LONDON'S GLOBAL UNIVERSITY

Review of emergent behaviours of systems comparable to infrastructure systems and analysis approaches that could be applied to infrastructure systems

S. Neda Naghshbandi, L. Varga, T. Dolan[1]

Civil, Environmental and Geomatic Engineering Dept, UCL

24 Apr 2020

Contents

Disclaimer: This report was produced to inform the National Infrastructure Commission's study on resilience. The views expressed and recommendations set out in this report are the authors' own and do not necessarily reflect the position of the National Infrastructure Commission.

[1] Naghshbandi identified cases and approaches and prepared case and approach descriptions, Varga led on emergent failure, characteristics of infrastructure and sectors similar to infrastructure, and supervised the work, Dolan conducted approaches' analytics. We are grateful for the excellent contributions from NIC, and in particular the constructive input and feedback from Eleanor Voss

1. Summary

This paper makes contributions to the understanding of emergent failure in economic infrastructure by considering case studies and approaches from sectors comparable to infrastructure. The review starts by identifying existing ways of thinking about emergent failure and narrows down the scope to system-of-systems' failures which are unexpected and arise when systems appear to be working normally. In order to target sectors similar to infrastructure, the characteristics of infrastructure sectors were identified; infrastructure scope was limited to energy, transport, water, and telecommunications. Other sectors were identified and assessed against infrastructure characteristics. The sectors most similar to infrastructure were then reviewed for cases and approaches, limiting our search to those outside the UK.

Multiple case studies and approaches were located initially via searches of academic articles (peer-reviewed) and grey literature (unpublished, informal papers). Through iteration with the National Infrastructure Commission (NIC) secretariat, in particular with a focus on how the case studies and approaches help to inform the challenges relating to emergent failure in infrastructure systems, we settled on five case studies and 11 approaches. Finally, we co-developed and agreed the templates for use for both the case studies and the approaches, and then populated the templates.

Each case study contains the following details: the sector in which the case arose, the particular failure that emerged, the interactions causing the failure, and their consequences. A narrative is included for each case describing: events during the failure, the background context to the failure, the emergent behaviour that arose, and latest understanding on the causes of the particular failure. Finally, the insights for infrastructure are noted by considering how the emergent failure could arise in infrastructure systems. The case studies heavily reinforce the dormant, or latent, systemic weaknesses that arise when multiple systems each with their own objectives, are connected and interdependent upon shared resources, flows, data.

The approaches relevant for analysis of failure, are described and analysed as follows: Name and Type, Rankings Summary (applicability to UK system of economic infrastructure, cross sector applicability, strategic relevance to NIC), Applications and Comparability Scores, Purpose, Key concepts, Data requirements and availability, Skills and resource requirements, Complementary approaches, Strategically relevant outputs. Overview and References.

The findings offer the UK Government insight into national infrastructure resilience from an international perspective.

The report is organised as follows: Section 2 discusses the scope of emergent failure for the purposes of this review. Section 3 sets out infrastructure characteristics. Section 4 identifies sectors similar to infrastructure. Sections 5 and 6 describe the search strategies and the results of the cases and approaches respectively.

2. Emergent failure

Engineered systems that stop delivering products and services, such as electricity, potable water, mobility, and wi-fi, are said to have failed. These failures are referred to as accidents, incidents and even disruptions and disturbances. Accidents, especially major ones, have been investigated, and when new forms of accidents arose in the past, new explanations of causes were introduced, fostering the belief that bad outcomes occur because something goes wrong, and if we can find and treat those causes, future accidents would be prevented[2]. This has fostered an interest in looking only at failures which is important for critical services, as failures may lead to harm or loss of life and property. However, things can also go right, and indeed that is the purpose of design, construction and operation of built systems. There are four possible states, using dimensions: Positive vs Negative outcomes, and High vs Low probability as shown in Figure 1.

> "**Positive outcomes that have a high probability.** This subset represents the successes or 'normal' actions, i.e. the things that not only go right, but also that are expected to go right. In other words, everyday work or everyday functioning. These are essential for resilience, but rarely if ever considered by safety.
>
> **Positive outcomes that have a low probability.** This subset represents the 'good' things that happen unexpectedly. There is no commonly recognized terminology for these; when they happen they are simply accepted with gratitude.
>
> **Negative or unwanted outcomes that have a low probability**, i.e. things that go wrong and which are unexpected – although not unimaginable. This is the subset of outcomes that traditionally is associated with safety (or rather, the lack of safety), particularly outcomes that cause significant losses and are hard to predict.
>
> **Negative or unwanted outcomes that have a high probability.** This basically means adverse outcomes that realistically must be expected to happen frequently or even regularly. The purpose of risk assessment and risk management is to identify how such outcomes can arise and prevent them from happening. This is usually done successfully; cf. the ANSI definition of safety as 'the freedom from unacceptable risks'. In practice this subset is therefore very small."

Figure 1 - From Hollnagel, E., 2014. Resilience engineering and the built environment. *Building Research & Information*, *42*(2), pp.225-226

The state of most concern due to the growing incidence of apparently low probability failures is **Negative or unwanted outcomes that have a low probability.** This state, as it stands, deals with imaginable or predictable outcomes that have low likelihood. To be predictable means that we can know causal pathways and deduce outcomes from low-level facts. This is also known as 'weak emergence.[3] Another way to say this is that investigators have discovered, often through close examination, how the emergent

[2] Hollnagel, E (2014) Resilience engineering and the built environment. *Building Research & Information*, 42(2), pp.221-228

[3] Fromm, J (2005), Types and Forms of Emergence, https://arxiv.org/abs/nlin/0506028

properties of a system (such as reliability and safety) were affected by the low-level organisation of its components.

Examples of explanations for predictable, weak emergent failures include:

1. components or sub-systems have **degraded** over time (e.g. due to under-investment or lack of adequate maintenance, or ignorance of degrading materials, or due to transfer of ownership/responsibility without due diligence of reliance placed on the component, or due to efficiencies through pooled resources, which reduce contribution toward maintenance)

2. components or sub-systems have changed in **criticality** (e.g. due to rising importance beyond design specification)

3. components or sub-systems are subjected to **common mode failure**, due to lack of diversity in the system, (e.g. all engineers taught the same knowledge, but new knowledge on how integrated systems are working is absent)

When weak emergent failures occur, they take operators by surprise because they had not treated with risk of sufficiently high probability for the engineering systems to have taken precautionary interventions.

There is a growing class of **Negative or unwanted outcomes that have a low probability** and these arise where the causal pathways are *unimaginable* or *unpredictable*. The failure of the system comes as a complete surprise as components and sub-systems are working within design limits. Others have described these types of failure as 'Black Swans' or 'Strong Emergence', where the pathway to the emergent failure was totally surprising, arising through multiple feedbacks and adaptation in complex adaptive systems due to evolution.

Examples of explanations for unpredictable, strong emergent failures include:

1. components or sub-systems have become (more) **coupled** and either depend on couplings or are depended upon by couplings which are outside the control of the system (e.g. coupled to a power grid which has other system demands, where control cannot be exercised as boundary of responsibilities are crossed)

2. components or sub-systems are subject to **high impact exogenous threats** (hurricanes, seismic activity, …) outside the design window of the built/engineered solution (i.e. there is 'theoretical' risk transfer which can't be managed in reality)

3. people and organisations **respond in totally unexpected ways** when components or subsystems fail (e.g. irrational protection of property, changed cultural norms have not been addressed by engineered/built systems, …)

Emergent failure is thus concerned with surprise disruptions to systems of systems which have the capacity to kill or seriously injure people, and/or disproportionately damage assets. Failures may be large single events affecting many people, such as aeroplane crashes, or multiple events affecting few people, such as road accidents) but overall, the failure event(s) is large and noticeable.

Every outcome is emergent including positive ones. When the pathway to that outcome is predicable or imaginable it is called weak emergence. Systems are designed to achieve positive outcomes via particular pathways.

When the pathway to an outcome is *not* imaginable, it is called strong emergence. Unexpected good outcomes an also arise, so strong emergence can occur for both negative and positive outcome.

It is worth clarifying the distinction between *engineer**ed*** systems, such as roads and water mains, and *engineer**ing*** systems which are the organizational, technical, political, and soft systems that operate the engineered systems in order to deliver products and services.[4] Engineered and engineering systems are organized in a way so as to attain **emergent properties,** such as security, resilience, affordability, reliability, safety, environmental friendliness, and social acceptability. These emergent properties have become increasingly well defined, and have grown in terms of theoretical understanding and validity of methods that justify our belief in their value to society. In fact, they have matured to an extent that we can measure and apply quality criteria as to society's and industry's minimum standards of performance, for example, security standards such as physical barriers, reliability quality such as proof that what is transmitted is received, and emissions limits that control air quality in urban areas. The emergence of these properties (and related quality levels) is achieved by the organization of components, processes and behaviours in engineered and engineering systems that produce and deliver infrastructure products and services. Changes in either engineered or engineering systems will affect whether or not these emergent properties arise and to what quality standard. Changes in the environment, both natural and socio-economical) can also cause emergent properties to change. Emergent properties arise in knowable, and unknowable ways. A failure may refer to either a failure of the engineered system, such as derailment, or the failure of an engineering system, such as a security breach. Both types of failure will limit or prevent the system being usable.

Information systems are typically large with many dynamics in network connection, lots of heterogeneity in components, and developed within time and cost constraints. Such systems have an implicit assumption that component behaviour and interactions are fully known, and great efforts go into verification and validation. But for complex systems, even if the functional behaviour of each single component of the system is known, their interactions can anyway produce unexpected situations leading to system failures. One source of ignorance about emergent failure is the use of 'Components off The Shelf' (COTS) as part of a larger solution; COTS are used in many engineered systems. Challenges arise due to lack of control and knowledge about the COTS: i) functionality, performance and evolution of COTS respond to market demand (not the needs of the COTS adopter); most COTS are not designed to interoperate with each other; iii) COTS vendor behaviour varies widely with respect to support, cooperation, and predictability[5].

One or more of the components of the system may not be working as anticipated by the system of systems in which they are embedded, but they are working in a way intended by their design or developer. I.e. they may be sub-optimal in the system of systems. It is

---

[4] Mayfield, M Punzo, G, Beasley, R, Clarke, G, Holt, N, Jobbins, S (2018), *Challenges Of Complexity and Resilience In Complex Engineering Systems*, Encore Network+ White Paper, EPSRC grant EP/N010019/1

[5] Vinerbi, L, Bondavalli, A, Lollini, P (2010) Emergence: A new Source of Failures in Complex Systems 2010 Third International Conference on Dependability, DOI 10.1109/DEPEND.2010.28

the system-of-systems, e.g. an electricity network, which fails, and the sub-optimal component may not be even within the scope of an investigation.

This report uses the following definition of emergent failure:

> **“A non-linearly large (many small or one single) disruption (not necessarily an entire collapse) of a system-of-systems (SoS) due to interactions between systems or between systems and people, in particular contexts, where systems do NOT fail (but may be sub-optimal) but the SoS does fail”**

3. Infrastructure characteristics

The starting point for characteristics of infrastructure is a discussion paper on "Characteristics of Infrastructure Sectors and Implications for Innovation Processes"[6] This paper introduces five dimensions of economic infrastructure sectors such as energy, gas or water supply, waste water treatment and telecommunication. These are: capital intensity, asset durability, a key role of public organizations, regulation intensity and a high degree of systemness (or interconnectivity).

A further four dimensions of infrastructure characteristics, identified at the ITRC conference on national infrastructure and economic prosperity[7] are included. These are: spill-over effects, investment leads to variety in economic growth, ramifications of failures, and uncontrollable demand. Infrastructure is not the same as other types of capital stock as it often exhibits features of a natural monopoly, tends to have public good characteristics, network effects and spillovers into other sectors[8]. In the event of a disruption to a critical infrastructure system, the impacts exert influence outside the system, specifically, on society, producing negative effects on national interests such as security, the economy, and basic human needs[9]. Urbanisation and city densification[10] combined with population growth, aging, demographic and increasing wealth/middle-class are leading to demand beyond design windows.

[6] Markard, J (2009) Characteristics of Infrastructure Sectors and Implications for Innovation Processes, Discussion Paper for the Workshop on Environmental Innovation in Infrastructure Sectors, Karlsruhe Sep. 29 - Oct. 1, 2009

[7] Varga, L (2014) Infrastructure, Growth and Sustainable Living*, ITRC conference: The future of national infrastructure systems & economic prospe*rity, St Catharine's College, Cambridge, 28.03.2014

[8] Égert, B., T. Kozluk and D. Sutherland (2009), "Infrastructure and Growth: Empirical Evidence", *OECD, Economics Department Working Papers*, No. 685, OECD Publishing. http://dx.doi.org/10.1787/225682848268

[9] Rehak D, Markuci J, Hromada M, Barcova, K. Quantitative evaluation of the synergistic effects of failures in a critical infrastructure system. International Journal of Critical Infrastructure Protection. 2016;14:3-17. DOI: 10.1016/j.ijcip.2016.06.002

[10] Esfahani, HS, Ramirez, MT (2003) *Journal of Development Economics* 70, 443–477

4. Sectors similar to infrastructure

A variety of sectors were considered for assessment of similarity to infrastructure. Other UK critical sectors[11] were the initial sectors: Chemicals, Defence, Emergency Services, Finance, Food, Government, Health, Space.

Next to be considered were **primary** (Materials (mining, forestry)), **secondary** (Industrials (defence, construction, manufacturing), Healthcare (biotech, medical devices), Consumer Staples (food, drink), and **tertiary** (Financials (banks, insurance, investment), Technology (electronics, IT)) stock market sectors[12].

Through a process of search for cases, and the requirement for a spread of sectors, five sectors, each with a strong case of emergent failure, were selected. Selected sectors are: Finance, Food, Healthcare, Industry and Natural systems. The sectors were evaluated, shown in Figure 2, using a scoring key from Markard (2009). Markard had previously scored various infrastructure sectors for the first five criteria in Figure 2. Given we have extended Markard's dimensions of economic infrastructure sectors (the first five criteria in Figure 2), and the scoring key was usable for both new criteria and for new sectors, we adopted Markard's key for assessment.

key: 3 very high, 2 high, 1 medium, 0 low

	Sector Criteria	Financials, banking, investment, insurance	Consumer staples (food, drink)	Healthcare	Industrials (defence, manufacturing, construction)	Natural systems
1	Capital costs	2	2	2	2	1
2	Asset Durability	2	2	2	2	3
3	Dominance of public organisations	2	3	3	3	3
4	Regulation intensity	3	2	3	2	3
5	Degree of systemness	2	2	2	2	3
6	Spill-over effects	2	2	2	2	1
7	Investment leads to variety in economic growth	2	2	2	2	1
8	Ramifications of failures	2	3	3	3	3
9	Uncontrollable demand	3	3	3	2	3
	Case study	Flash Crash	Moldova Agri-food	SARS	Car Configuration	Beached Whales

Figure 2: Five sectors comparable to infrastructure:
Finance, Food, Healthcare, Industry, Natural systems.

[11] Cabinet Office (2018) Public Summary of Sector Security and Resilience Plans

[12] https://etfdb.com/etf-education/the-10-sectors-of-the-stock-market/

5. Case studies

Searches for cases were conducted in both academic and grey literatures for case studies from sectors similar to infrastructure but not infrastructure. The search for academic articles used the Scopus database. The search string shown in Figure 3 yielded 28 results.

```
TITLE-ABS-KEY ( ( "case stud*" )
AND ( emergent OR emergence OR unexpect* OR unpredict* OR unforseen* )
AND ( failure OR compromised )
AND ( finance OR banking OR airspace OR aerospace OR pharmacy OR epidemic OR famine OR agriculture OR "foodmarket" OR stockpiling OR "perishable" OR "raw material" OR "catalytic converts" )
AND NOT ( infrastructure OR energy OR electricity OR transport OR road OR rail OR telecom OR water OR sewage ) )
AND ( LIMIT-TO ( LANGUAGE , "English" ) )
```

Figure 3: Search string for Scopus to locate cases of emergent failure

A general search in Google for “emergent failure case studies” returned 32.6 million results, and identifies a good source of example from NASA.[13]

By excluding cases where the cause of the failure is not described, i.e. all included cases can be scientifically explained; including cases where emergent failure as defined in section 2; and excluding cases on emergency or emergencies, we reduced the list to 13 cases as shown in Figure 4.

