Managing Unexpected Risks Event Report

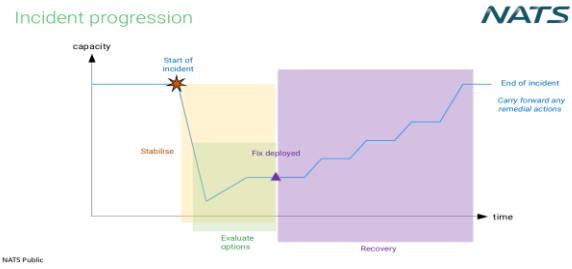


The Seminar "Managing Unexpected Risks: Handling Rare and Severe Events Now and in the Future", took place in person at the BCS offices in London and online on 26th May 2022. Paul Hampton and Martin Atkins provide the highlights of the event.

The event opened with Mike Parsons, SCSC Managing Director, introducing the concepts of 'Black Swans'. He said that increasingly complex systems and new technologies like autonomous vehicles are presenting new opportunities for the occurrence of Black Swan events.

Managing Novel Incidents

The first presentation was by John Holmes from NATS, the UK air traffic service provider, on the topic of Managing Novel Incidents. John talked about an incident associated with a well-established system.



Traffic was low due to an overnight storm and there was an intermittent fault with a radar display system in the morning resulting in delays. Intermittent low-level packet loss was being experienced on a network switch, but it was decided not to replace it, because of the storm. However, a

switch on the redundant network then also failed, resulting in track data blocks – data associated with the trails displayed on Air Traffic Control (ATC) displays – being intermittently lost.

To deal with the situation, NATS implemented traffic control methods, by reducing the number of aircraft taking off. The fault was diagnosed and a fix was completed in around 4 hours.

There is a mature hierarchical incident management system at NATS and incidents are escalated based on the level of impact. This is well-exercised through training. However, analysis of the event found that:

- There was loss of a single point of truth between ATC and Engineering
- Focus was on the controller positions but less on other affected systems connected to the same network
- There was inconsistent use of language and communication between different stakeholders
- There was insufficient recording of the decision-making process to provide evidence that the correct actions had been taken

Although the team arrived at what proved to be the correct course of action, these good decisions were not an inevitable product of the process.

Following an investigation, NATS developed a more prescriptive process for evaluating options for risks, benefit and trade-offs and a set structure for recording decision rationale. This was based around a structured series of questions, but was not adopted in the end, as it was felt to be cumbersome and risked stifling the flexible and reactive nature of the more informal problem solving approach.

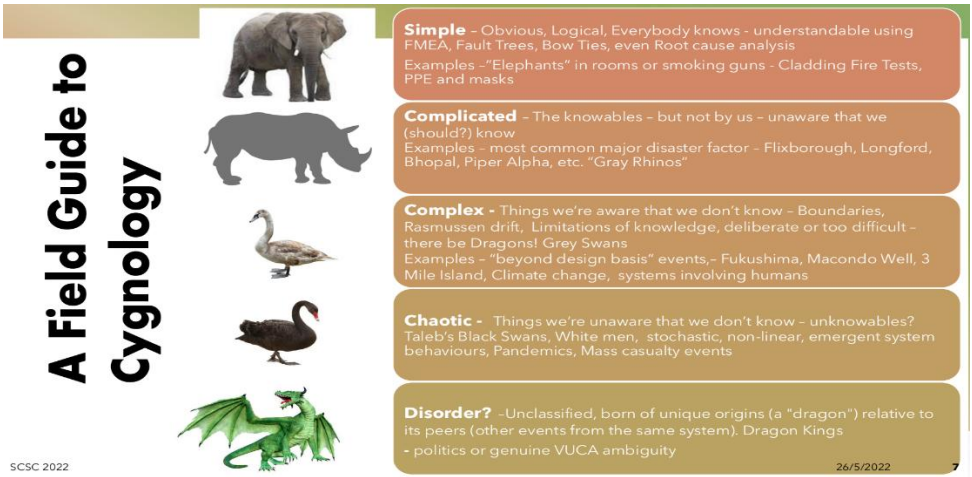
It was acknowledged that there is heavy reliance on highly trained, skilled, adaptable and empowered people and NATS decided to create a better training programme for staff to ensure there is a clear framework for necessary discussions, retaining flexibility and pace.

Black Swans - Decisions under Uncertainty

David Slater from Cardiff University presented on the importance of instinct, experience, and time for thinking in emergencies.

"Normal" emergencies are usually well-handled as the system is well understood but 'black swans' are different as we are dealing with the 'Unknown Unknowns' as famously expressed by Donald Rumsfold.

