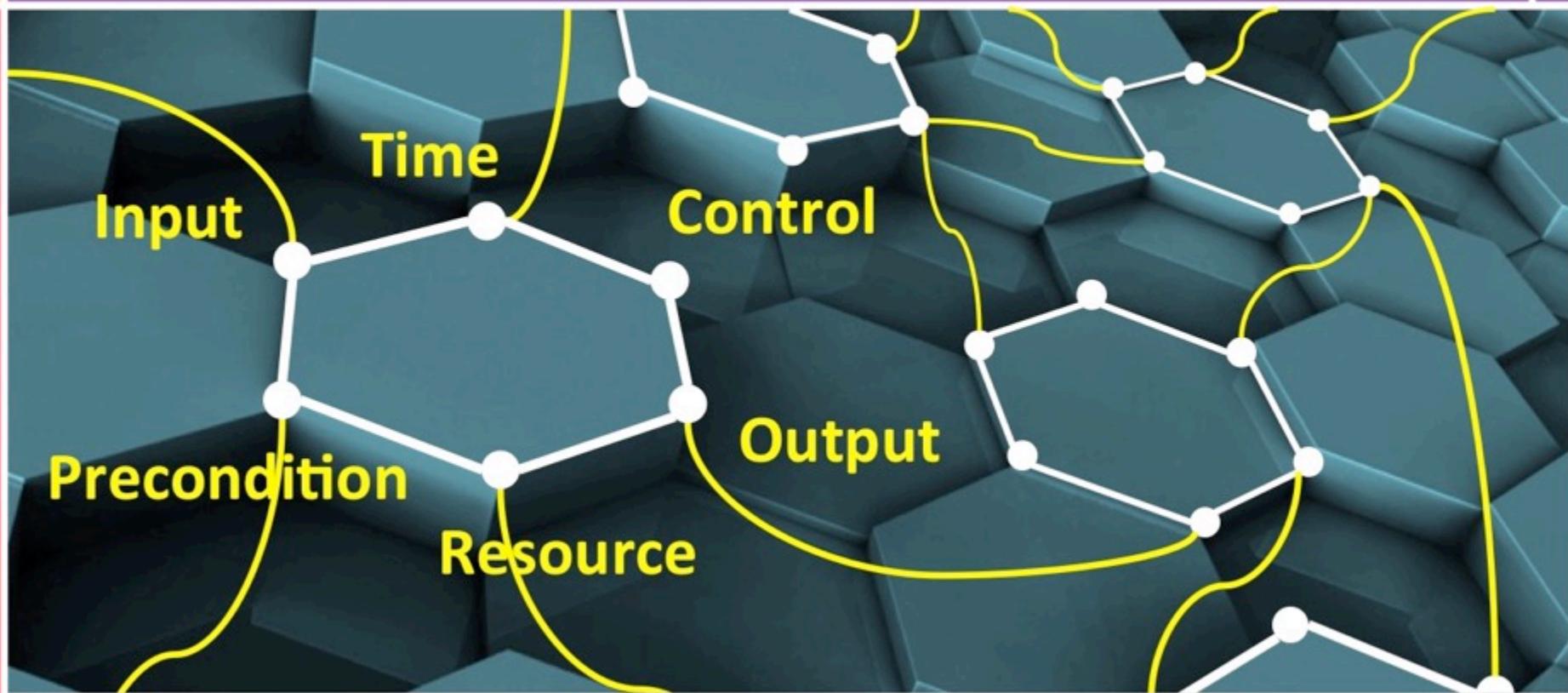
*"When the interactions among factors become more important than the factors themselves then we need to revise our approach"*