Case title	Sector
Hidden Hazards (Car Configuration)	Automotive design
Chaos and crisis: The Swiss bank case study	Banking
Methodological strategies in resilient health care studies: An integrative review	Health Sector
Storm Clouds Over Stonehenge	Defence
Pushing the Envelope of Flight Test Safety	Aeroplane testing
The Poldercrash; Turkish Airlines Flight 1951	Aeroplane operations
The Collapse of Lehman Brothers: A Case Study	Finance
Iceland’s Banking Crisis	Banking operations
The 2007–2009 Financial Crisis: An Erosion of Ethics: A Case Study (finance)	Finance
Financial Failure Prediction in Banks: The Case of European Union Countries	Finance
Insurance Company Failure	Insurance
System weaknesses as contributing causes of accidents in health care	Health Sector
Overcoming supply chain failure in the agri-food sector: A case study from Moldova	Food

Figure 4: Long list of cases

[13] https://nsc.nasa.gov/resources/case-studies

Through a process of discussion and honing in on five exemplary cases, the final five cases were identified: Flash Crash (2010), Moldova Agri-Food (2003), SARS (2002), Car Configuration (2014), and Beached Whales (2009). The cases highlight a variety of system-of-systems (SoS) characteristics relevant for infrastructure:

a) A SoS weakness which arises from multiple independent and automated system interactions
b) An automated system can be disrupted by unplanned human intervention and can experience rapid failure
c) Systems that work in one social context may fail in another; the social environment is an important part of determining the success of a system
d) Geographical spread of failure arises from tightly coupled and connected systems
e) Information sharing and communication which leads to swift action can reduce escalation and contagion
f) Sub-optimal, albeit working, systems may may lead to unwanted effects in the wider system
g) Large numbers of small failures are comparable to single large system failures
h) The magnitude of the failure will be context dependent

The headings for the case study template were agreed with NIC to include: Title, Summary With Key Points, The Events During The Failure, Background, Emergent Behaviour, Causes Of The Emergent Failure, Insights For Infrastructure, and References. The case studies appear on the following pages.

TITLE

2010 Flash Crash

SUMMARY

Sector: Finance, Stock Market

Emergent failure: Very fast and escalating failure/crash of a system stuck in a vicious positive feedback loop, with no ability to estimate the specific effects of the failure.

Interactions that caused failure: the detailed interactions of the automated transactions and their associated algorithms, caused an unexpected market scale failure. The behaviour of a single trader's activity triggered the cascade of interactions, but the interactions of the algorithms created the emergent behaviour.

Consequences: biggest stock market drop in the shortest period ever ($1tr in 10 minutes) and only around 70% was recovered.

Insight for infrastructure: latent (dormant) system failures may be introduced through automation and the interaction of many independent systems, and triggered by unplanned for human action; evidence on causation may be impossible to collect without monitoring and recording mechanisms.

THE EVENTS DURING THE FAILURE

On 6th May 2010, the United States trillion-dollar stock market crashed. Dubbed the Flash Crash, it started at 2:32 p.m. EDT and lasted for approximately 36 minutes. The Flash Crash featured the biggest one-day point decline (998.5 points) in the history of the Dow Jones Industrial Average (DJIA). The DJIA index dropped over 1000 points in just 10 minutes, which was the biggest drop of its kind on record at the time. Futures were also affected, with the price of the E-mini S&P 500 futures collapsing by 5% between 2:30pm and 2:45pm, on top of the 2.97% it had already retreated intraday.

This price drop was accompanied by an unusually large volume of transactions. Between 2:30pm and 3:00pm, in excess of 1.1 million contracts were exchanged in E-mini S&P 500 June 2010 futures alone. Across both futures and equity markets, "there was a complete evaporation of liquidity in the marketplace". While US indices dropped by as much as 10%, some individual stocks plunged by much larger amounts. Overall, the Flash Crash is thought to have wiped off $1 trillion in equity. While the DJIA recovered, it only managed to regain about 70% of the lost value by the end of the day – demonstrating the severe impact these events can have.

BACKGROUND

The primary contributing factors to the Flash Crash were high frequency and speed of trades by computer generated algorithms, along with high degree of coupling between the components of the system. These high frequency trades are powered by a technical development called quantitative trading in which "Quant analysts" use mathematical algorithms in computer programs to trade stocks. Sophisticated investment and hedge funds with thousands of computers are programmed to sell when certain events occurred. Program trading has grown to the point where it's replaced individual investors.

Different things can trigger a failure, **but computer trading programs make any crash worse.** These "bots" use algorithms that recognize aberrations, such as sell orders. They automatically react by selling their holdings to avoid further losses. When a world event, or a computer glitch, tell these programs that something unusual is happening, they automatically sell according to their code. These trading programs make any stock movement more intense, thus adding risk.

EMERGENT BEHAVIOUR

Vicious and very fast positive feedback resulted from automated, independent systems acting as expected and responding to systemic information. The system of systems (the stock market) had no means to detect spoof activity and trusted the information from independent trades.

In today's electronic financial markets, an electronic trader can execute more than 1000 trades in a single second. The actions of a multitude of human traders and automated trading systems at the micro-level cause the valuation of assets at the macro level which in turn influences the actions of the human traders and the algorithms of the automated trading systems, thus forming causal loops and cascade effects that can result in emergent misbehaviour.

Flash crashes are a systemic feature, the consequence of the interaction of system components. They are desirable if they reflect legitimate micro trades, and indeed we see mini crashes (and surges) all the time as stock prices oscillate based on buyer and seller behaviour.

However, the degree to which the stock market, or system of stock markets, can detect, contain and protect itself from rogue trades, which have the potential for unwarranted damage, is ambiguous. Loose coupling or verification of suspect trades may provide ways to avoid future spoofed crashes.

CAUSES OF THE EMERGENT FAILURE

On April 21, 2015, nearly five years after the incident, the U.S. Department of Justice laid "22 criminal counts, including fraud and market manipulation" against Navinder Singh Sarao, a trader. Among the charges included was **the use of spoofing algorithms**. Just prior to the Flash Crash, he placed orders for thousands of E-mini S&P 500 stock index futures contracts which he planned on cancelling later. These orders amounting to about "$200 million worth of bets that the market would fall" were "replaced or modified 19,000 times" before they were cancelled.

Attempts to manipulate the market through an illegal method known as 'spoofing' (sometimes also known as 'dynamic layering') occurs when someone places large sell orders at a price far from the current market value and then quickly cancels them before the security hits that price. This gives the illusion that there is a large sell-off happening and prompts others to begin selling too in fear the price will decline.

And the rapid decline in price triggered large numbers of automated trading to take place as prices broke through pre-determined thresholds. As the majority of trading is done through automated programs, most high frequency traders end up trading with other high frequency traders, all of which have their own orders and limits in place. This means when those high frequency trading orders were triggered by Sarao's fraudulent sell orders, it went on to trigger orders from other high frequency traders – **causing a downward spiral.**

The person that placed the initial sell order also has orders to buy the same security at a value much less than the market value but cancels the order to sell the security before the security hits the price that would execute it. This means they can then buy the security at the bottom of the flash crash and sell it at a considerably higher price after it recovers – potentially allowing huge profits to be made in seconds.

The CFTC-SEC Staff Report on the market events of May 6 identifies **automated execution of a large sell order in the E-mini contract as precipitating the actual crash.** What then followed was "two liquidity crises – one at the broad index level in the E-mini, the other with respect to individual stocks." This generalized severe mismatch in liquidity was exacerbated by the withdrawal of liquidity by some electronic market makers and by **uncertainty about, or delays in, market data affecting the actions of market participants**.

Traders Magazine journalist, John Bates, argued that blaming a 36-year-old small-time trader who worked from his parents' modest stucco house in suburban area for sparking a trillion-dollar stock market crash is "a little bit like blaming lightning for starting a fire" and that the investigation was lengthened because regulators used "bicycles to try and catch Ferraris." Furthermore, he concluded that by April 2015, traders can still manipulate and impact markets in spite of regulators and banks' new, improved monitoring of automated trade systems.

A system weakness, the capacity for flash crashes, was exposed by human intervention. Sometimes human error plays its role with previous crashes being caused by accidental trading, when a trader or fund manager has unintentionally added an extra zero to their order or made an order at the wrong price, often referred to as a 'fat-finger' mistake.

INSIGHTS FOR INFRASTRUCTURE

Automation plays a significant role in infrastructure and most infrastructure services are provided through high speed computer algorithms, such as telecommunication services and smart transportation. Infrastructure operators cannot assume 'all is known' because **the timing, speed and severity of failures arising from multiple independent and automated system interactions, is unknowable.**

Human action, both the potential for mistakes and for malicious action, can trigger positive feedbacks in automated systems. Components, created by different developers may operate in unexpected ways, not necessarily due to poor design or implementation, but because of inappropriate use or context. A component may respond correctly to an interaction, but the consequence of the interaction may trigger a cascade of interactions leading to massive failure.

The Flash Crash raises difficult, policy-relevant questions of causation. As is the case with most market events, the circumstances of the Flash Crash cannot be reconstructed because a **detailed record of the precise temporal order of all relevant events is not available**. This "Flash Crash" occurred in the absence of fundamental news that could explain the observed price pattern and is generally viewed as the result of endogenous factors related to the complexity of modern equity market trading. Digital twins, or other means of collecting evidence trails through monitoring and recording, may provide insight into causation, for example via scenario modelling to examine the limits of system behaviours.

REFERENCES

2010 flash crash; https://en.wikipedia.org/wiki/2010_flash_crash

Easley, D., De Prado, M.M.L. and O'Hara, M., 2011. The microstructure of the "flash crash": flow toxicity, liquidity crashes, and the probability of informed trading. The Journal of Portfolio Management, 37(2), pp.118-128.

Flash Crashes Explained; https://www.ig.com/us/trading-strategies/flash-crashes-explained-190503

Flash Crash Explained With Examples; https://www.thebalance.com/what-is-a-flash-crash-3306184

Kopetz, H., Bondavalli, A., Brancati, F., Frömel, B., Höftberger, O. and Iacob, S., 2016. Emergence in Cyber-Physical Systems-of-Systems (CPSoSs). In Cyber-Physical Systems of Systems (pp. 73-96). Springer, Cham.

Rainey, L. B., Jamshidi, M. 2018. Engineering Emergence: A Modeling and Simulation Approach; ISBN 9781138046160

Stock Market Crash, Its Causes, Effects, and How to Protect Yourself; https://www.thebalance.com/stock-market-crash-examples-cause-impact-3305864

Vinerbi, L., Bondavalli, A. and Lollini, P., 2010, July. Emergence: A new source of failures in complex systems. In 2010 Third International Conference on Dependability (pp. 133-138). IEEE.

TITLE

Moldova Agri-Food

SUMMARY

Sector: Agri-Food (milk supply chain)

Emergent failure: socio-economic regime change can bring down an entire supply chain system of systems when it challenges the viability of one of the systems.

Interactions that caused failure: transition from centrally planned to more market based economies in Central and Eastern Europe, led to land reform, food industry privatization, change in agricultural structures and asymmetric information between farmers and food processors.

Consequences: food processors could no longer operate a viable (quantity and quality) milk processing system leading to whole supply chain failure.

Insight for infrastructure: don't expect legacy systems to work in a new social context; transformational change may require more information to be shared; control and monitoring major upheaval to governance and regulation contexts is needed for systems to operate; expect to provide sufficient information and/or get feedback early on how existing incentives work.

THE EVENTS DURING THE FAILURE

The milk supply chain collapsed after over a decade of increasingly lower productivity and lower quality of milk. A restructuring of ownership of agricultural land, driven by privatisation, had created an increasingly large population of small dairy farmers in rural households. The inability of food processors and rural households to sustain milk production created fragmentation and ultimately failure of the milk supply chain.

The dairy sector was an important source of income for rural households. Milk was procured by collecting stations. Many issues arose. Firstly, such milk tended to have high total bacterial counts caused by contamination (dirty equipment, lack of mastitis control measures) and the absence of adequate cooling and cold storage facilities. Secondly, transaction costs were high as lots of small payments were made to a large number of actors. Thirdly, the output from small-scale producers was highly seasonal, so dairy collection would be highly erratic. Finally, many collecting stations in the Former Soviet Union (FSU) were poorly equipped to monitor the quality of milk purchased allowing small privatised dairies to sell poor quality milk. This led to asymmetric information between buyers and sellers regarding product quality. The costs of monitoring milk quality to avoid market failure from adverse selection were significant.

BACKGROUND

In 1990 most states in Central and Eastern Europe and the FSU embarked on the privatisation of formal agri-food channels. During the 1990s much of Moldova's agricultural land was transferred from state to private ownership. Over 1 million landowners were created by 2003 managing individual plots of 1.4 ha and further sub-divided into separate plots based on land type (arable, orchard, and vineyard).

In the dairy sector this resulted in the break-up of most of the large livestock herds managed by the state and collective farms that previously supplied state-owned dairy processors. Preventing small-scale producers being marginalised from dairy supply chains was an important factor in safeguarding and improving rural livelihoods.

These reforms have meant that in Moldova there were two main types of milk producer: (a) relatively large private corporate farms and (b) rural households. Corporate farms sold directly to dairies while rural households, where they market their output, sell at village collecting stations. The corporate farms, despite having their origin in the former collectivised farms, operated on a smaller scale than the latter did in the FSU.

A large drop in milk production in the region was witnessed: from 1.5 (1991) to 0.6 (2003) million tonnes. Over the same time period the output of corporate farms (the collective farms and their successors) fell from 1.23

million tonnes to 34,000 tonnes, whilst household output doubled (.28 to .56 million tonnes). The drop in milk production reflected decreasing productivity: cow numbers reduced by 30% yet production reduced by 60%.

Slightly greater than 40% of rural households were engaged in milk production but the vast majority of these (81.7%) had just one cow. Only 12 households had more than five cows with largest herd size being 8. Households with 5 or more cows accounted for less than 0.5% of the total animal stock.

In many cases it was not possible to use these small plots efficiently. It reduced the extent of large scale mechanisation for food production. After privatisation the pattern of animal ownership was highly fragmented and there were very few organised animal based production units. 97% of milk was produced by smallholders with less than 5 cows, and milked by hand. As a result, a large drop in milk production in the region was witnessed.

EMERGENT BEHAVIOUR

Changes in agrarian structures (to a dual structure with a limited number of relatively large private corporate farms, and a large number of small-scale individual farms) **had a profound unexpected effect on the operational viability of food processors.**

Supply chain fragmentation occurred for food processors due to lack of supply as milk markets became subject to problems of adverse selection between good quality and bad quality milk that was sold by households. The dual agrarian structure could not develop successful relationships to exploit the inherent competitive advantages that many states appear to possess for some agricultural commodities.

An expected outcome of the post-privatization phase was that private landownership and secure property rights would promote an accelerated transfer of land from less efficient to more efficient producers or, more precisely, from passive landowners operating collectivised agricultural enterprises to energetic active operators. And it was **expected to lead to a more efficient and competitive agricultural sector, but it had a completely opposite effect.**

The collapse in output (milk quantity) was triggered by the disbandment of the sovkhozi and kolkhozi which were formal supply channels characterised by a high degree of vertical co-ordination, managed by central planners and linked large state (sovkhoz) and collective (kolkhoz) farms with state-owned food processing plants (kombinats) and retail co-operative and distribution systems.

Emergent behaviour of milk producers was: a lack of engagement with the new privatisation regime which meant they largely reduced their milk supply activity; and a reduction in quality of milk due to a lack of incentives in the new regime to continue to provide high quality product: quality was not checked so the cost to maintain high quality of milk could be avoided.

CAUSES OF THE EMERGENT FAILURE

A number of external parallel independent factors acted as triggers for the changes to agri-food production. The transition from centrally planned to more market based economies in Central and Eastern Europe, the disruption caused by land reform and privatisation programs, the greater international contestability of markets, a fall in real protection, a cost-price squeeze, supply chain disruption.

Supply chain disruption, with a high level of asymmetric information between farmers and processors led to market (food market/dairy) failure.

INSIGHTS FOR INFRASTRUCTURE

The agri-food industry in this case is similar to infrastructure in terms of delivering critical services, and ramifications of failure.

Quality of services and products are very important in both agri-food and infrastructure systems, and people's lives can be severely affected by poor quality products or services. Collaboration and cooperation both up and down stream between various players in the supply chain is critical to address public and private sector integration.