David introduced a range of complexity categorisations from Obvious or Simple (the known), Complicated (the knowable), Complex (the unknowable), Chaotic (incoherent), Disorder (not determined). He introduced a 'Cygnology' for these systems and gave examples: for Complicated emergencies, he gave examples of Bhopal and Piper Alpha and for Chaotic emergencies, he gave Black Swan events, such as Pandemics.



The Cynefin framework helps the decision-making process but David noted that there can be drift between quadrants (Rasmussen Drift).

David gave further examples of Simple, Complicated and Complex accidents and gave examples of real Black Swans in the Chaotic category such as 9/11, Covid-19 and the shelling of Ukrainian Nuclear Power stations.

David then went on to discuss what we can do about managing these types of events. There is acceptance that Chaos does happen, we live in a complex environment, but we have evolved to survive in these environments. Planning and training are seen as important but is 'robotic' Plan Do Check Act (PDCA) methodologies sufficient? David discussed other models such as John Boyd's OODA loop (Observe, Orient, Decide and Act). Klein also had a model called Recognition Primed Response. But the real question is whether there is time to think logically or read the manual during a crisis.

David also referred to Kahneman's thinking 'fast and slow' with system 1 being automatic and little or no effort and no sense of voluntary control. System 2 allocates attention to the effortful mental activity.

He referred to Libet's experiment and the complexity of the brain.

David noted how people respond differently to emergency situations and referred to the Fukushima Daini (No 2) plant which survived a similar set of problems to the Daiichi (No 1) plant that experienced the well-publicised meltdown. The No 2 plant was saved due to innovative human ingenuity to help route power after the flooding by the tsunami. David thought that AI systems can help in the simple or more complicated systems, but their inflexibility could limit their utility in more complex situations.

David concluded that the instinct, experience and time for thinking in emergencies is critical. It's important to have more than just classroom-based training, there should be empowerment of those responsible, leadership not micromanagement, team leading and building resilience.

The Buncefield Explosion

Martin Atkins from MCA Ltd discussed the events surrounding the Buncefield Explosion. He defined a Black Swan as an event that is a surprise, has a major impact and in hindsight, is rationalised as predictable.

He stressed however, that Black Swans are very much 'in the eye of the beholder' and relative to role an affected party plays in an incident.

The Fuji Building



Martin discussed the Buncefield Site in 2005, an Oil Storage Terminal near Hemel Hempstead, the 5th largest oil storage depot in the UK with a capacity of 60,000,000 gallons and filling ~400 tankers a day.

Each tank had 3 indicators if it was full: a gauge, another (which was not operating at the time) and a backup full/empty switch that was intended to be an independent safety mechanism.

For tank number 912, only the backup was operational and the gauge was known to stick occasionally. A lever selected whether the backup was looking for full or empty and was supposed to be locked in the full position. However, the padlock to protect this was never fitted and there is some doubt of which mode was selected.

There were also design and construction issues: the tank construction caused overflowing fuel to "bounce" and increase evaporation, and the walls ("bunds") between tanks could not contain a spill due to gaps and bad gaskets.

Early in the Sunday morning of the incident, the tank was being remotely filled and started to overflow, with about 250,000l of fuel making a pool 2m deep. There were then several explosions with the largest one being a "fuel-air" explosion, which was felt 28 miles away. This led to a fire that burned for 3 days.

This in itself was not a Black Swan event, being a conventional failure of safety mechanisms. However, when considered from the perspective of organisations situated in buildings adjacent to the site, this was clearly a Black Swan event. One building in particular, the Northgate building, contained a datacentre which contained the Schengen Information System, the Police National Computer's hot stand-by backup system and the Addenbrookes Hospital Admission and Discharge system. Further afield, other consequences included the closure of a motorway, fuel rationing of flights at Heathrow, closures of schools and public buildings, and pollution from the fire and the fire-fighting chemicals.

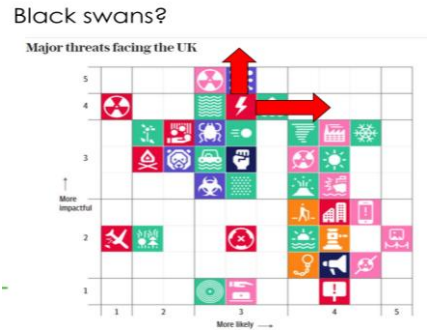
Martin then discussed an issue in January 2021 where data was accidentally deleted from the Police National Computer; it took ~15 weeks to recover the records, which could not have been helped by the hot stand-by backup system, destroyed during Buncefield event, never having been replaced. Martin argued that although the event itself was a normal predicted event, it became a Black Swan event for many people outside, such as businesses, a hospital, the Police, the environment etc.