Prof. Erik Hollnagel

European Safety and Reliability Conference, 2011

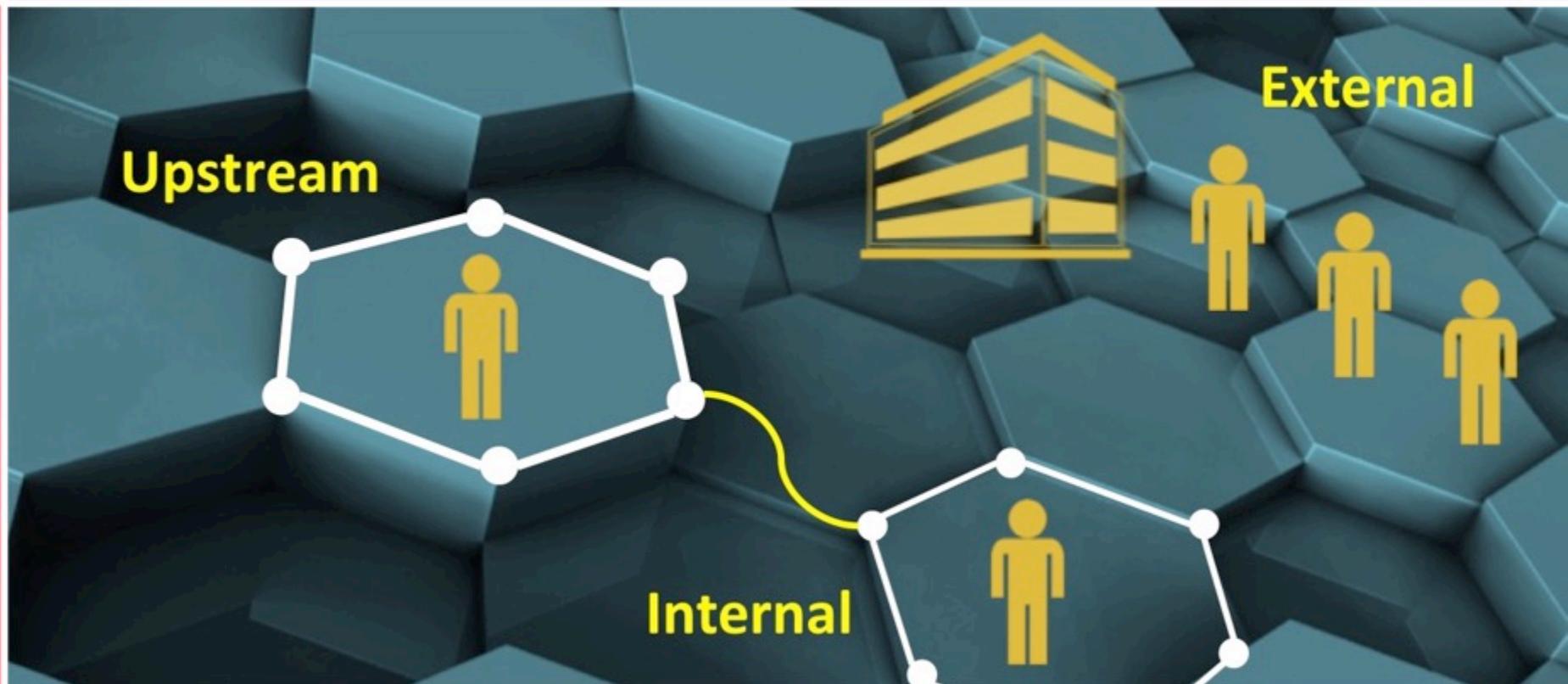


# Focus on function not architecture



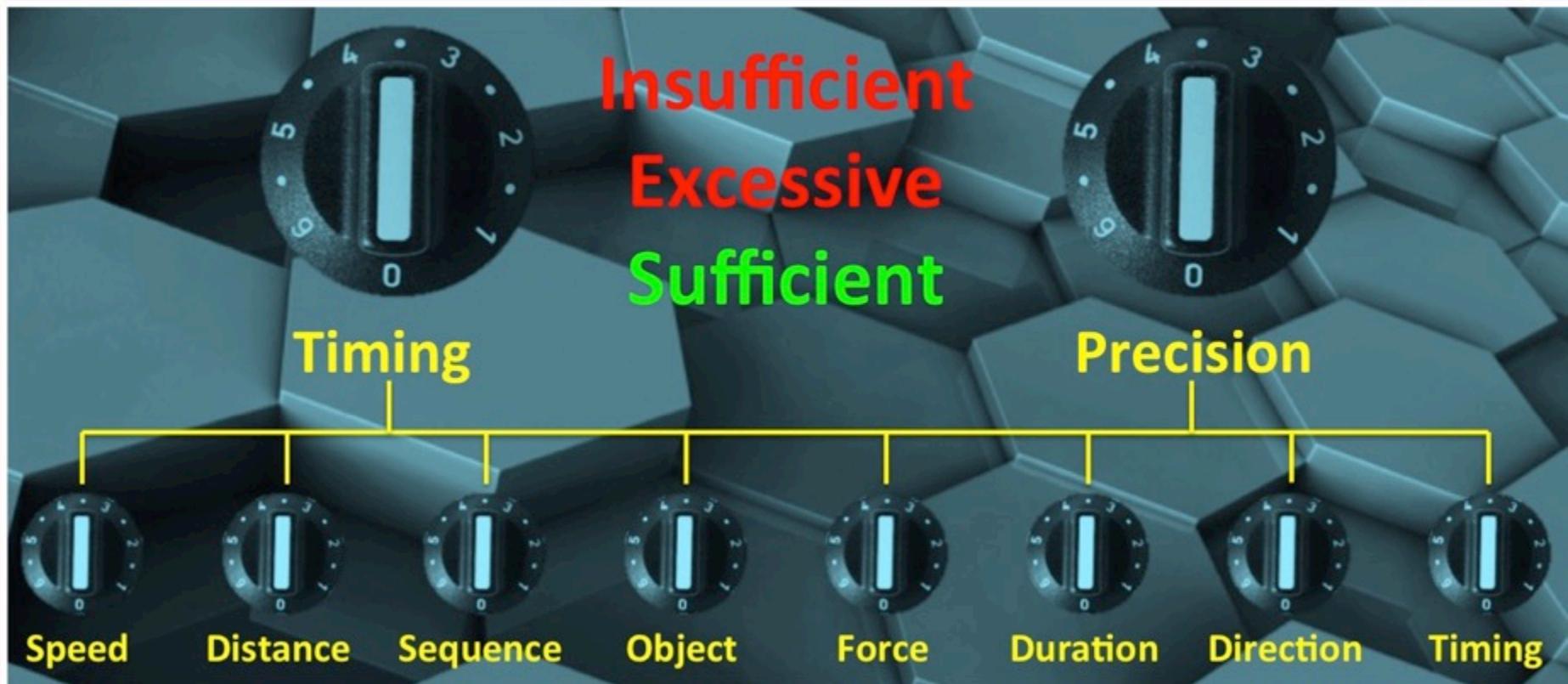


# Understand sources of variability



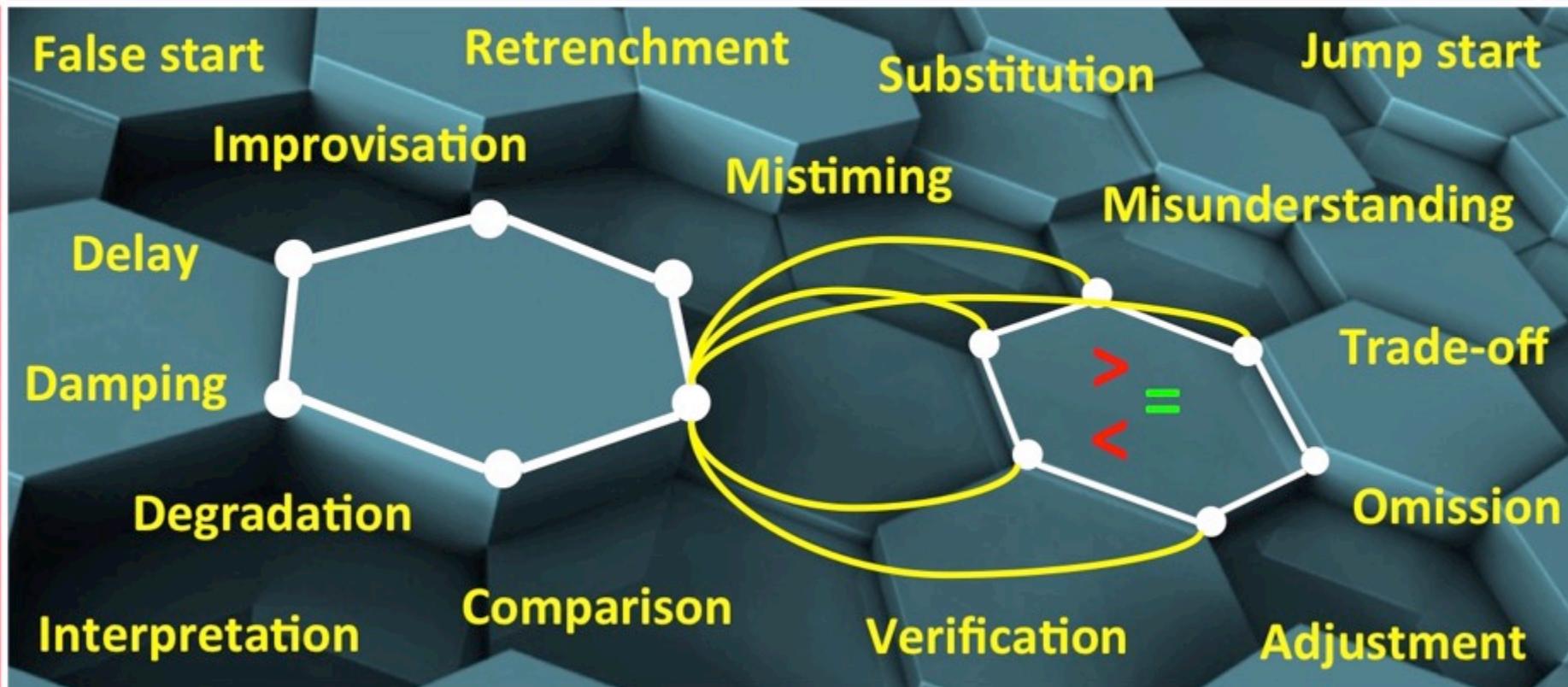


# Understand types of variability





# Identify potential functional resonance





# Monitor and influence variabilities

+

**Productivity  
and quality**

Amplify  
under control

Performance  
variability

-

**Safety and  
security**

(Eliminate)  
(Prevent)