When a social context change occurs, a System of systems (SoS) approach should be taken to appraise the impact of change on different aspects. This would identify contextual considerations, allowing policies and existing mechanisms in related areas to become known.

When regime change is necessary, for example, on train timetables, **sufficient information is needed for everyone in the supply chain**. Early feedback on challenges to the implementation of a new regime would identify issues more quickly and provide evidence for decision making.

Changes to infrastructure benefit from an **understanding of the behaviour of the actors in the system and the incentives they act under**.

REFERENCES

Cimpoies, L., 2015. The potential of Moldovan agri-food products on EU markets. Rural Areas and Development, 12(740-2019-3057), pp.21-33.

FAO. Republic of Moldova to boost agrifood promotion, improve data collection; http://www.fao.org/europe/news/detail-news/en/c/1203376/

Gorton, M., Dumitrashko, M. and White, J., 2006. Overcoming supply chain failure in the agri-food sector: A case study from Moldova. Food Policy, 31(1), pp.90-103.

Millns, J., 2013. Agriculture and rural cooperation examples from Armenia, Georgia and Moldova. Policy Studies on Rural Transition, (2013-2).

Newcastle University. Research Challenge: Integrated Infrastructure Systems; https://www.ncl.ac.uk/media/wwwnclacuk/instituteforsustainability/files/IIS.pdf

Spoor, M. and Izman, F., 2008. Land reform and interlocking agricultural markets in Moldova. In The Political Economy of Rural Livelihoods in Transition Economies (pp. 111-134). Routledge.

Stratan, A., Moroz, V. and Ignat, A., 2014. Modernization of the agri-food sector of the Republic of Moldova in the context of international trade development. In Agrarian Economy and Rural Development-Realities and Perspectives for Romania. 5th Edition of the International Symposium (pp. 55-60). Bucharest: The Research Institute for Agricultural Economy and Rural Development (ICEADR).

TITLE

Severe acute respiratory syndrome: SARS

SUMMARY

Sector: Health Sector, SARS Epidemic

Emergent failure: scale and pattern of progression unpredictable and so emergent.

Interactions that caused failure: Human contact with virus infected mammals or their faeces, and person to person contamination through sneezing or coughing. Symptoms arise only after incubation, so the infected person may travel and spread the virus into new places unknowingly; context is modern society.

Consequences: SARS pandemics (2002, 2004) with 774 deaths (8,098 reported cases) causing large social and economic effects through restricted movement, whilst the contagion is brought under control. Viruses are continuously mutating; it is normal and expected behaviour.

Insight for infrastructure: infrastructure networks provide channels to distribute people and things. If one or more parts of a tightly coupled network become infected, the infection needs early diagnosis, containment and purging. Contaminated water can be spread geographically over a large area; IT viruses can be spread over telecoms networks. Information sharing and communication are considered key tools for the coordination of prevention and management of unexpected outbreaks.

THE EVENTS DURING THE FAILURE

Between November 2002 and July 2003, an outbreak of SARS in southern China spread from Hong Kong to individuals in 37 countries. Because of the contagious nature of the disease and the delayed public-health response, the epidemic spread rapidly around the globe.

The SARS epidemic was not simply a public health problem. Indeed, it caused the most severe socio-political crisis for the Chinese leadership since the 1989 Tiananmen crackdown. Outbreak of the disease fuelled fears among economists that China's economy was headed for a serious downturn.

A fatal period of hesitation regarding information-sharing and action spawned anxiety, panic, and rumour-mongering across the country and undermined the government's efforts to create a milder image of itself in the international arena. As Premier Wen Jiabao pointed out in a cabinet meeting on the epidemic, "the health and security of the people, overall state of reform, development, and stability, and China's national interest and international image are at stake (Zhongguo xinwen wang, 2003a)." The illness developed into an epidemic in Hong Kong, which proved to be a major international transit route for SARS.

Health Effects: The SARS outbreak infected thousands of people, causing widespread serious illness across a large population and many deaths. The psychological impact of SARS was also very serious. Studies show that the SARS outbreak also fostered negative impacts on people's mental health.

Social Impacts: SARS caused a very large impact on society, particularly in China. During the early period of the SARS outbreak, tension surged in the community. Due to a lack of trustworthy official information, rumours about the epidemic situation spread through word of mouth, mobile phone short messages, social media transmission, and other ways. The spread of misunderstandings exacerbated social panic, reflected in an escalation of panic buying of drugs in Guangdong province.

Economic Impacts: It was estimated that Asian states lost USD 12–18 billion as the SARS crisis depressed travel, tourism, and retail sales. SARS had a large impact on tourism and its related industries, and due to the spread of SARS, population movement in China and many counties decreased. Families reduced their demand for food, clothes, travel, and entertainment, and the numbers of guests in hotels declined sharply.

BACKGROUND

SARS-CoV likely originated in wild bats and then spread to palm civets or similar mammals. The virus then mutated and adapted itself in these animals until it eventually infected humans. There was ample opportunity for the virus to come into contact with humans. Bats serve as a food source in parts of Asia, and sometimes used in folk medicines. The virus may have spread directly or indirectly through animals held in Chinese markets.

Civets are cat-like mammals that live in the tropics of Africa and Asia and produce musk from their scent glands, which is used in perfumes. Civets are also hunted for meat in some parts of the world. These animals could easily transmit the virus to humans.

When someone with SARS coughs or sneezes, infected droplets spray into the air. Breathing in or touching these particles transmits the virus. The SARS virus may live on hands, tissues, and other surfaces for up to several hours in these droplets. The virus may be able to live for months or years when the temperature is below freezing. Airborne transmission is a real possibility in some cases. Live viruses has even been found in the stools of people with SARS, where it has been shown to live for up to 4 days.

Symptoms mostly occur about 2 to 10 days after coming in contact with the virus. People with active symptoms of illness are contagious. But it is not known for how long a person may be contagious before or after symptoms appear.

EMERGENT BEHAVIOUR

Behaviour at all scales was such that it denied what was clearly being observed. Actual behaviour was therefore emergent, irrational, and contrary to reasonable expectations of citizens.

When first SARS patients were admitted to hospitals in Beijing and Inner Mongolia, doctors could not correctly diagnose the illness with only little information about the disease. Even as the traffic through emergency rooms began to escalate, major hospitals in Beijing took **few measures to reduce the chances of cross-infection**.

The unknown disease, originating in Guangdong province, was characterized by high fever, severe respiratory symptoms, and death. SARS had not been reported in humans before 2002. Health officials requested expert support, but their **report was marked "top secret," a security designation which prevented health authorities receiving information about the disease**, and consequently they were denied the knowledge they needed to prepare.

The initial **failure to inform the public** heightened anxieties, fear, and widespread speculation. In fact, there were media blackouts and a slow government response but there was little knowledge about the true cause of the disease and its rate and modes of transmission. The top-secret document did not even mention that the disease showed signs of being considerably contagious. Neither did it call for rigorous preventive measures. Through contagion, many victims were health care workers.

CAUSES OF THE EMERGENT FAILURE

There is no doubt that government inaction paralleled by the absence of an effective response to the initial outbreak resulted in the crisis.

Organizational barriers delayed the process of correctly **identifying the cause of the disease** including obstructions to information flow and the lack of interdepartmental cooperation during the crisis.

Government reaction to the emerging disease, was delayed by the problems of **information flow within the Chinese hierarchy** because of staff availability and 'Chinese new year' holidays. Furthermore, legislation prevented any physician or journalist reporting on the disease due to risk of being persecuted for leaking state secrets.

The continuing news blackout **restricted the flow of information to the public which should could have reduced the spread of contagion.**

The Law on Prevention and Treatment of Infectious Diseases contains a number of significant loopholes that disincentivise the government from effectively responding: including that atypical pneumonia is not listed as an infectious disease, and no procedures to add new diseases.

Other regulations **hampered cooperation between China and the World Health Organization:** only the Chinese CDC can be the legal holder of virus samples and attempts to get samples by other means were thwarted. Even the Chinese CDC in Beijing had to negotiate with local disease-control centres to obtain the samples.

INSIGHTS FOR INFRASTRUCTURE

In both health sector and infrastructure, outbreaks can have wide social and economic impacts, and political issues are involved in decision making when managing an outbreak.

SARS, in particular, highlighted that connected networks create the possibility of problems spreading geographically. Randomness and limited information means that they can spread in unpredictable ways. Infrastructure systems are **tightly coupled and connected,** the parallels between the SARs system and infrastructure systems means that it is possible that this risk of geographical spread can occur.

The **response to an outbreak should be swift and appropriately transparent to avoid escalation and contagion**. An effective and efficient emergency response can reduce avoidable spreads and reduce the economic, social, and security impacts of all outbreaks.

The effectiveness of emergency preparedness and responses is highly dependent on the quality and amount of information that is available at any given time, and quality communication and coordination among partners is crucial. **Information sharing and communication** are considered key tools for the coordination of prevention and management of unexpected outbreaks.

REFERENCES

Cooper, K. China coronavirus: The lessons learned from the Sars outbreak https://www.bbc.co.uk/news/world-asia-china-51221394

Gompf , S.G. Severe acute respiratory syndrome (SARS) https://medlineplus.gov/ency/article/007192.htm

Huang, Y., 2004. The SARS epidemic and its aftermath in China: a political perspective. Learning from SARS: Preparing for the next disease outbreak, pp.116-36.

Institute for Sustainability, Research Challenge: Integrated Infrastructure Systems https://www.ncl.ac.uk/media/wwwnclacuk/instituteforsustainability/files/IIS.pdf

Medicinenet, Severe Acute Respiratory Syndrome (SARS) https://www.medicinenet.com/severe_acute_respiratory_syndrome_sars/article.htm

Qiu, W., Chu, C., Mao, A. and Wu, J., 2018. The Impacts on Health, Society, and Economy of SARS and H7N9 Outbreaks in China: A Case Comparison Study. Journal of environmental and public health, 2018.

Response to SARS-Like Virus an Improvement Over 2003 Outbreak https://abcnews.go.com/blogs/health/2012/09/25/response-to-sars-like-virus-an-improvement-over-2003-outbreak

Reuters, The shadow of SARS: China learned the hard way how to handle an epidemic; https://www.reuters.com/article/us-china-health-sars/the-shadow-of-sars-china-learned-the-hard-way-how-to-handle-an-epidemic-idUSKBN1ZL12B

ScienceDirect data base for Severe Acute Respiratory Syndrome (SARS); https://www.sciencedirect.com/topics/medicine-and-dentistry/severe-acute-respiratory-syndrome

TITLE

Car Configuration

SUMMARY

Sector: Industry, Manufacturing, Design

Emergent failure: Unexpected and unexplored interactions: In this case, components functional dependencies impact on the system was not diagnosed for a long time. Functional dependencies might be clear or easy to be identified but dependencies impact on the system is not obvious and needs more analysis and consideration.

Interactions that caused failure: People using poorly configured system (Sensing Diagnostic Module (SDM) and Airbag System depended on the Ignition Switch positions and components), ignition switch fault created an airbag deployment problem; aggregated impact of faulty switch; focus on technical design rather than system use.

Consequences: isolated but avoidable injuries and death (include near misses, and the stalled cars also having potential for further accidents).

Insight for infrastructure: A System of Systems (SoS) approach is essential: to understand vulnerabilities created through coupling and interactions; to consider the effects of sub-optimal components; to recognise the true scale of system failure; and to understand failure in terms of the dependency on adverse contexts.

THE EVENTS DURING THE FAILURE

In March 2010, a 29-year-old shift nurse left her job in Atlanta, Georgia and headed to her boyfriend's house. She was driving her 2005 Chevy Cobalt on a two-lane road as she approached a half-mile downhill straight. As the road leveled after the straight, she approached an area where some rainwater had accumulated. Shortly after encountering this section of roadway, she apparently lost control of her Cobalt as it hydroplaned across the centre line. The rear passenger side of her car was struck by an oncoming Ford Focus, causing the Cobalt to spin off the road and fall 15 feet before landing in a large creek around 7:30 p.m. The impact of the crash broke the nurse's neck, an injury that led to her death shortly after she arrived at the hospital.

While this tragedy might sound like a typical crash scenario, it was particularly puzzling to the victim's parents. Her parents pushed for a detailed investigation but sadly, this unsettling question remained unanswered until several years later—after many more drivers suffered similar fates.

BACKGROUND

In March 2014, law firm Jenner & Block LLP was commissioned by GM to investigate over a decade of operational issues with an ignition switch used in several GM vehicles, including the Chevy Cobalt. According to the firm's Valukas report, drivers had problems with the ignition switch slipping out of position, stalling engines and cutting power to vehicle systems. In many cases, the stalling would disable the vehicle's airbags just as the car was about to crash. In April 2017, Forbes reported that the ignition switch had been associated with 124 deaths and 275 injuries. Since the initial product recall in February 2014, GM has recalled 30 million vehicles and paid over $2 billion in fines, penalties and settlements.

Aside from the ignition switch's technical problems, the Valukas report identified several social (organizational) issues involving the relationship between GM's management and its engineering teams. These fundamental problems are not unique to GM. Any large, complex organization is vulnerable to poor communication and oversight.

During 2003–2004 customers had complained to GM about start and stalling issues. According to the Valukas report, the large volume of starter complaints caused GM to focus on fixing the ignition switch's starting issues instead of addressing the stalling issues. The report revealed that GM engineers considered the stalling problem to be a version of the starting problem.

However, the stalling issue was a completely different problem with the ignition switch. GM classified the moving stall as a non-safety issue. During March 2005 various GM committees considered possible fixes for the ignition switch problem. However, they rejected them as "too costly," since the ignition switch stalling issue was not deemed a safety concern. GM closed the initial safety investigation regarding the stalling issue without taking action. None of the stalling complaints received adequate attention and they both stayed unsolved as they have been considered as a "convenience" issue rather than a "safety" issue. The impact of stalling failures on airbag functioning was not diagnosed.

EMERGENT BEHAVIOUR

Functional interdependency of components (airbag and ignition switch) in a vehicle resulted in the safety system not being deployed and severe accidents to arise.

Suboptimal performance of the ignition switch is exposed during driving by the proximity of the driver's knee which causes the engine to stall and disables the airbag. Poor technical design is exposed during operational use.

The failure is emergent: it is a result of unexpected and unexplored interactions in the technical configuration of an engineered system and is triggered by unintended user behaviour. The consequences are non-linear and severe (death and serious injury) but not quantifiable as the context in which the car stalls (e.g. at speed, or where the car cannot safely stop) are very varied.

It took a long time to diagnose during which many were killed and seriously injured. This is because of a second issue with the ignition switch which appeared more critical.

The ignition switch did not meet the mechanical specifications for torque and required less force to turn the key than its designers originally ordered. If the driver's knee hit the key fob, the car would often turn off, causing stalling at highway speeds and disabling the airbags. See Figure 1.

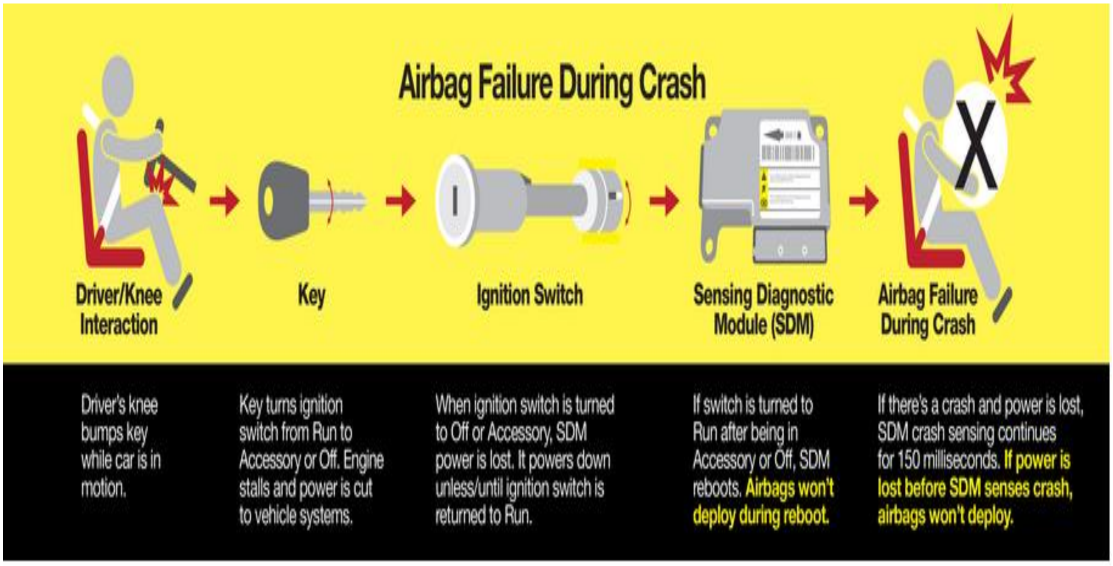

Figure 1: Chain of events leading to airbag failure during a car crash (Source: NASA Safety Centre)

Additional factors in the failure:

Organisation failure: people behaved in unexpected ways. The acceptance of "quality escapes" (non-conformance to specifications) and a lack of use of Systems Engineering and Integration (SE&I) principles prevented effective hazard communication. The organizational structure had no formal integrative roles and responsibilities that could have identified the hazards.