Martin concluded that there will always be Black Swan events, but whether it counts as a Black Swan depends on who you are.

Martin suggested that to protect against these events requires approaches that are not dependent on the nature of the disaster, such as Disaster Recovery planning and "general" resilience. Organisations need to take a wider view, not just within themselves, but also including their suppliers, the physical surroundings and how failures in external organisations may affect them.

Hunting Black Swans in Power Grids Related to EV Charging and Satellite Navigation Timing Signals

Andrew Larkins from Sygensys Ltd discussed Black Swans in the context of Power grids.



Failures of power grids typically arise from severe weather, failures and supply imbalance and these can have significant impact as there is an extreme societal dependency on power. For example, outages in 2021 in Texas led to many businesses being left without power for several days and there were hundreds of fatalities associated with the event.

The dependency on power is reflected in the National Risk Register with impact at the high end and medium likelihood.

Andrew said that the introduction of electric vehicles (EV) will increase the load on the grid and represents a rapid change that will present a significant challenge to grid operators – by 2035 charging is predicted to be over 40% of the total load at certain times of the day.

A key question is whether the system will still work when faced with these external challenges, and so, this might be a good hunting ground for Black Swans. Andrew found that there were no detailed investigations about the impact of the short-term stability of EV charging after a fault, to prevent a "domino" effect occurring.

Andrew said to help hunt potential Black Swans you need time, skill and freedom to think around the issues.

EVs, by their nature, are high demand and users will want to charge on low tariffs in a smart optimised way, and there is the potential to manage this using IOT technologies. This means that the operator can shift from varying the supply to match the demand, to controlling the demand itself, but this introduces new failure modes.

Andrew suggested some of types of teams and techniques required to explore Black Swans, such as cross-functional teams, mix of generalist and specialists and trying to get people to think in different ways.

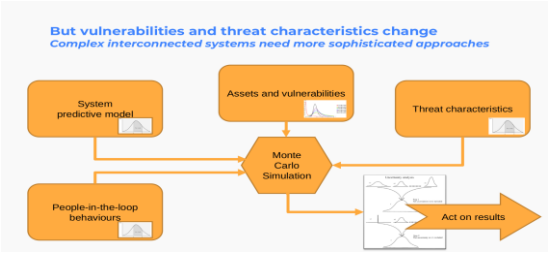
The results of a number of workshops in this area resulted in 6 ways in which EV chargers can present a risk to grid security. For example:

- Step: Too many chargers switching on or off at the same moment
- Ramp: Too many chargers switching on or off within a few minutes
- Oscillations: a group of chargers switching on and off repeatedly
- Degraded stability: increases risk of post-fault collapse
- Demand control: deficiencies are eroded
- Restoration: Erratic behaviour after restart hindering process of restoration.

Andrew asked whether it can be classed as Black Swan if it is predicted before it happened. His focus is on how to fix these future issues but noted there is, for various reasons, resistance from industry to focus on this area at the moment.

Andrew concluded with a discussion on Satellite navigation signals, which are subject to Jamming and Spoofing despite the high dependency that modern society has on them, and so are potential future sources of Black Swan incidents.

Grey Swans



Bill Blackburn from Process Renewal Group concluded the afternoon session with a discussion on Grey Swans. Bill noted that things do happen, such as financial collapses and security breaches that affect large volumes of people.

Bill noted that there are a large number of regulators but noted that it is impossible to regulate away risk and regulators are quite fragmented. Often companies align their organisations around the regulator requirements, compliance is more 'tick box' and regulators struggle to keep abreast of change.

Bill then showed the national risk register and noted that there are several risks that are clearly safety-critical but others that might be classed as safety-related such as Cyber attacks, serious and organised crime and animal diseases.

Bill discussed what items were not in the national risk register such as the Stephen Hawking warning around AI being the 'best or worst thing' for humanity, which then brought in the question around ethics.

Other areas are Quantum computing, which might bring benefits, such as improving the accuracy of inertial GPS systems (eg. using quantum accelerometers and gyroscopes), but might have downsides, such as undermining current encryption techniques. Bill asked how best to gain this foresight and noted that some government organisations like the Department for Business, Energy & Industrial Strategy (BEIS) are doing horizon scanning and commissioning others like the Royal Society to glimpse into future technologies, such as computer/neural interfaces.

Bill said that Quantum Computing, AI and Ethics are hot topics for lawyers who are exploring these areas as potential future areas of litigation.

Bill said the UK Financial Conduct Authority (FCA) are building resilience into financial services after various crashes and discussed some of the challenges the FCA see, such as, technical innovation (AI, blockchain, crypto assets), changing behaviour, keeping pace, challenging environments and system complexity.