Redesign  
Monitor  
Dampen

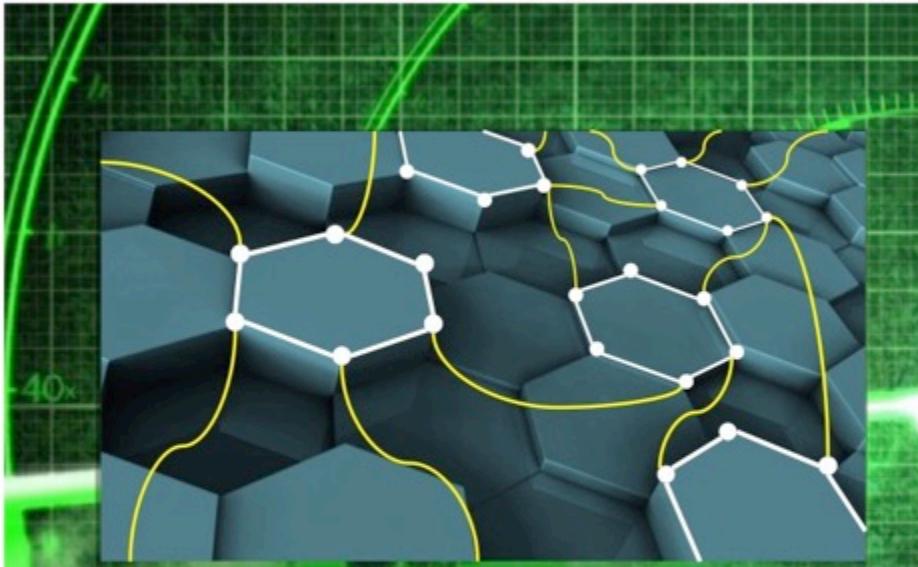


## Insights





# Situational awareness inside and beyond



**Internal accident**

| Incident Summary  | Date              | Severity  |
|---|-------------------|-----------|
| Multiple documents on misconfigured device  | 28 Dec 2015 09:30 | Very High |
| Summary: Network Attached Storage (NAS) device which is publishing documents to the public internet.                    | 28 Dec 2015 09:30 | High      |
| Summary: We have detected a Network Attached Storage (NAS) device which is publishing documents to the public internet. | 28 Dec 2015 09:30 | Medium    |
| Summary: We have detected a Network Attached Storage (NAS) device which is publishing documents to the public internet. | 28 Dec 2015 09:30 | Low       |
| Summary: We have detected a Network Attached Storage (NAS) device which is publishing documents to the public internet. | 28 Dec 2015 09:30 | Very Low  |
| Summary: We have detected a Network Attached Storage (NAS) device which is publishing documents to the public internet. | 28 Dec 2015 09:30 | None      |