The technical system was sub-optimal; the management system was sub-optimal as well. Interaction of sub-optimal design systems, as well as interaction of sub-optimal design system and management systems lead to the failures of a system of systems (SoS).

The bottom line is that a significant communication breakdown allowed the core technical issue involving the ignition switch and airbags to be concealed from anyone with technical oversight until 2013. Poor communication was responsible for partially blocking the flow of information throughout GM, affecting management's interpretation of the information.

CAUSES OF THE EMERGENT FAILURE

In addition to technical problems, the systemic failure was allowed to persist because of lack of understanding of the problem, inadequate communication, lack of urgency, lack of oversight, and company culture.

Technical Problem

The ignition system was acting only sub-optimally, but not completely failing. However, this did lead to a whole system failure. In fact, the ignition switch did not meet the mechanical specifications for torque and required less force to turn the key than its designers originally ordered. If the driver's knee hit the key fob, the car would often turn off, causing stalling at highway speeds and disabling the airbags.

Lack of Understanding of the Problem

For many years, GM personnel did not fully understand the primary safety issue related to the ignition switch. GM engineers on committees did not associate turning the key to Accessory or Off with disabling the airbags.

Further, the individuals involved in the initial investigation did not know the appropriate questions to ask to understand the technical problem. The information that was available regarding complaints, negative reviews and fatalities was not readily shared with all levels of the company.

Inadequate Communication

GM had no organizational arrangement in place to question or validate the designer's decision. Plus, no organizational check was in place to verify his actions or inactions.

Interaction of System of Systems (SoS): Interaction of different technical systems as well as interaction of a technical problem and organisational culture. Aside from the ignition switch's technical problems, the Valukas report identified several organizational issues involving the relationship between GM's management and its engineering teams including structural secrecy, a lack of urgency, inadequate oversight and a company culture characterized by low accountability, contributed to the ignition switch problems.

Lack of Urgency

The Valukas report revealed a lack of urgency at many stages of the evolution and investigation of the ignition switch problem. Because of this, GM personnel classified the problem as a customer convenience issue rather than a safety issue.

INSIGHTS FOR INFRASTRUCTURE

Any large, complex organization (like those managing infrastructure) is **vulnerable to coupled functionality, interaction of different technical systems, and lapses in good communication and governance**. Therefore, a SoS approach and geographically co-located implications assessment are essential for understanding emergent failure.

System weaknesses, created by complex vulnerabilities, may be life threatening especially when component systems (such as the ignition switch) are acting sub-optimally. **Sub-optimal systems** should not be allowed to operate in infrastructure without consideration of SoS effects.

Large numbers of small system failures (e.g. lone car fatalities) should be treated as **comparable to single large system failures** (e.g. aeroplane crashes), and are equally important. Rising numbers of individual failures should be reported and actions taken to escalate. Reporting should be transparent and products withdrawn until system failures are diagnosed.

The **magnitude of each failure is dependent on the 'wrong' context** (e.g. high speed, no safe place to shelter). The SoS consequences of a component failure must be assessed for adverse contexts.

REFERENCES

Basu, T. Timeline: A History of GM's Ignition Switch Defect. NPR. March 31, 2014.

Blau, M. No Accident: Inside GM's Deadly Ignition Switch Scandal. Atlanta. Jan. 2016.

Boudette, N. Supreme Court Rebuffs GM's Bid to Limit Ignition-Switch Lawsuits. New York Times. April 24, 2017.

Klayman, B. GM Restructures Engineering to Improve Vehicle Quality, Safety. Fox Business. April 22, 2014.

Lilley, S. Hidden Hazards; Valukas Report Reveals, Social and Technical Issues Behind Faulty GM Ignition Switch: https://nsc.nasa.gov/resources/case-studies/detail/hidden-hazards

Muller, J. Supreme Court Allows Ignition-Switch Lawsuits To Proceed Against GM In Pre-Bankruptcy Crashes. Forbes. April 24, 2017.

Seeger Weiss LLP, GM Ignition Switches. https://www.consumersafetyguide.com/automotive/gm-ignition-switches/ Accessed 06 Feb 2020

Valukas, A. Report to Board of Directors of General Motors Company Regarding Ignition Switch Recalls. Jenner & Block. May 29, 2014. (redacted).

Vlasic, B. GM Settles Switch Suit, Avoiding Depositions. NY Times. March 13, 2015.

TITLE

Beached Whales

SUMMARY

Sector: Natural System

Emergent failure: group demise in unknown contexts.

Interactions that caused failure: regular behaviour, but in the wrong place.

Consequences: whole groups, shoals, flights of mammals and birds become stranded and die.

Insight for infrastructure: mass demise is possible in unknown contexts; contexts can change and may restrict the availability of resources to users that have not adapted and persist in traditional behaviours.

THE EVENTS DURING THE FAILURE

In December 2009, a pod of seven sperm whales were stranded along the coastline of the Gargano Promontory (Italy), in the Southern Adriatic Sea. Three animals were still alive but died within 48 hours after stranding.

When such mammals enter shallow waters most of them have a tendency to become disorientated. Whales are **highly social and usually travel in tight groups or pods, which is why so many of them become stranded at once**.

Sperm whales are considered to be vagrant or absent in the waters surrounding the stranding place, and particularly in the Central and Northern areas of the Adriatic Sea, where the habitat is not appropriate to this deep-diving species. Sperm whales in the Mediterranean Sea occur preferentially in deep continental slope waters where mesopelagic cephalopods are most abundant. In fact, they have been frequently encountered in the Ionian Sea, especially along the Hellenic Trench, as in the Ligurian Sea, where they mostly appear along the continental slope.

BACKGROUND

A multi-factorial cause underlying this sperm whales' mass stranding was proposed based upon the results of post-mortem investigations as well as detailed analyses of the geographical and historical background. The seven sperm whales **took the same "wrong way"** into the Adriatic Sea, a potentially dangerous trap for Mediterranean sperm whales. Seismic surveys should be also regarded as potential co-factors, even if no evidence of direct impact has been detected.

In this particular case, causes of death did not include biological agents, or the "gas and fat embolic syndrome", associated with direct sonar exposure. Environmental pollutant tissue concentrations were relatively high, in particular organochlorinated xenobiotics. Gastric content and morphologic tissue examinations showed prolonged starvation which likely caused the mobilization of lipophilic contaminants from the adipose tissue. Chemical compounds subsequently entered the blood circulation and may have impaired immune and nervous functions.

Despite all these observations, it was not possible to confirm that these stranded sperm whales formed a single stable group with a social hierarchy, although we would rather suggest that more than one loose male aggregation and/or several solitary individuals could have coalesced in a limited sea area, most likely in the Ionian Sea, between summer and fall. From there they subsequently entered the Adriatic Sea for unknown reasons. **No relevant unusual natural events** (e.g. seaquake or weather storms) **or noxious anthropogenic activities** (military drills using sonar) that could have caused an avoidance behaviour **occurred temporally and spatially associated with the event**.

The only relevant anomaly reported by the marine data archives was the increased sea superficial temperature in November and December along the Hellenic Trench and Eastern part of the Adriatic Sea, possibly constituting a thermal front in which upwelling and/or downwelling could have been favourable to the development of cephalopod populations. Several studies have documented the influence of frontal zones on sperm whale distribution worldwide. This species and other teutophageous cetaceans (e.g. dwarf and pigmy pilot whales, Risso's dolphin, and Ziphiidae) appear in places forming thermal fronts because of the aggregation of main preys near these zones. Such places include abyssal depths, at the steepest sea superficial temperature gradients, at the periphery of a cyclone zone and in convergence zones.

The “Hellenic Trench”, the likely winter aggregation area, is 600 km (Lefkada Island) to 1100 km (Crete) away from the stranding site (distance calculated on a straight way with no deviation due to marine currents). Considering the maximum horizontal speed reported for male sperm whales (90 km/day) it took no less than 7 days for these whales to reach the Gargano Promontory.

The low quantities of highly digested squid beaks found within the gastric cavities are in open contrast with the feeding habits and daily intake typical of the species, thus suggesting a starvation period of at least 3 to 7 days, an amount of time compatible with the traveling time. Furthermore, the mild portal hepatic steatosis observed at microscopic examination, along with the real body weights of the seven animals that were lower than the expected values, further support this hypothesis.

Foreign bodies (including fishing gears and hooks, ropes, and plastic objects) were found in all the examined stomachs, with an incidence higher than those reported for other mass stranding. Nevertheless, all the objects recovered from the whale stomachs cannot be proposed as a likely cause of stranding, given the absence of any evident obstructions.

EMERGENT BEHAVIOUR

A group of sperm whales, **acting normally in their search for food or possibly to avoid one or more human or natural disturbances, entered an unsafe marine area.** The cetaceans swam northward toward a dead end and soon found themselves starving. These animals took the same wrong way that already lead five other sperm whale pods to strand along the Adriatic Sea coastline in the past.

Prolonged starvation, environmental conditions improper for the species, along with breakdown of adipose body reserves and the consequent release into the bloodstream of chemical substances likely displaying neurotoxic and immunotoxic effects, altered the orientation and space perception of the whales, worsening their welfare and health. Prevailing meteorological conditions finally led the cetaceans to strand on the Gargano Promontory.

CAUSES OF THE EMERGENT FAILURE

Mass stranding of sperm whales remain peculiar and rather unexplained events, which rarely occur in the Mediterranean Sea. Solar cycles and related changes in the geomagnetic field, variations in water temperature and weather conditions, coast geographical features and human activities have been proposed as possible causes.

Other hypotheses have been considered and analysed, including natural factors, such as biologic disease agents; impairment of the navigation and echo-location systems due to bathymetric features, acoustic dead zones or anomalies of the Earth's geomagnetic field due to solar activity; the effects of lunar cycles; meteorological and oceanographic factors like local disturbances or basin-related temperature variations influencing prey distribution and large-scale climatic events.

Furthermore, anthropogenic factors like noise pollution or environmental contaminants have been also proposed as possible causes of stranding. A strong social component, which may prompt healthy animals to follow sick or disordered members of a pod, has been also considered as an additional relevant feature to be pondered in investigating the causes of mass stranding. Mass mortalities involving sperm whales are usually clustered in determined geographical areas, such as the North Sea and in the Southern Australian and New Zealand waters.

The morphology of the stranding location and the meteorological conditions registered during the days before the event (winds, currents and waves directed to the Gargano coasts) could explain why the seven sperm whales arrived on their stranding and beaching destination. Preliminary observations, in particular the distribution and the position related to the coastline, suggested that all animals were debilitated, possibly by a common pathological condition. The presence of copepods of the genus Pennella, that affected the skin of the seven whales, has been suggested as a reliable indicator of poor health in free-ranging cetacean populations.

INSIGHTS FOR INFRASTRUCTURE

Infrastructure systems are similar to natural systems in terms of the **potential scale of ramification of failure in diverse co-located groups which may be starved of resources**. Social and economic groups exposed to shortages in infrastructure services are especially vulnerable.

An example of new demand in transport systems is the introduction of connected autonomous vehicles (CAV). CAV promises to reduce road accidents, traffic congestion, traffic pollution and energy use, as well as to increase productivity, comfort and accessibility. However, the diversity of road infrastructure and connectivities to other modes of transport, were not designed for CAV and as the diffusion of CAV increases, it will create unknown and uncertain demand on aging infrastructure. Even the assumptions in CAV and the embedded machine learning which decides how the autonomous car will behave will be based on the driving contexts that it was trained on. The implications are that CAV **may expect the context to provide things not available in it, furthermore, the context may starve other groups, such as conventional users.**

The Beached Whales case demonstrates the risks of moving into **resource-poor contexts**, but similar risks arise when users do not adapt to changing context. Indeed, infrastructure change is a norm responding to climate change, globalisation, technology churn, continuous productivity improvement, etc.

An example of a changing context is the need to improve the UK's digital infrastructure as an essential prerequisite for the uptake of connected vehicles. Four key challenges related to connectivity will shape the speed and breadth of connected vehicles deployment in the UK: coverage, reliability, bandwidth and capacity. Ubiquitous coverage is the automotive industry's top priority, and the NIC recommend connectivity by 2025 of all motorways which carry 21% of all vehicle traffic, although being only 1% of the total UK road network length. Safe transitions and seamless communication between different environments is required for CAV. Vehicle manufacturers need to invest in technology and design that will exploit digital infrastructure way ahead of anticipated 5G roll-out.

REFERENCES

Alonso Raposo, M., Ciuffo, B., Makridis, M. and Thiel, C., 2017. The r-evolution of driving: from connected vehicles to coordinated automated road transport (C-ART). Part I: Framework for a safe & efficient Coordinated Automated Road Transport (C-ART) system, EUR, 28575.

Cetacean stranding; https://en.wikipedia.org/wiki/Cetacean_stranding

Iceland pilot whales: Dozens of dead mammals found beached; https://www.bbc.co.uk/news/world-europe-49048652

Markolf, S.A., Chester, M.V., Eisenberg, D.A., Iwaniec, D.M., Davidson, C.I., Zimmerman, R., Miller, T.R., Ruddell, B.L. and Chang, H., 2018. Interdependent Infrastructure as Linked Social, Ecological, and Technological Systems (SETSs) to Address Lock-in and Enhance Resilience. Earth's Future, 6(12), pp.1638-1659.

Mazzariol, S., Di Guardo, G., Petrella, A., Marsili, L., Fossi, C.M., Leonzio, C., Zizzo, N., Vizzini, S., Gaspari, S., Pavan, G. and Podesta, M., 2011. Sometimes sperm whales (Physeter macrocephalus) cannot find their way back to the high seas: a multidisciplinary study on a mass stranding. PLoS One, 6(5).

Millbrook and RACE Develop Practical CAV Testing Infrastructure https://www.millbrook.co.uk/press-office/news/millbrook-and-race-develop-practical-cav-testing-infrastructure/

New Zealand whales: Why are so many getting stranded? https://www.bbc.co.uk/news/world-asia-46400957

National Infrastructure Commission (2016) Connected Future https://www.nic.org.uk/our-work/connected-future/

Once Again, a Massive Group of Whales Strands Itself; https://www.theatlantic.com/science/archive/2018/03/whales-mass-stranding-australia/556400/

Photos: Mass Pilot Whale Death in Snæfellsnes, West Iceland; https://grapevine.is/news/2019/07/22/mass-whale-death-snaefellsnes-iceland/

Pilot whales turned up again on a Georgia beach. 16 of them died; https://edition.cnn.com/2019/09/28/us/beached-whales-georgia-trnd/index.html

Scientists demand military sonar ban to end mass whale strandings; https://www.independent.co.uk/environment/whales-sonar-ban-military-navy-stranding-beached-canary-islands-a8752611.html

SMMT, Connected and Autonomous Vehicles https://www.smmt.co.uk/wp-content/uploads/sites/2/SMMT-CAV-position-paper-final.pdf

What Is a Beached Whale? https://www.wonderopolis.org/wonder/what-is-a-beached-whale

Why Do Whales Beach Themselves? https://www.livescience.com/32818-why-do-whales-beach-themselves-.html

6. Approaches

In order to reveal approaches for the analysis of failures, disruptions and accidents from areas comparable to infrastructure, both academic and grey literatures were examined. The search for academic articles used the Scopus database. The search string shown in Figure 5 yielded 58 results.