Assessing threats in the real world is expensive and can be dangerous and Bill noted some commonly used approaches – techniques (such as those in SCSC Guidance documents), system modelling, crisis-management and simulations.

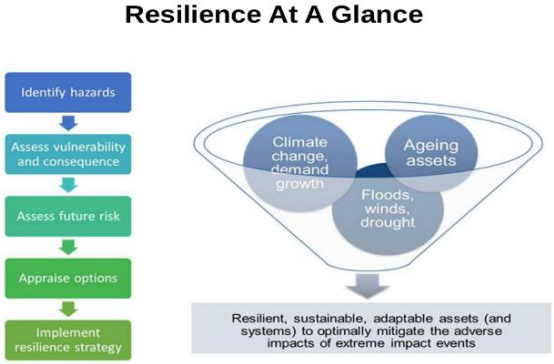
Vulnerabilities also evolve, for example, behaviourally with people moving to higher risk areas, the demand for greater mobility and overuse of drug/antibiotics. New business models and technology adoption and supply chains can often mask vulnerabilities and can have exposure to cyber threats.

Bill concluded that the Royal United Services Institute's (RUSI) viewpoint of the National Risk Register is that half of the risks are missing. Having an entry on the register does not mean that we have methods to manage the risk.

Safety and Resilience of Designs of the Future

Wendy Owen from Bangor University discussed resilience and the work she has been involved in with the Institute of Asset Management (IAM) working group producing SSG-32 Contingency Planning & Resilience Analysis.

Wendy started by explaining the terminology around resilience, resilience analysis and contingency planning. She discussed the resilience analysis process and some points around resilient organisations being typically forward thinking.



She gave examples of the typical processes where resilience analysis is undertaken and contingency planning activities are developed.

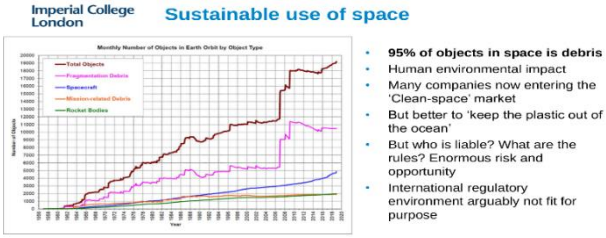
- Prevention: technique used to prevent the issue from occurring
- Response: what is done to respond to an issue once it has occurred
- Recovery: how to return the business back to normal operations and importantly want to learn lessons and prevent reoccurrences

Wendy provided several case studies that were in SSG-32 such as the Pacific Gas & Electric San Bruno (2010) rebuilding after a gas explosion.

In this study, after the incident, rather than abandoning the site, they rearchitected the site with automation, replacement of pipeline, testing and enhanced telemetry and set their goal to be the safest and most reliable company in the industry.

Wendy also noted that there are standards for Business Continuity Management (BCM) such as those used by Network Rail. Some BCMs can use questionnaires to help structure assessments.

Space Weather Risks



The final presentation was pre-recorded by David Southwood and Jonathan Eastwood from Imperial College and introduced in the meeting by Bill Blackburn. David introduced Jonathan as an expert in Space and Atmospheric Physics at Imperial College London.

Jonathan explained what Space Weather meant and he noted it was on the national risk register. He said auroras are the most recognisable visible part of a much larger system resulting from solar activity. Solar flares are common but there are also Coronal Mass Ejections (CME) from time to time that take about 1 or 2 days to reach the Earth but can have significant interaction with the Earth's Magnetosphere.

Jonathan then discussed the worst that could happen from a severe space weather event, typically those that might occur every 100 years. There is real concern that it can disrupt the supply of electricity. Other impacts would be PNT (Position Navigation and Timing) signals from GPS. In space, it can affect the services provided by satellites, and the satellites themselves.

Jonathan gave an example, of a weather event in 1989 that affected supplies in Quebec, North America. However, this was not as severe as that thought to have occurred in 1859, known as the 'Carrington' event.

In another example, in February 2022 SpaceX launched 40 Starlink satellites, but lost most of these because of a small geomagnetic storm.

Space weather is hard to assess as many extreme events have not occurred in the modern technological era. Each event is unique and could last for a period in the order of two weeks. Jonathan asked for feedback from this community about this topic.

Jonathan made some observations:

- The economic impact could be huge based on studies
- Many organisations are not aware of their reliance on space infrastructure and how their products may be exposed to space weather
- There is much more predicted use of satellites in space, such as ubiquitous internet access, and this will bring new challenges, such as managing the 95% of objects now in space, which are debris

Jonathan concluded by asking what a reasonable response is to space weather risk?