**External criminal**

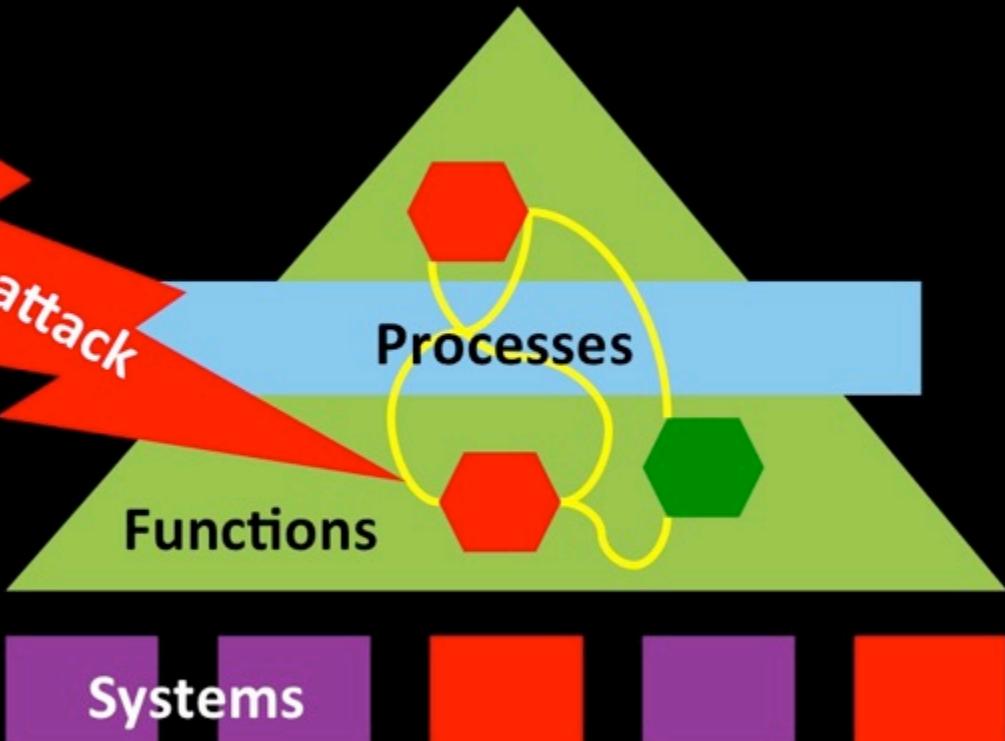


# Facilitating intelligence-led testing



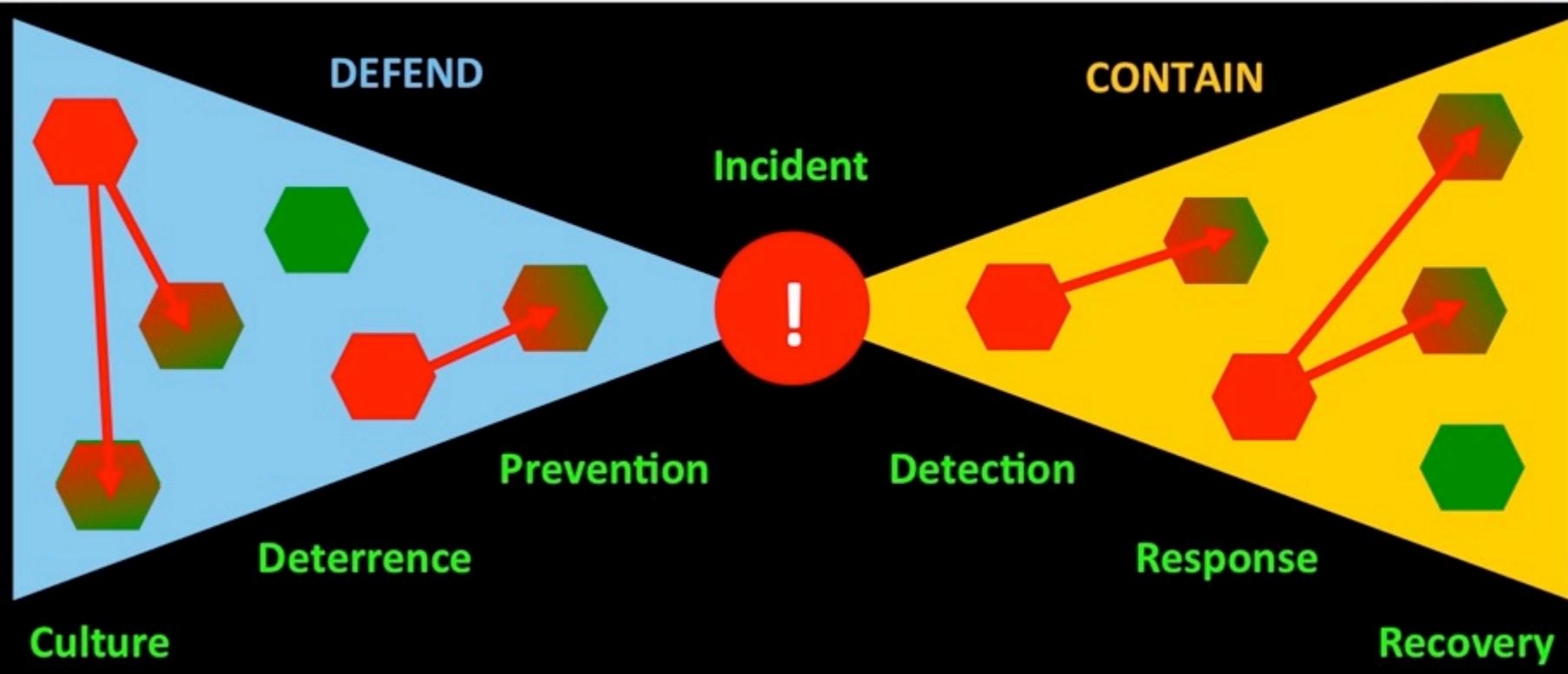
CBEST

*Cyber attack*