TITLE-ABS-KEY ((approach* OR way*)

AND (understand* OR recognis* OR "figure out" OR interpret* OR know* OR "find out")

AND (emergence OR emergent OR unexpect* OR unpredict* OR unforseen*)

AND (failure OR compromised)

AND (finance OR banking OR airspace OR aerospace OR pharmacy OR epidemic OR famine OR agriculture OR "food market" OR stockpiling OR "perishable" OR "row material" OR "catalytic converts")

AND NOT (infrastructure OR energy OR electricity OR transport OR road OR rail))

AND (LIMIT-TO (LANGUAGE , "English"))

Figure 5: Search string for Scopus to locate cases of emergent failure

A general search in Google for "(approach) AND (understand*) AND ("emergent failure") generated 5,470 results.

One of the leading results was a systematic literature review conducted by Wienen et al in 2017 which identified 63 approaches that fall into three different classes of approaches, analysis methods and models: Sequential, Epidemiological, and the Systemic[14]. **Sequential** accident models describe the accident as the end point of a string of causes. This category is called "sequential" by Hollnagel because originally, many methods restricted themselves to a sequential string of causes. However, in general, there may be several causes contributing to an incident or accident. **Epidemiological** models describe the accident as the product of the interaction among a set of entities and actors, some of which may be visible, and others invisible, similar to models of how diseases develop. A key factor in epidemiological types of analysis is the description of latent factors that contribute to the development of an unsafe act into an accident. **Systemic** accident models describe the accident as the result of the interaction within a system and between a system and its context. Feedback loops may play an important role in these models.

[14] Wienen, H.C.A., Bukhsh, F.A. Vriezekolk, E. Wieringa, R.J. (2017), Accident Analysis Methods and Models — a Systematic Literature Review, https://functionalresonance.com/onewebmedia/Accident_Analysis_Methods_and_Models_a_Systematic_Literature_Review.pdf

These classes of model can be distinguished along two dimensions: coupling and socio-technical context awareness. Sequential and Epidemiological approaches are loosely coupled, only Systemic approaches are tightly coupled. Only Sequential approaches are unaware of socio-technical context. See Figure 6.

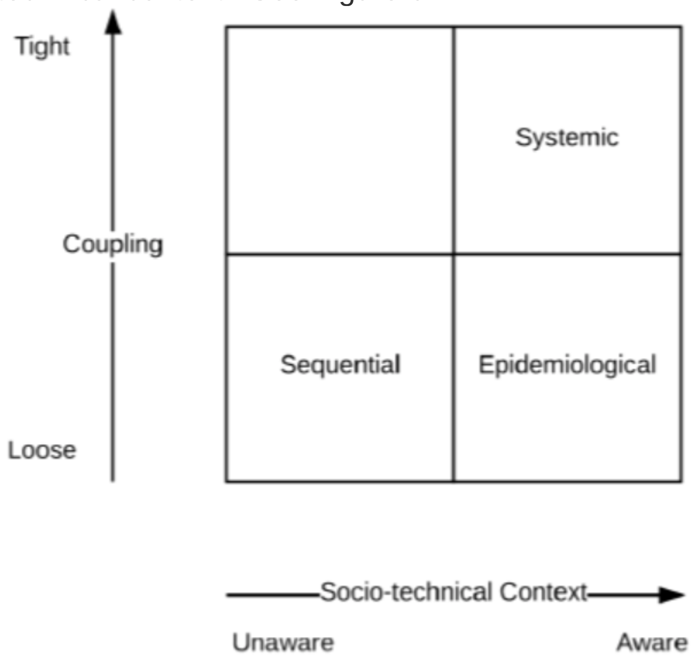

Figure 6: comparing the three classes of models along two distinguishing axes (Wienen et al, 2017)

Based on the findings from grey and academic literatures, approaches, which sufficiently met criteria in Figure 7 representing the ability of the approach to produce strategic outputs, were included in a long list of 31 approaches.

1. Conceptual Mapping, and enhanced systemic understanding, of the individual components of the System of Interest (SoI)	6. Assessment of the potential impacts on SoI performance from distribution to parts fo the SoI
2. Identification and classification of SoI internal dynamics: dependencies, interdependencies and feedback loops	7. Assessment and diagnosis of the relative criticality of potential root cause(s) of emergent failures
3. Identification and classification of dynamics between SoI and external environment	8. Assessment of the expected type, scale, intensity, duration of disruptive impacts on SoI performance associated with changes to the SoI or the external environment
4. Identify Latent Vulnerabilities where disruption to specific components or interdependencies would initiate disproportionately large impact on SoI performance	9. Assessment of the overall impacts on the systemic resilience of the SoI associated with changes to the SoI or the external environment
5. Assessment of the relative criticality of individual component performance and specific interdependencies for normal operations of the SoI	10. Assessment of incertitude within the SoI or its external environment; 11. Retrospective analysis and learning from past emergent failures

Figure 7: Criteria for approach selection

These 31 approaches were further reduced to 11 approaches which had the highest scores for strategic relevance to NIC work, based on whether the approach has been applied in at least one system with high or very high comparability to infrastructure, and has been used in cross sector applications. The 11 approaches which are included are in bold in Figure 8.

Ref	Approaches (alphabetically)	Example references (provided only for approaches *not* detailed later in this report)
1	**AcciMap**	
2	BREAM (Bridge Reliability and Error Analysis Method - Maritime)	Abujaafar (2012) Quantitative Human Reliability Assessment in Marine Engineering Operations http://researchonline.ljmu.ac.uk/id/eprint/6115/1/564142.pdf
3	Defect Elimination Techniques	Sondalini (2020) World Class Physical Asset Reliability Needs Failure Prevention, Problem Prevention and Defect Elimination Strategies https://www.lifetime-reliability.com/cms/free-articles/work-quality-assurance/defect-elimination/
4	Cognitive Systems Engineering	Hollnagel (2005) Joint Cognitive Systems: Foundations of Cognitive Systems Engineering ISBN 0-8493-2821-7
5	**Corporate Governance and Risk Management**	
6	Corporate Risk Management Framework	COSO (2017) Enterprise Risk Management https://www.coso.org/Documents/2017-COSO-ERM-Integrating-with-Strategy-and-Performance-Executive-Summary.pdf Grant Thornton (2017) Corporate risk frameworks (https://www.grantthornton.co.uk/globalassets/1.-member-firms/united-kingdom/pdf/documents/corporate-risk-frameworks.pdf
7	**CREAM (Cognitive Reliability and Error Analysis Method)**	
8	Crisis Prone Organisation Theory	Pearson & Mitroff (1993) From crisis prone to crisis prepared: a framework for crisis management https://doi.org/10.5465/ame.1993.9409142058
9	DREAM (Driver Reliability and Error Analysis Method)	Warner et al (2008) Manual for DREAM http://publications.lib.chalmers.se/records/fulltext/80432.pdf
10	**EFM (Emergent Failure Modes)**	
11	Error Analysis	Taylor (2016) Human Error in Process Plant Design and Operations, ISBN 978-1498738866
12	Extended FFIP	Seppo et al (2013) Common cause failure analysis of cyber–physical systems situated in constructed environments https://link.springer.com/article/10.1007/s00163-013-0156-2
13	**FFIP (Functional Failure Identification and Propagation)**	

14	**FMEA (Failure Mode and Effects Analysis)**	
15	FMECA - (Failure Mode, Effects, and Criticality Analysis)	Carlson (2012) Failure Mode Effects and Criticality Analysis (FMECA) https://doi.org/10.1002/9781118312575.ch12
16	**FPTA (Failure propagation and Transformation Analysis)**	
17	FPTC (Fault Propagation and Transformation Calculus)	Wallace (2005) Modular architectural representation and analysis of fault propagation and transformation. https://doi.org/10.1016/j.entcs.2005.02.051
18	FPTN (Failure Propagation Transformation Notation)	Fenelon and McDermid (1993) An integrated tool set for software safety analysis https://doi.org/10.1016/0164-1212(93)90029-W
19	**FRAM (Functional Resonance Accident Model)**	
20	**FTA (Fault Tree Analysis)**	
21	High Reliability Organisation Theory	Roberts (1989). "New challenges in organizational research: High reliability organizations" https://doi.org/10.1177/108602668900300202
22	Human Reliability Analysis (HRA)	Calixto (2015) Human Reliability Analysis *in* Gas and Oil Reliability Engineering https://www.sciencedirect.com/science/article/pii/B9780128054277000051
23	Network Analysis	Goodrum et al (2018) Understanding cascading failures through a vulnerability analysis of interdependent ship-centric distributed systems using networks https://doi.org/10.1016/j.oceaneng.2017.12.039
24	Normal Accident Theory	Perrow (1984) Normal Accidents: Living with High-Risk Technologies ISBN 978-0691004129
25	Probabilistic Safety Assessment	Verma et al (2010) Probabilistic Safety Assessment https://link.springer.com/chapter/10.1007/978-1-84996-232-2_9
26	Quality Engineering	Phadke (1995) Quality Engineering Using Robust Design ISBN 978-0-13-745167-8
27	Reliability Engineering	Kiran (2017) Reliability Engineering *in* Total Quality Management https://doi.org/10.1016/B978-0-12-811035-5.00027-1
28	Safety Engineering	Sgobba et al (2018) System safety and accident prevention *in* Space Safety and Human Performance https://doi.org/10.1016/B978-0-08-101869-9.00008-X
29	**STAMP System Theoretic Accident Model and Processes**	
30	**Swiss Cheese Model**	
31	System Reliability Study	Chang and Mori (2014) A Study of System Reliability Analysis Using Linear Programming https://doi.org/10.3130/jaabe.13.179

Figure 8: Long list of approaches
red indicates those ones which were removed in the final short-listing

The headings for the approach template were agreed with NIC. The codings for the various components of the approaches template are described in Figure 9 below.

<table>
<tr><td>A. Approach Name and Type</td><td>The usual form of the name of the approach;
Type is one of Sequential Methods Approach; Epidemiological Methods Approach or System Model Approach based on Wienen et al, 2017 as described above.</td></tr>
<tr><td>B. Approach Rankings Summary: Applicability to UK System of Infrastructure:</td><td>Very High (6/6): The Approach has been applied to at least one system with Very High (6/6) comparability to economic infrastructure
High (5/6): The Approach has been applied to at least one system with High (5/6) comparability to economic infrastructure
Medium-High (4/6): The Approach has been applied to at least one system with Medium-High (4/6) comparability to economic infrastructure</td></tr>
<tr><td>B. Approach Rankings Summary: Cross sector applicability</td><td>High Cross-Sectoral Applicability: examples of cross sector applications are provided in the approach literature AND the Approach scored High or Very High Applicability to Infrastructure (see row above).
Medium Cross-Sectoral Applicability: examples of cross sector applications are provided in the approach literature AND the Approach scored Low or Medium Applicability to Infrastructure (see row above).</td></tr>
<tr><td>B. Approach Rankings Summary: Strategic Relevance to NIC</td><td>High Strategic Relevance: the Approach can support one or more of the Strategically Relevant Outputs in Figure 7 AND the approach scored High or Very High for Applicability to UK System of Infrastructure (two rows above) AND the approach scored High Cross-Sectoral Applicability (row above)
Medium Strategic Relevance: the Approach can support one or more of the Strategically Relevant Outputs in Figure 7 AND the approach scored Medium for Applicability to UK System of Infrastructure (Table 2) (two rows above) AND the approach scored Medium Cross-Sectoral Applicability (row above)</td></tr>
<tr><td>C. Approach Applications and Comparability Scores by System</td><td>The systems in which the approach has been applied are listed.
Each type of system has been assessed for Systemic, Contextual, Organisational, Operational Timeframe, and Socio-Technical comparability to infrastructure. The Comparability Score reflects the system's comparability to economic infrastructures
<table>
<tr><td>Businesses and corporations</td><td>Medium (3/6)</td></tr>
<tr><td>Economic Regulation</td><td>Medium-High (4/6)</td></tr>
<tr><td>Facilities: Hospitals</td><td>High (5/6)</td></tr>
<tr><td>Facilities: Industrial Plants</td><td>Medium (3/6)</td></tr>
<tr><td>Facilities: Nuclear Reactors</td><td>Medium (3/6)</td></tr>
<tr><td>Facilities: Offshore Platforms</td><td>Medium (3/6)</td></tr>
<tr><td>Facilities: The International Space Station</td><td>High (5/6)</td></tr>
<tr><td>Industrial: Chemical and pharmaceutical</td><td>Medium (3/6)</td></tr>
<tr><td>Industrial: Petrochemical and other high hazard industries</td><td>Medium (3/6)</td></tr>
</table></td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td>Large Organisations</td><td>Medium (3/6)</td></tr>
<tr><td>Systems: Area navigation (RNAV) systems</td><td>Medium-High (4/6)</td></tr>
<tr><td>Systems: Civil Aerospace systems</td><td>Very High (6/6)</td></tr>
<tr><td>Systems: Complex Electromechanical Systems,</td><td>Medium (3/6)</td></tr>
<tr><td>Systems: Healthcare Systems</td><td>High (5/6)</td></tr>
<tr><td>Systems: Military/Defence Systems</td><td>Medium-High (4/6)</td></tr>
<tr><td>Systems: Power systems</td><td>Very High (6/6)</td></tr>
<tr><td>Systems: Social Systems</td><td>Very High (6/6)</td></tr>
<tr><td>Systems: Software Systems</td><td>Medium-High (4/6)</td></tr>
<tr><td>Systems: Transport Systems (Road/ Rail/ Air/ River/ Ocean)</td><td>Very High (6/6)</td></tr>
<tr><td>The Economic system</td><td>High (5/6)</td></tr>
<tr><td>The Public Sector</td><td>Very High (6/6)</td></tr>
<tr><td>Vehicles: Space Shuttles</td><td>Medium (3/6)</td></tr>
<tr><td>Activities: Led Outdoor Activities</td><td>Medium (3/6)</td></tr>
</table>
</td></tr>
<tr><td>D. Approach Purpose</td><td>These are a list of purposes for which the approach has been applied. They are taken from the literature describing the approach.</td></tr>
<tr><td>E. Approach Key Concepts</td><td>These are statements of the key concepts, principles and terminology that need to be understood prior to application of the approach.</td></tr>
<tr><td>F. Data Requirements and Availability</td><td>Each approach has been assessed on a variety of dimensions relating to the type and availability of data needed to apply the approach.

Type of data: Qualitative, Quantitative, Quantitative with a Qualitative foundation (Semi-Quantitative) or both Qualitative and Quantitative
Whether data requirements are: formally specified as part of the approach or generic data requirements are not important
Whether primary (i.e. new, relevant) data collection is: essential, ideal (but not essential), or not needed
Whether secondary data[15] is: available and described as part of the approach, additional secondary data collection is needed or it is not applicable
Whether specialist knowledge of the system of interest is: essential, ideal (but not essential), or not needed

NB: The information presented in this section is partial and based on research team judgement. In the first instance at least, data availability or the lack of data should not be a reason to accept or reject an approach.</td></tr>
<tr><td>G. Skills and Resource Requirements</td><td>Each approach has been assessed on a variety of dimensions relating to the skills and resource requirements needed to apply the approach.</td></tr>
</table>

[15] Primary data is data collected first hand (could be by interview, survey, etc.) to try and resolve a particular research question. It will be up-to-date and specifically relevant to the research question being addressed. Secondary data may be out of date, and/or may have been collected for a slightly different purpose, but it may be good enough, and avoids primary data collection. Secondary data is often quantitative, e.g. location and size of installed solar panels. For literature, see for example Hox and Boeije (2005), Data Collection, Primary vs. Secondary, Encyclopaedia of Social Measurement, 1 https://dspace.library.uu.nl/bitstream/handle/1874/23634/hox_05_data+collection,primary+versus+secondary.pdf?sequence=1

	• Specialist Software: Specialist Software is not needed, Specialist Software is essential or Specialist Software is Available • Approach specific training: Approach specific training is recommended, the approach can be applied without specific training • Sector/Discipline/Industry support: Sector/Discipline/Industry expertise to support data acquisition and validation is recommended, Multiple phases of cross-sectoral consultation with experts from multiple sectors are recommended, Cross sectoral collaboration between experts from multiple sectors is recommended • Other resource requirements: Computing power

Figure 9: Coding for the approaches templates

A visualisation of the key characteristics of the approaches using a red, amber, green (RAG) method is provided in Figure 10. Green status indicates a close match to economic infrastructure strategic policy needs; amber status indicates that some work is needed to make it useful; whilst red status indicates significant work is needed. Green ticks indicate reasonably easy to achieve green RAG status. Amber ticks indicate it is more tricky, but not impossible to achieve green RAG status.

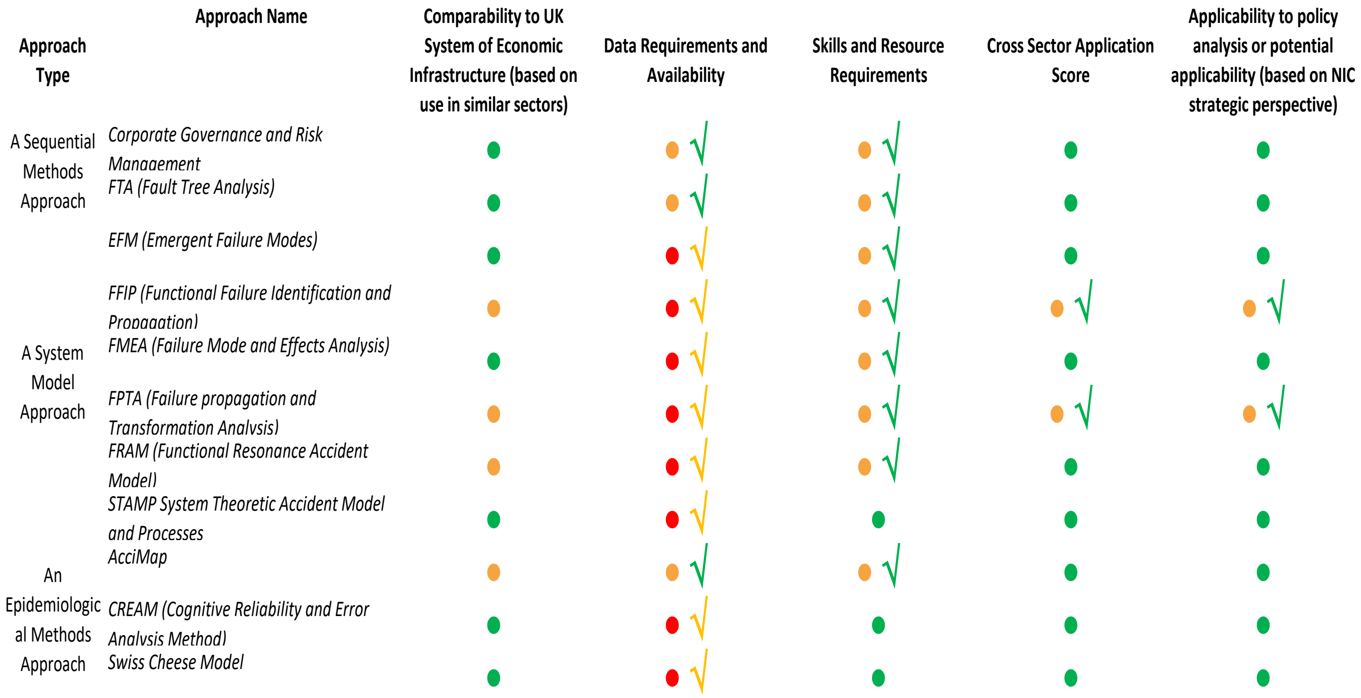

Figure 10: Approaches overview

A. Approach Name and Type	AcciMap Model An Epidemiological Methods Approach

B. Approach Rankings Summary		
	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High

C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Activities: Led Outdoor Activities (e.g. outdoor education and recreation providers)	Medium (3/6)
	Transport Systems: Road/ Rail/ Air/ River/ Ocean	Very High (6/6)

D. Approach Purpose
Risk Assessment
Safety and Accident Analysis
Situational awareness
Reliability and/or safety: System Processes
Hazards (external /internal/ human factors)
Risk Assessment

E. Approach Key Concepts
Hierarchical Systems
Vertical Integration
Migration of work practises
System Levels (parts, units, assets, artefacts, sub-system, system)
Performance Variability (internal and external)

F. Data Requirements and Availability
A semi-quantitative approach
Data requirements are formally specified
Primary data is essential
Sufficient secondary data is available
Specialist knowledge of the system of interest is essential

G. Skills and Resource Requirements	Specialist software is essential
	Approach specific training is recommended
	Multiple phases of Cross-Sectoral Consultation with experts from multiple sectors are recommended

H. Complementary Approaches		
	Swiss Cheese Model	

J. Approach Overview

Rasmussen's (1997) risk management framework is underpinned by the idea that work systems can be described as a hierarchy of multiple levels (e.g., government, regulators/associations, company, management, staff, work), as shown in the Figure 1. The actions and decisions of those operating within and across these levels interact, and contribute to the control of hazardous processes. Safety is maintained through a process referred to as "vertical integration," where decisions made at higher levels of the system (i.e., by government, regulators, and the company) are reflected in practices occurring at lower levels of the system, while information at lower levels (i.e., work, staff) informs decisions and actions at the higher levels of the hierarchy. A lack of vertical integration can result in a loss of control and accidents. The framework also describes how work practices constantly adapt and change in response to various external pressures and conditions. This process, referred to as "migration," causes accidents when changes in work practices erode existing control measures.

The accompanying AcciMap technique provides a methodological framework for analysing accidents from this perspective. The method enables analysts to graphically represent the contributing factors across all levels of the system in question, along with the relationships between them.

Rasmussen's framework also makes a series of predictions, regarding accidents and safety in complex sociotechnical systems. These predictions reflect the three core principles of accident causation underpinning the systems approach, and also describe the role that vertical integration and the migration of work practices play in accident causation.

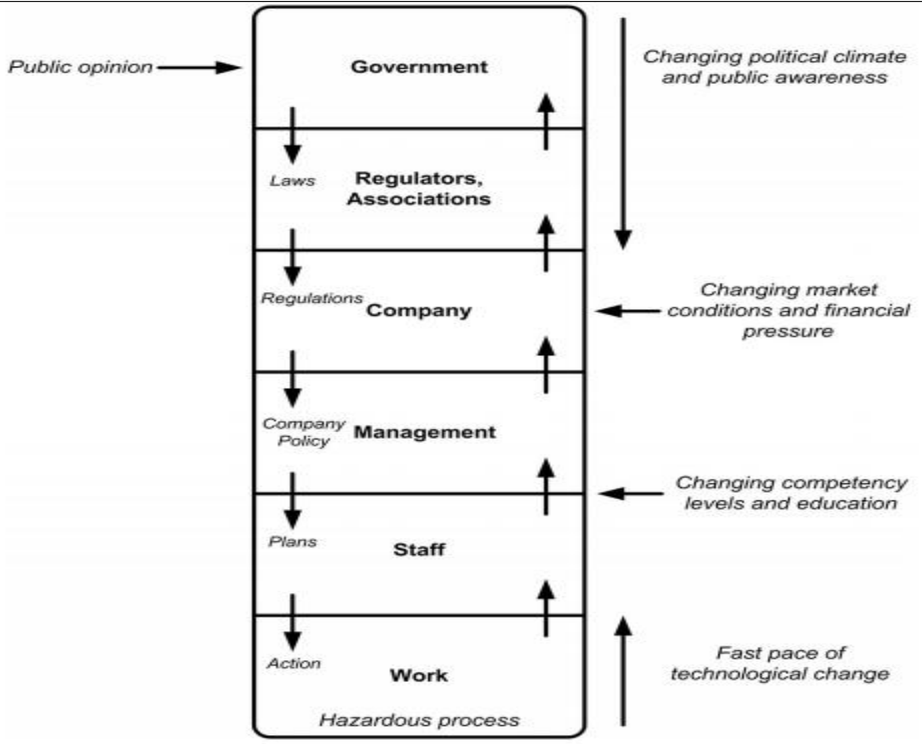

Figure 2 Rasmussen's risk managemnet framework (adapted from Rasmussen, J., 1997).

K. Approach Literature:

[1] Qureshi, Z., 2007. A Review of Accident Modelling Approaches for Complex Socio-technical Systems. Australian Computer Society, 47-59.

[2] Goode, N., Read, G.J., van Mulken, M.R., Clacy, A. and Salmon, P.M., 2016. Designing system reforms: using a systems approach to translate incident analyses into prevention strategies. Frontiers in psychology, 7, p.1974; https://www.frontiersin.org/articles/10.3389/fpsyg.2016.01974/full

[3] Rasmussen, J., 1997. Risk management in a dynamic society: a modelling problem. Safety science, 27(2-3), pp.183-213.

A. Approach Name and Type	<u>Corporate Governance and Risk Management (including Normal Accident Theory, High Reliability Organisation Theory, Crisis Prone Organisation Theory) Model</u>
	A Sequential Methods Approach

B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High

	System	**Comparability Score**
	Facilities: Industrial Plants	Medium (3/6)
C. Approach Applications and Comparability Scores by System	Facilities: Nuclear Reactors	Medium (3/6)
	Facilities: Offshore Platforms	Medium (3/6)
	Industrial: Chemical and pharmaceutical	Medium (3/6)
	Systems: Transport Systems (Road/ Rail/ Air/ River/ Ocean)	Very High (6/6)
	Systems: Military/Defence Systems	High (5/6)
	Large Organisations	Medium (3/6)
	Public Sector Bodies	Very High (6/6)

D. Approach Purpose	
	Systemic Analysis: Organisational accidents
	Create Organisational capability to anticipate disruption and mitigate impacts
	Prevent Organisational Failures
	Systemic Mitigate the Effect of Unpredictable failures in Complex systems
	Systemic Analysis: Reasons for/cause of of system failure
	Risk Assessment and Risk Factor Analysis
	Systemic Analysis: Reliability
	Systemic Analysis: Safety and Accident

E. Approach Key Concepts	Interactive complexity (linear vs complex interactions)	
	Tight/loose coupling	
	Interdependency Dimensions	
	Incertitude Types (Risk vs uncertainty vs ambiguity vs ignorance)	
	Controls (systems/ structures / Levels / software)	
	Learning, Mindfulness and Reporting Culture	
	Accident Opportunities	
	Error-provoking conditions (and condition types)	

F. Data Requirements and Availability	A qualitative approach
	Generic data requirements are not important
	Secondary data is not applicable
	Primary data is essential
	Specialist knowledge of the system of interest is essential

G. Skills and Resource Requirements	Specialist software is not needed
	Approach specific training is recommended
	Cross sectoral collaboration between experts from multiple sectors is recommended

H. Complementary Approaches	Crisis Prone Organisation Theory	
	High Reliability Organisation Theory	
	Normal Accident Theory	
	Swiss Cheese Model	
	STAMP	

J. Approach Overview
This is a basket of approaches using analytical techniques, and are management focussed.
Corporate Governance and Risk Management
Corporate Governance and Risk Management has been adapted to prevent organisational failures before they occur. Drawing on a number of conceptual traditions including Normal Accident Theory (why large complex organisational systems tend to fail), High Reliability Organisations (how some organisations minimise failure), and Crisis Prone Organisations, a capacity to anticipate failures and mitigate loss is theoretically possible as a result of enhanced and directed professional practice in Corporate Governance and Risk Management.

Normal Accident Theory (NAT)
NAT emerged from analysis of a range of industrial disasters and accidents spanning a period of at least the last 40 years. It introduced the idea that in some technological systems, accidents are inevitable or 'normal'. It has two related dimensions - interactive complexity and loose/tight coupling - that defined organisational susceptibility to accidents.
The notion of interactive complexity includes two factors: Linear and complex interactions. Linear interactions are elements in expected or planned operational sequences. The attributes of linear systems generally behave in planned ways with single functions. Interactive complexities, however, derive from unfamiliar, unplanned or unique operational sequences that might not be visible or comprehensible to users of the system. According to theory, systems with interactive complexity and tight coupling have increased potential to experience accidents that cannot be foreseen or prevented. Perrow (1984) refers to these as 'system' accidents. When the system is interactively complex, inter-dependent failure events can interact in ways that cannot be predicted by the designers and operators of the system. If the system is also tightly coupled, the cascading of effects can quickly spiral out of control before operators are able to understand the situation and perform appropriate corrective actions. Systems accidents result from a gestalt of the processes not the component parts themselves.
High Reliability Organisations (HRO)
HRO as the words suggest, are closely linked to safety, regularity and accuracy. To achieve this HRO operate in a context of near full knowledge of the physical and technical aspects of the operational activities they carry out. People in these organisations know almost everything technical about what they are doing and aim at having prepared for nearly every conceivable contingency. The tendency to seek and require complete knowledge of a system or process by HRO's contrasts against the 'interactive complexity,' described by NAT where the interactions between components cannot be thoroughly planned, understood, predicted, or guarded against. Ideally for HRO's, it would be relatively easy to lower risk through standard system safety and industrial safety approaches. Unfortunately, most complex systems, particularly high technology and social systems, do not fall into this category.
Crisis Prone Organisations
Analyses of iconic organisational failures and their aftermath have shown that in addition to certain causal triggers of crises being unexpected and predisposing factors overlooked the capacity to respond quickly and appropriately once emergent signs appeared also seemed restricted. Specific organisational cultural patterns or 'operating rules' have been retrospectively linked to the genesis and amplification of well-known organisational crises. It has been strongly argued that the presence of such patterns in an operational repertoire increase vulnerability and the likelihood of accidents and crises (Perrow, 1984).
Corporate governance is grounded in the effective use of information management and control mechanisms. An adequate capacity for corporate governance therefore would require the existence of a variety of channels of information to senior decision makers. Effective corporate governance also requires capacities for coping with this phenomenon and structuring suitable internal control mechanisms. With suitable reporting mechanisms in place, enhanced variety in strategic information creation can be developed to generate increased capacity to attenuate corporate risk. Thus as organisations increase in complexity and opaqueness, so too must the sophistication and variety of acquisition of corporate information and regulatory control. While sophistication of the information in such circumstances is a given, it must be timely, be couched in forms that aid decision making and not impede it.

The below figure displays a possible operational structure designed to both minimise the emergence of the signs and symptoms of organsiational failure and identify them when they appear.

The framework comprises a standard internal control capacity embodied in an Internal Audit committee with an expanded governance capacity in the form of separate Legislative and Finance committees. It also includes a separate Corporate Risk Management Committee (CRMC). All four committees report in parallel to the Departmental Board of Governance. The Legislative Committee provides advice on legislative reform related to departmentally regulated matters and external legislation. The Finance Committee, as might be expected, ensures accurate and detailed reporting of financial statements to the Board. An eclectic view on the combined exposures would allow comprehensive and robust organisational mitigation strategies to be chosen and implemented. A key function related to this strategic view is the preparation of a Corporate Threat Register. The Corporate Threat Register (CTR) is used a decision-making aid by the Board of Governance to prioritise risk management activities, decision making and enhance governance generally.

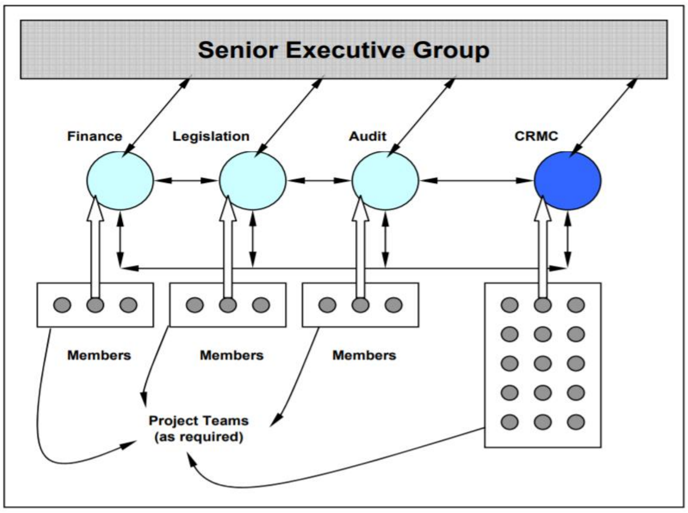

Figure 3 A corporate Risk Management Framework (adopted form Barnes, P.H., 2005)

A higher order purpose of the Corporate Risk Management Framework shown in Figure 1 is to overcome any propensity of the department to become crisis prone and succumb to the many interactive complexity and coupling factors present in such a large and diverse public organisation. By engaging in a structured analytical process the benefits of strategic foresight, issue and scenario analysis and the engagement of expertise at all levels of the organisation, a capacity to recognise unexpected and usual changes in organisational functioning is part of the register’s design goal.