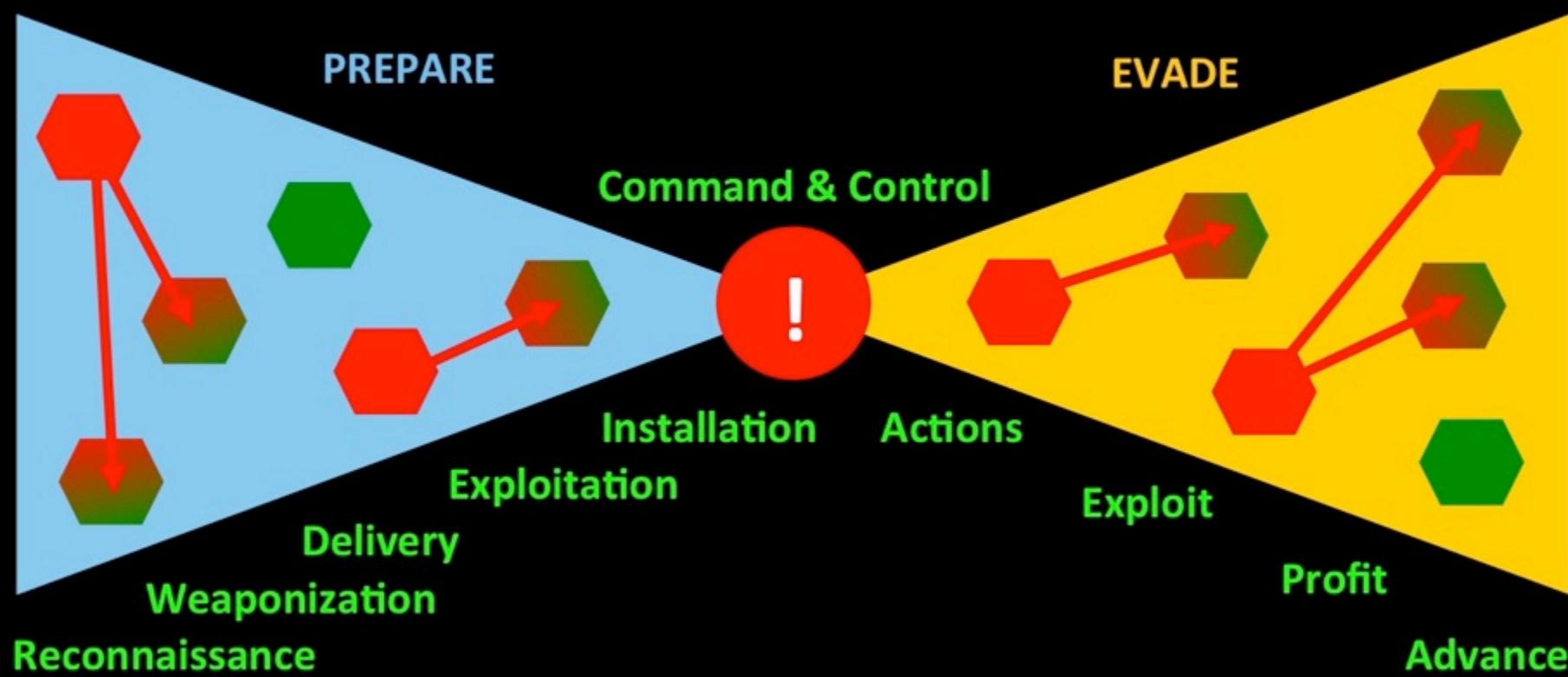


# Testing our cyber defenses



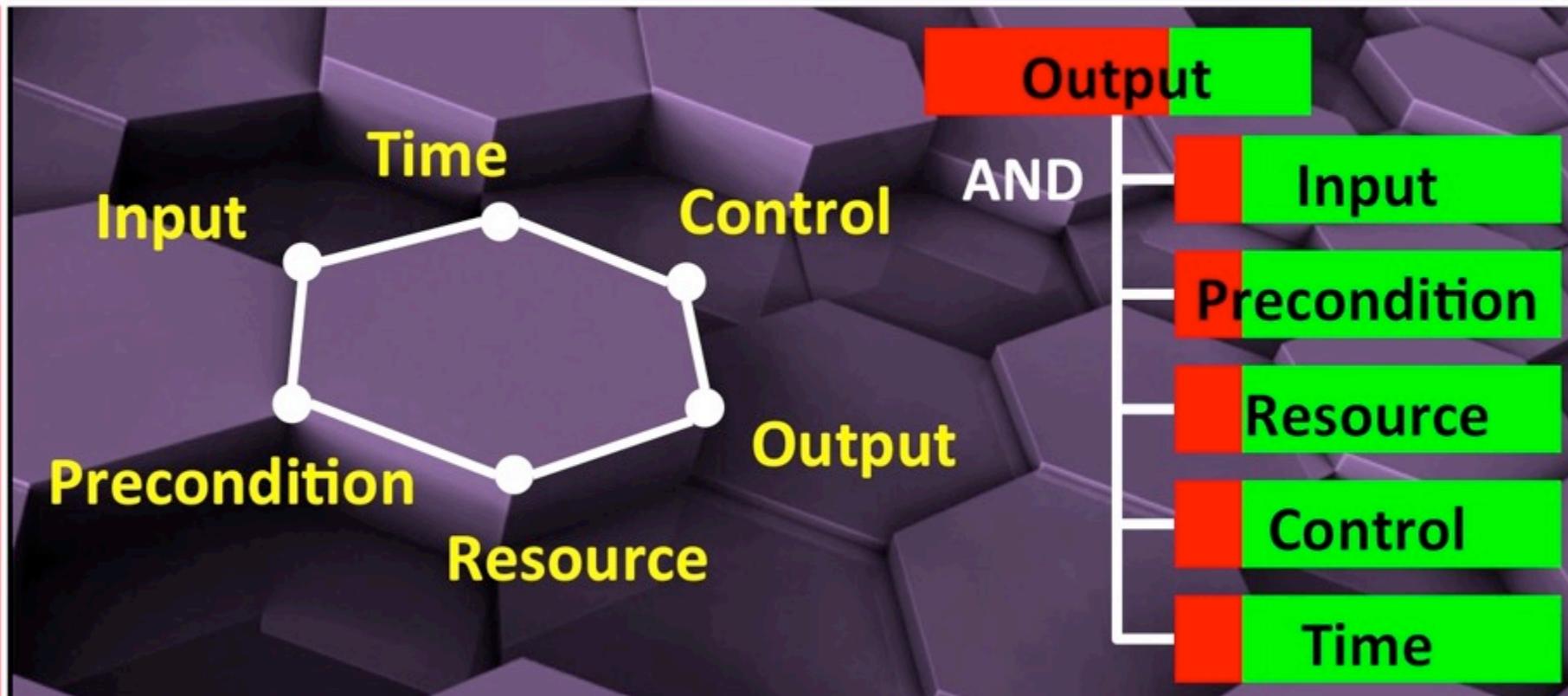


# Disrupting the kill chain





# 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



Your systems are intractable

People don't make errors

Situational awareness illuminates



# 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





Thank you

digital shadows\_