K. Approach Literature:

[1] Barnes, P.H., 2005. Can Organisational Failures be prevented before They Occur?(A discussion about Corporate Governance and Risk Management). University. https://eprints.qut.edu.au/2120/1/2120_1.pdf

A. Approach Name and Type	CREAM (Cognitive Reliability and Error Analysis Method) Model	
	An Epidemiological Methods Approach	
B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High
C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Facilities: Nuclear Reactors	Medium (3/6)
	Systems: Transport Systems (Road/ Rail/ Air/ River/ Ocean)	Very High (6/6)
	Facilities: Hospitals	High (5/6)
D. Approach Purpose	Error Mode Identification and Classification	
	Task Analysis	
	Error Reduction opportunities	
	Human performance for system safety	
	Failure / disruptions: Anticipation or Prediction	
E. Approach Key Concepts	Active Failures (and Active Failure types)	
	Error-provoking conditions (and condition types)	
	Error Reduction opportunities	
	Human Factors	
	Functional and Behavioural Models	
	Risk Factors (and Risk Factor types)	
F. Data Requirements and Availability	A semi-quantitative approach	
	Generic data requirements are not important	
	Primary data is essential	
	Secondary data is not applicable	
	Specialist knowledge of the system of interest is essential	

G. Skills and Resource Requirements	Specialist Software is not needed
	Approach specific training is recommended
	Sector/Discipline/Industry expertise to support data acquisition and validation is recommended

H. Complementary Approaches		
	DREAM (driver Reliability and Error Analysis Method)	
	BREAM (Maritime Reliability and Error Analysis Method)	
	Human Reliability Analysis (HRA)	
	Error Analysis	
	Swiss Cheese Model	
	FRAM	
	Cognitive System Engineering	

J. Approach Overview

CREAM is based on the modelling of cognitive aspects of human performance for an assessment of the consequences of human error on the safety of a system (Hollnagel, 1998). In other words, CREAM methodology was developed by Eric Hollnagel in 1998 following an analysis of already in place Human Reliability Analysis (HRA) methods. It is the most widely utilized second generation HRA technique and is based on three primary areas of work; task analysis, opportunities for reducing errors and possibility to consider human performance with regards to overall safety of a system. Two versions of CREAM have been developed for accident modelling: DREAM (Driver Reliability and Error Analysis Method) for analysis of traffic accidents; and BREAM for use in maritime accident analysis (Hollnagel 2006).

CREAM can be used both predictively, to predict potential human error, and retrospectively, to analyse and quantify error. The CREAM technique consists of a method, a classification scheme and a model. According to Hollnagel (1998) CREAM enables the analyst to achieve the following:

1. Identify those parts of the work, tasks or actions that require or depend upon human cognition, and which therefore may be affected by variations in cognitive reliability.
2. Determine the conditions under which the reliability of cognition may be reduced, and where therefore the actions may constitute a source of risk.
3. Provide an appraisal of the consequences of human performance on system safety, which can be used in PRA/PSA.
4. Develop and specify modifications that improve these conditions, hence serve to increase the reliability of cognition and reduce the risk.

It should be mentioned that FRAM approach (which appears in our list of approaches) is also based on principle of cognitive systems engineering.

K. Approach Literature:

[1] Qureshi, Z., 2007. A Review of Accident Modelling Approaches for Complex Socio-technical Systems. Australian Computer Society.

[2] Cognitive Reliability and Error Analysis Method, https://www.skybrary.aero/index.php/Cognitive_Reliability_and_Error_Analysis_Method_(CREAM)
[3] Hollnagel, E., 1998. Cognitive reliability and error analysis method (CREAM). Elsevier.
[4] Griebel, M., 2016. Applying the cognitive reliability and error analysis method to reduce catheter associated urinary tract infections (Doctoral dissertation, Kansas State University).
[5] De Felice, F., Petrillo, A., Carlomusto, A. and Romano, U., 2013. Modelling application for cognitive reliability and error analysis method. Int J Eng Technol, 5(5), pp.4450-4464.
[6] Hollnagel, Erik., CREAM - Cognitive Reliability and Error Analysis Method, https://erikhollnagel.com/ideas/cream.html

A. Approach Name and Type	EFM (Emergent Failure Modes) Model	
	A System Model Approach	
B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High
C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Systems: Civil Aerospace systems	Very High (6/6)
	Power Systems	Very High (6/6)
	Vehicles: Space Shuttles	Medium (3/6)
	Facilities: The International Space Station	High (5/6)
D. Approach Purpose	Systemic Mitigate the Effect of Unpredictable failures in Complex systems	
	Systemic Analysis: Reasons for/cause of of system failure	
	Systemic Mitigate the Effect of Unpredictable failures in Complex systems	
	Detect, diagnose and redress emergent failure	
	Improve situational awareness	
	Analysis of Component failures	
	Systemic Analysis: Failure Modes	
	Systemic Analysis: Active Failures (typically Human Factors) and Latent Conditions	
E. Approach Key Concepts	Situation awareness	
	System Integrity	
	Controls (systems/ structures / Levels / software)	
	System Dynamics	
	closed-loop Control processes	
	Active Failures (and Active Failure types)	
	Human Factors (and latent conditions)	
F. Data Requirements and Availability	A Quantitative approach	
	Data requirements are formally specified	
	Primary data is essential	
	Significant additional secondary data is required	

	Specialist knowledge of the system of interest is essential
G. Skills and Resource Requirements	Approach specific training is recommended
	Cross sectoral collaboration between experts from multiple sectors is recommended

H. Complementary Approaches		
	FMEA	

J. Approach Overview

EFM is a means to mitigate the effects of unpredictable failures in complex systems. It outlines a formal analysis of complex systems that focuses on emergent system dynamics, some of which may be failure modes that are impossible to predict. The mathematical basis for the analysis, and some real-world implications of the mathematics are introduced in Harris, S.D. and Narkevicius, J.M., (2016).

EFM are real artifacts of systems design and implementation. The analysis of complex systems (including SOA/SoS) shows the unpredictable and nearly inevitable character of EFM. The Harris, S.D. and Narkevicius, J.M., 2016 outlined a principle-based approach that apportions aspects of control processes to human and machine components in a way that exploits human strengths to detect, diagnose and redress emergent failures provides an approach to solutions. The recommendation is to ensure that a proposed system architecture conforms to the process architecture in Figure 1 below.

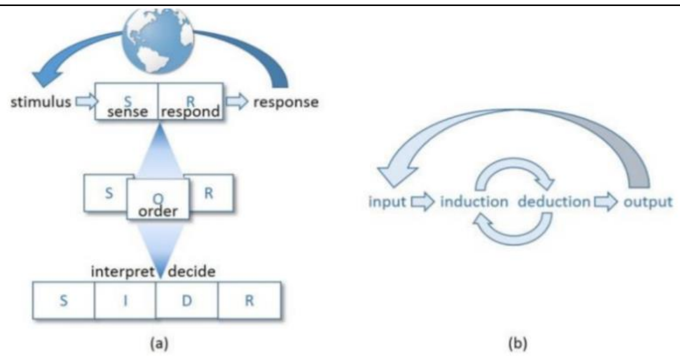

Figure 4 Logical Structure of closed-loop control (adopted from Harris, S.D. and Narkevicius, J.M., 2016)

The logical structure of any closed-loop control problem is illustrated in Figure 1. The top illustration in Figure 1 depicts the most elementary observations about control systems, that they have inputs and generate outputs, and that there must be some boundary between input and output processes, as the energy impinging on the system (the stimuli) differs from the energy emitted by the system (i.e., its responses).

The middle and lower illustrations in Figure 1 expand the boundary between input (S) and response (R) processes, to illustrate that of necessity, there must be processes that resolve induction. The middle illustration (S-O-R) expands the boundary between S and R processes in the depiction above, indicating that there must be some intervening organizing (O) processes between the S and the R processes. For example, the same S may elicit a different R as a result of intervening experience and feedback.

The bottom illustration of Figure 1 expands the O to reflect that it must comprise distinct components, as there are two separable mappings evident. Mapping from stimulus to an internal representation (often called an interpretation or situation awareness), and mapping from that internal representation to a response (also called decision making). The structure of both of these mappings is of the character of a logical induction.

K. Approach Literature:

[1] Harris, S.D. and Narkevicius, J.M., 2016, July. Emergent failure modes and what to do about them. In INCOSE International Symposium (Vol. 26, No. 1, pp. 1044-1058).

A. Approach Name and Type	FFIP (Functional Failure Identification and Propagation) Model
	A System Model Approach

B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Medium (3/6)
	Cross Sector Applicability	Medium
	Strategic Relevance to NIC	Medium

C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Systems: Complex Electromechanical Systems,	Medium (3/6)
	Facilities: Nuclear Reactors	Medium (3/6)

D. Approach Purpose	System Dynamics: Information flows, feedback loops, delays and abnormal flows
	System Dynamics: Physical flows, feedback loops and delays
	System Design
	System Dynamics: Critical interdependencies
	Failures / Disruptions: Systemic Impacts
	System Reliability
	Component Reliability

E. Approach Key Concepts	Abnormal Flow States	
	Functional and Behavioural Models	
	Feedback Loops	
	Interdependency Dimensions	
	Configuration Flow	
	System Levels (parts, units, assets, artefacts, sub-system, system)	
	SysML	
	Failure Logic	

F. Data Requirements and Availability	A qualitative and quantitative approach
	Generic data requirements are not important
	Primary data is essential
	Significant additional secondary data is required
	Specialist knowledge of the system of interest is essential

G. Skills and Resource Requirements	Specialist Software is essential
	Approach specific training is recommended
	Multiple phases of cross-sectoral consultation with experts from multiple sectors are recommended
	Other resource requirements: Computing power

H. Complementary Approaches	Extended FFIP	
	FMEA	
	FMECA - (Failure Mode, Effects, and Criticality Analysis)	

J. Approach Overview

FFIP simulation framework reveals the propagation of abnormal flow states and can thus be used to infer emergent system-wide behaviour that may compromise the reliability of the system. An advantage of FFIP is that it is used to model early phase designs, before high cost commitments are made and before high fidelity models are available.

The FFIP framework was developed to capture the effect of complex system interactions early in the design stage and presenting the effect and propagation of faults in terms of functional losses. The simulation and reasoning approach in FFIP has its roots in qualitative physics and qualitative reasoning. FFIP utilizes a finite state representation of system behaviour, and performs reasoning based on qualitative relationships between functional and behavioural models of system components.

FFIP can use discrete set of flow state values and a simple behavioural logic; this has had the advantage of limiting the range of possible parameter values, but it has not been possible to model continuous process dynamics. So the extended FFIP framework supports continuous flow levels and linear modeling of component behaviour based on first principles. The extension further expanded the range of model parameter values, methods and tools for studying the impact of parameter value changes. The result is an evaluation of how the FFIP results are impacted by changes in the model parameters and the timing of critical events.

K. Approach Literature:

2012. Simulation of interactions and emergent failure behaviour during complex system design. Journal of Computing and Information Science in Engineering, 12(3), p.031007.

A. Approach Name and Type	FMEA (Failure Mode and Effects Analysis)	
	A System Model Approach	
B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High
C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Systems: Civil Aerospace systems	Very High (6/6)
	Vehicles: Space Shuttles	Medium (3/6)
	Facilities: The International Space Station	High (5/6)
	Systems: Military/Defence Systems	Medium-High (4/6)
	Systems: Software Systems	Medium-High (4/6)
	Systems: Medical/healthcare/clinical Systems	High (5/6)
	Systems: Civil Aerospace systems	Very High (6/6)
	Vehicles: Space Shuttles	Medium (3/6)
D. Approach Purpose		
	Failure / disruptions: Failure Modes	
	Failure / disruptions: Prevention (Component Failures)	
	Detect, diagnose and redress emergent failure	
	Systemic Analysis: Criticality	
	Systemic Analysis: Root causes Analysis and potential Failure modes	
	Systemic Analysis: Reliability	
	Systemic Mitigate the Effect of Unpredictable failures in Complex systems	
	Systemic Analysis: Safety and Accident	
E. Approach Key Concepts	Constraints	
	control loops	
	Controls (systems/ structures / Levels / software)	
	Process Model	
	Failure Modes	
	Failure Logic	
	Analysis types (functional, design, process)	
	Criticality Index	
F. Data Requirements and Availability	A qualitative and quantitative approach	
	Data requirements are formally specified	
	Primary data is essential	
	Significant additional secondary data is required	

	Specialist knowledge of the system of interest is essential

G. Skills and Resource Requirements	Specialist Software is Available (ReliaSoft XFMEA or RCM++)
	Approach specific training is recommended
	Multiple phases of cross-sectoral consultation with experts from multiple sectors are recommended

H. Complementary Approaches		
	Error Analysis	
	Crisis Prone Organisation Theory	
	EFM	
	Probabilistic Safety Assessment	
	FMECA - (Failure Mode, Effects, and Criticality Analysis)	
	Reliability Engineering	

J. Approach Overview

FMEA is a structured process of reviewing as many components, assemblies, and subsystems as possible to identify potential failure modes or error-prone situations in a system, as well as their causes and their effects. Broadly, this follows three distinct steps:

i. process mapping – to identify all the steps that must occur for a given process to occur.

ii. Errors mapping – to identify the ways in which each step of a process can go wrong; the probability that each error can be detected; and the consequences or impact of the error not being detected.

iii. Criticality Index - The estimates of the likelihood of a particular process failure, the chance of detecting such failure, and its impact are combined numerically to produce a criticality index. This criticality index provides a rough quantitative estimate of the magnitude of hazard posed by each step in a high-risk process. Assigning a criticality index to each step allows prioritization of targets for improvement.

A dedicated FMEA worksheet is produced for each component to record failure modes identified, and potential impacts on system performance. The FMEA process is flexible and FMEA worksheets can be tailored to meet specific analytical needs. Indeed a few common types of FMEA analyses exist, Functional, Design and Process.

FMEA can be a purely qualitative analysis. Or FMEA can combine qualitative and quantitative analysis. For example, through use of mathematical failure rate models and a statistical failure mode ratio database.

FMEA is an inductive reasoning (forward logic) single point of failure analysis and is a core task in reliability engineering, safety engineering and quality engineering.

A successful FMEA activity helps identify potential failure modes based on experience with similar products and processes—or based on common physics of failure logic. Effects analysis refers to studying the consequences of those failures on different system levels. It is widely used in development and manufacturing industries in various phases of the product life cycle as well as military systems. It also useful for high-risk industries, including health care as well as for computer/ software/hardware.

The classical safety engineering technique Failure Modes and Effects Analysis (FMEA) can be used for infrastructure to analysis of failure propagation behaviour from the system engineering perspective which is a process for identifying the failure modes of a system starting from an analysis of component failures. Generally, the process of failure analysis consists of several activities: identifying failures of individual components, modelling the failure logic of the entire system, analysing a failure's effect on other components, and determining and engineering the mitigation of potential hazards.

K. Approach Literature:

[1] Systems Approach, Patient Safety Network website, http://psnet.ahrq.gov/primer/systems-approach
[2] Failure Mode & Effects Analysis (FMEA), https://www.moresteam.com/toolbox/fmea.cfm
[3] Failure Mode and Effect Analysis (FMEA) and Failure Modes, Effects and Criticality Analysis (FMECA), https://www.weibull.com/basics/fmea.htm

A. Approach Name and Type	FPTA (Failure Propagation and Transformation Analysis)Model	
	A System Model Approach	
B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Medium-High (4/6)
	Cross Sector Applicability	Medium
	Strategic Relevance to NIC	Medium
C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Systems: Software Systems	Medium-High (4/6)
D. Approach Purpose	Failures / Disruptions: Systemic Impacts	
	Failure / disruptions: systemic impact pathways	
	System Dynamics: Critical components	
	System Dynamics: Critical interdependencies	
	Component Reliability	
	Probabilistic Safety Assessment	
	Analysis of Component failures	
	Failure Mode Identification	
E. Approach Key Concepts	Component Failure Types (sequential, time and value)	
	Cyber-Physical Systems	
	Cybersecurity	
F. Data Requirements and Availability	A qualitative and quantitative approach	
	Generic data requirements are not important	
	Primary data is essential	
	Significant additional secondary data is required	
	Specialist knowledge of the system of interest is essential	
G. Skills and Resource Requirements	Specialist Software is not needed	
	Approach specific training is recommended	
	Multiple phases of cross-sectoral consultation with experts from multiple sectors are recommended	

H. Complementary Approaches	FMEA	
	FMECA - (Failure Mode, Effects, and Criticality Analysis)	
	FPTA	
	FPTC	
	FPTN	
	FFIP	
	Extended FFIP	

J. Approach Overview

Failure propagation and transformation analysis (FPTA) – A System Approach

It is a failure behaviour analysis technique which derives the system level failure behaviour from the failure behaviours of its building elements and is particularly suitable for performing the analyses at early stages of component based development where the costs of correcting the design faults are relatively minor compared to the faults discovered at, for instance, testing phase of the development. It is a safety analysis technique, which automatically and quantitatively analyses failures based on a model of failure logic. The technique integrates previous work on automated failure analysis with probabilistic model checking supported by the PRISM tool.

This method is an extension of FPTC technique, that overcome the limitations existing system engineering analysis techniques such as FMEA, FPTN, FPTC.

FPTC Analysis Technique

To represent the system as a whole, every element of the system architecture – both components and connectors – is assigned FPTC behaviour. Each model element that represents a relationship is annotated with sets of tokens (e.g., omission, late). The architecture as a whole is treated as a token-passing network, and from this the maximal token sets on all relationships in the model can be automatically calculated, giving us the overall failure behaviour of the system. This calculation resolves to determining a fix-point.

FMEA, FPTN, FPTC Limitations

– FMEA and FPTN generally provide manual or non-compositional analysis. Such analysis is expensive, especially in a typical component-based development process, because if changes are made to components, the failure analysis has to be carried out again, and previous analysis results will be invalidated.

– FPTC does not provide facilities for quantitative analysis, particularly in terms of determining the probability of specific failure behaviours. Such quantitative analysis can help to provide more fine-grained information to help identify and determine suitable (cost-effective) mitigation to potential hazards.

K. Approach Literature:

[1] Ge, X., Paige, R.F. and McDermid, J.A., 2009, September. Probabilistic failure propagation and transformation analysis. In International Conference on Computer Safety, Reliability, and Security (pp. 215-228). Springer, Berlin, Heidelberg.
[2] Briesemeister, L., Denker, G., Elenius, D., Mason, I., Varadarajan, S., Bhatt, D., Hall, B., Madl, G. and Steiner, W., 2011, November. Quantitative fault propagation analysis for networked cyber-physical systems. In Proc. of 2nd AVICPS Workshop.

A. Approach Name and Type	FRAM (Functional Resonance Accident Model)
	System Model Approach

B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High

C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Facilities: Offshore Platforms	Medium (3/6)
	Organisations: Large Organisations	Medium (3/6)
	Systems: Area navigation (RNAV) systems	Medium-High (4/6)
	Systems: Civil Aerospace systems	Very High (6/6)
	Transport Systems: Road/ Rail/ Air/ River/ Ocean	High (5/6)

D. Approach Purpose	Safety and Accident Analysis
	System Dynamics: Critical components
	Reliability and/or safety: Components
	Reliability and/or safety: System Processes
	Reliability and/or safety: Whole System
	System Dynamics: Critical interdependencies
	Failure / disruptions: Anticipation or Prediction
	Failures / Disruptions: systemic root causes

E. Approach Key Concepts	Approximate Adjustments	Functional view of systems
	Functional Resonance	Interdependencies
	Emergence	Performance Variability (internal and external)
	Equivalence (failures and successes)	Process Model

F. Data Requirements and Availability	
	A qualitative approach
	Data requirements are formally specified
	Primary data is essential
	Significant additional secondary data is required
	Specialist knowledge of the system of interest is essential

G. Skills and Resource Requirements	Specialist Software is not needed
	Approach specific training is recommended
	Cross sectoral collaboration between experts from multiple sectors is recommended

H. Complementary Approaches	Cognitive System Engineering	

J. Approach Overview

Functional Resonance Accident Model (FRAM) Approach, Systemic Accident Models

FRAM is a qualitative accident model that describes how functions of system components may resonate and create hazards that can run out of control and lead to an accident (Hollnagel 2004). It is a systemic accident models for safety and accident analysis that was developed based on the principles of cognitive systems engineering. FRAM is based on the premise that performance variability, internal variability and external variability are normal, in the sense that performance is never stable in a complex socio-technical system such as aviation.

The FRAM perspective is that a system interacts with its context through a collection of functions, which can be characterized by input, output, resources it needs, its control and real-time behaviour. Functions interact through these aspects. A functional view of systems abstracts away from its internal components and concentrates on logical behaviour. It is similar to the view of systems taken by structured analysis for real-time systems.

The FRAM is based on four principles: the equivalence of failures and successes, the central role of approximate adjustments, the reality of emergence, and functional resonance as a complement to causality. The FRAM does not imply that events happen in a specific way, or that any predefined components, entities, or relations must be part of the description. Instead it focuses on describing what happens in terms of the functions involved. These are derived from what is necessary to achieve an aim or perform an activity, hence from a description of work-as-done rather than work-as-imagined. But functions are not defined a priori nor necessarily ordered in a predefined way such as hierarchy. Instead they are described individually, and the relations between them are defined by empirically established functional dependencies.

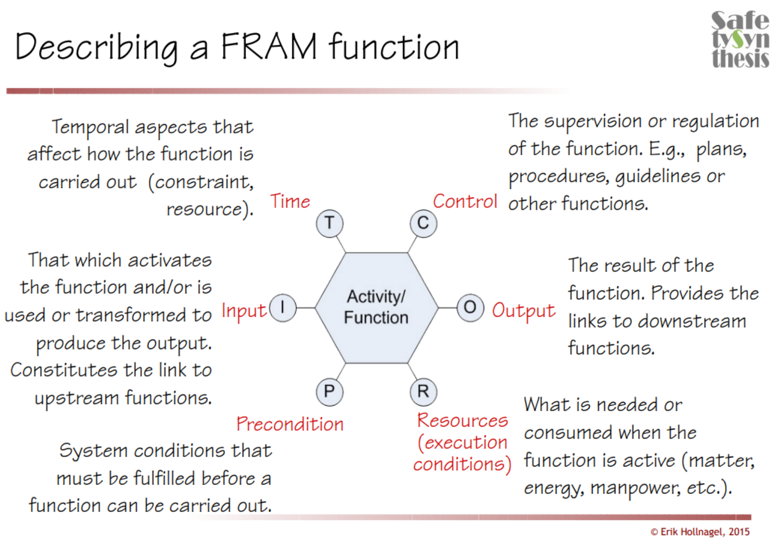

Figure 5 Describing a FRAM function (adopted from http://www.resolute-eu.org/images/media_centre/1st_workshop/EH_Firenze_DEC15-ferreira.pdf)

K. Approach Literature:

[1] Qureshi, Z., 2007. A Review of Accident Modelling Approaches for Complex Socio-technical Systems. Australian Computer Society.
[2] Wienen, H.C.A., Bukhsh, F.A., Vriezekolk, E. and Wieringa, R.J., 2017, June. Accident analysis methods and models—a systematic literature review. In Centre for Telematics and Information Technology (CTIT).
[3] FRAM - the FUNCTIONAL RESONANCE ANALYSIS METHOD for modelling non-trivial socio-technical systems, https://www.functionalresonance.com/.
[4] Hollnagel, E. and Goteman, O., 2004. The functional resonance accident model. Proceedings of cognitive system engineering in process plant, 2004, pp.155-161.
[5] Hollnagel, Erik, Modelling transport systems with FRAM: Flows or functions? http://www.resolute-eu.org/images/media_centre/1st_workshop/EH_Firenze_DEC15-ferreira.pdf

A. Approach Name and Type	STAMP (System Theoretic Accident Model and Processes)	
	System Model Approach	
B. Approach Rankings Summary	Applicability to UK System of Infrastructure	Very High (6/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High
C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Systems: Civil Aerospace systems	Very High (6/6)
	Systems: Military/Defence Systems	Medium-High (4/6)
	Vehicles: Space Shuttles	Medium (3/6)
D. Approach Purpose	Failures / Disruptions: systemic root causes	
	Safety and Accident Analysis	
	Systemic Impacts: Internal Change	
	Risk Factor Analysis	
	Reliability and/or safety: System Processes	
	Human Factors	
	Hazards (external /internal/ human factors)	
	Systemic Risk Factors	
E. Approach Key Concepts		
	Constraints	
	closed-loop Control processes	
	Feedback Loops	
	Controls (systems/ structures / Levels / software)	
	Risk Factors (and Risk Factor types)	
	System Levels (parts, units, assets, artefacts, sub-system, system)	
	System Dynamics	
	Emergence	
F. Data Requirements and Availability	A qualitative and quantitative approach	
	A process to Identify specific data requirements is part of the approach	
	Primary data is essential	
	Significant additional secondary data is required	
	Specialist knowledge of the system of interest is essential	

G. Skills and Resource Requirements	Specialist Software is not needed
	Approach specific training is recommended
	Cross sectoral collaboration between experts from multiple sectors is recommended

H. Complementary Approaches		
	FRAM	
	Normal Accident Theory	
	High Reliability Organisation Theory	

J. Approach Overview

Systems Theoretic Accident Model and Processes (STAMP) Approach, Systemic Accident Models

Leveson (2004) proposes a model of accident causation that considers the technical (including hardware and software), human and organisational factors in complex socio-technical systems. According to Leveson, “The hypothesis underlying the new model, called STAMP (Systems-Theoretic Accident Model and Processes) is that system theory is a useful way to analyze accidents, particularly system accidents”. In the STAMP approach, accidents in complex systems do not simply occur due to independent component failures; rather they occur when external disturbances or dysfunctional interactions among system components are not adequately handled by the control system. Accidents therefore are not caused by a series of events but from inappropriate or inadequate control or enforcement of safety-related constraints on the development, design, and operation of the system.

A STAMP accident analysis can be conducted in two stages: 1) Development of the Hierarchical Control Structure, which includes identification of the interactions between the system components and identification of the safety requirements and constraints; 2) Classification and Analysis of Flawed control (Constraint Failures), which includes the classification of causal factors followed by the reasons for flawed control and dysfunctional interactions.

In STAMP, systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control. A system in this conceptualization is not a static design—it is a dynamic process that is continually adapting to achieve its ends and to react to changes in itself and its environment.

The basic concepts in STAMP are constraints, control loops and process models, and levels of control.

K. Approach Literature:

[1] Qureshi, Z., 2007. A Review of Accident Modelling Approaches for Complex Socio-technical Systems. Australian Computer Society.

[2] Wienen, H.C.A., Bukhsh, F.A., Vriezekolk, E. and Wieringa, R.J., 2017, June. Accident analysis methods and models—a systematic literature review. In Centre for Telematics and Information Technology (CTIT).

[3] Zhou, Z., Zi, Y., Chen, J. and An, T., 2019. Hazard Analysis for Escalator Emergency Braking System via System Safety Analysis Method Based on STAMP. Applied Sciences, 9(21), p.4530.

[4] Leveson, N., 2004. A new accident model for engineering safer systems. Safety science, 42(4), pp.237-270.

A. Approach Name and Type	Swiss Cheese Model	
	An Epidemiological Methods Approach	

B. Approach Rankings Summary	Applicability to UK System of Infrastructure	High (5/6)
	Cross Sector Applicability	High
	Strategic Relevance to NIC	High

C. Approach Applications and Comparability Scores by System	**System**	**Comparability Score**
	Systems: Medical/healthcare/clinical Systems	High (5/6)
	Facilities: Hospitals	High (5/6)

D. Approach Purpose	Systemic Analysis: Error Identification, Classification and Management
	Systemic Analysis: Organisational accidents
	Systemic Analysis: Active Failures (typically Human Factors) and Latent Conditions
	Systemic Analysis: Safety warning signs (mishaps, incidents, near misses, free lessons)
	Systemic Analysis: Safety and Accident
	Systemic Analysis: Root causes Analysis and potential Failure modes
	Systemic Analysis: Reliability
	Systemic Analysis: Reasons for/cause of system failure

E. Approach Key Concepts		
		Error-provoking conditions (and condition types)
	Latent Conditions	Learning, Mindfulness and Reporting Culture
	Defensive Layers (Defences, Barriers, Safeguards)	Error analysis and Management (reduce errors)
	Holes / weaknesses in Defensive layers (and types)	Error Analysis and Management (limit error impacts)
	Accident Opportunities	
	Risk Factors (and Risk Factor types)	

F. Data Requirements and Availability	Generic data requirements are not important
	Primary data is essential
	Significant additional secondary data is required
	Specialist knowledge of the system of interest is essential

G. Skills and Resource Requirements	Specialist Software is not needed
	Approach specific training is recommended
	Cross sectoral collaboration between experts from multiple sectors is recommended

H. Complementary Approaches	Error Analysis	
	High Reliability Organisation Theory	
	Normal Accident Theory	

J. Approach Overview

Swiss Cheese Model, A System Model Approach

Defences, barriers, and safeguards occupy a key position in the system approach. High technology systems have many defensive layers: some are engineered (alarms, physical barriers, automatic shutdowns, etc), others rely on people (surgeons, anaesthetists, pilots, control room operators, etc), and yet others depend on procedures and administrative controls. Their function is to protect potential victims and assets from local hazards. Mostly they do this very effectively, but there are always weaknesses.

In an ideal world each defensive layer would be intact. In reality, however, they are more like slices of Swiss cheese, having many holes—though unlike in the cheese, these holes are continually opening, shutting, and shifting their location. The presence of holes in any one "slice" does not normally cause a bad outcome. Usually, this can happen only when the holes in many layers momentarily line up to permit a trajectory of accident opportunity—bringing hazards into damaging contact with victims Figure 1.

The holes in the defences arise for two reasons: active failures and latent conditions. Nearly all adverse events involve a combination of these two sets of factors.

Active failures are the unsafe acts committed by people who are in direct contact with the system. They take a variety of forms: slips, lapses, fumbles, mistakes, and procedural violations. Active failures have a direct and usually short lived impact on the integrity of the defences. At Chernobyl, for example, the operators wrongly violated plant procedures and switched off successive safety systems, thus creating the immediate trigger for the catastrophic explosion in the core. Followers of the person approach often look no further for the causes of an adverse event once they have identified these proximal unsafe acts. But, as discussed below, virtually all such acts have a causal history that extends back in time and up through the levels of the system.

Latent conditions are the inevitable "resident pathogens" within the system. They arise from decisions made by designers, builders, procedure writers, and top level management. Such decisions may be mistaken, but they need not be. All such strategic decisions have the potential for introducing pathogens into the system. Latent conditions have two kinds of adverse effect: they can translate into error provoking conditions within the local workplace (for example, time pressure, understaffing, inadequate equipment, fatigue, and inexperience) and they can create long lasting holes or weaknesses in the defences (untrustworthy alarms and indicators, unworkable procedures, design and construction deficiencies, etc). Latent conditions—as the term suggests—may lie dormant within the system for many years before they combine with active failures and local triggers to create an accident opportunity. Unlike active failures, whose specific forms are often hard to foresee, latent conditions can be identified and remedied before an adverse event occurs. Understanding this leads to proactive rather than reactive risk management.

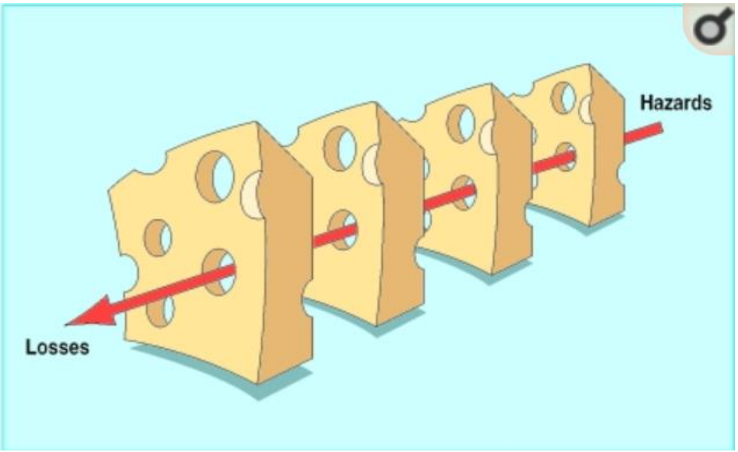

Figure 6 The Swiss Cheese model of how defences, barriers, and safeguards may be penetrated by an accident trajectory (adopted from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/)

K. Approach Literature:

[1] Systems Approach, Patient Safety Primer, U.S. Department of Health and Human Services, http://psnet.ahrq.gov/primer/systems-approach
[2] Reason., James, Human error: model and management, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1117770/
[3] Cross, S.R.H., 2018. The systems approach at the sharp end. Future healthcare journal, 5(3), p.176, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6502592/

End of report