Using Big Data to Understand Complex Warship Asset Risk

Authors

Lead Author: Lt Will Thomas BSc (Hons), MSc, MIET IEng RN
Contributing Author: Cdr Suzanna Seagrave MBE RN

Synopsis

Modern complex warships, amongst the most complicated machines ever built, must be both sustainable and safe to operate. Understanding overall complex warship asset risk requires holistic assessment of every factor which could add to availability or safe to operate risk, including logistical, personnel, engineering support and performance data. Risk is presently evaluated through best human judgement, with many disparate data streams of available data analysed by multi-disciplinary teams; however, the volume of data generated is overwhelming. There is a need to provide an aggregate assessment of risk to pre-empt and prevent accumulated risks from becoming large issues. This is balanced against the challenge of information-overload; if every possible risk is flagged as a warning or a priority then this is also counterproductive. The emergence of the ability to integrate big data has provided opportunities to better predict and manage warship availability and the safe to operate envelope through the automation of data. This paper proposes a model for an availability and safe to operate risk tool which could be used to enhance understanding of the risk to sustaining readiness and maintaining a safe to operate position. It proposes a method to analyse the sub-components of capability taking into account all supporting elements as well as criticality analysis to aid prioritisation. Key is to understand the thresholds at which a capability is lost. This paper proposes an expert system which will integrate available data sets to deliver a better understanding of complex warship availability and safety whilst also considering some of the challenges which will arise as higher fidelity of the overall picture is attainable.

Keywords

Digitalisation; Big Data; Expert System; Risk; Machine Learning

Biographical notes

Lt Will Thomas RN joined the Royal Navy in 2001 and has served in a variety of roles. He presently works in In-Service Capability Management for Capital Ships in Navy Command, supporting safety, security and availability of the platforms. He completed a BSc in 2014 and read for an MSc in Engineering and Management at Portsmouth University with a thesis on digitalisation, certification and assurance, graduating in 2021.

Cdr Suzanna Seagrave MBE RN joined the Royal Navy as a Marine Engineer in 1999. She is currently the Renown 'Data Sherriff' working to automate the integration and exploitation of support data from dozens of legacy systems, some of which are older than she is, to improve platform availability. She was awarded an MA in Defence Studies by KCL in 2019 with a dissertation on the Implications of AI for Military Leadership and is awaiting final results for an MSc in Computer Science and AI.

1. Introduction

Modern complex warships, amongst the most complicated machines ever built, must be both sustainable and safe to operate. Warship complexity is amplified by the integration of the Defence Lines of Development (UK Gov 2009) to deliver capability. Therefore, understanding overall complex warship asset risk requires holistic assessment of every factor which could add to availability or safe to operate risk, including logistical, personnel, engineering support and performance data. Risk is presently evaluated through best human judgement, with many disparate data streams of available data analysed by multi-disciplinary teams; however, the volume of data generated is staggering. Whilst the data may all be tracked as a line on a spreadsheet or database the overall risk is exceptionally challenging, if not impossible, to quantify using existing techniques which may lead to catastrophic events. For example, Haddon-Cave's investigation (2009) argues that the complex accumulation of risk is a significant contributing factor to the Royal Air Force Nimrod crash, 2006. Moreover, history provides further prominent examples including the Challenger space shuttle explosion, 1986 (Brummer 1986), and the Piper Alpha disaster, 1988 (Cullen 1990).

With huge volumes of data to analyse, which is continuously changing, there is a need to provide an aggregate assessment of risk to pre-empt and prevent accumulated risks from becoming large issues. This is balanced against the challenge of information-overload; if every possible risk is flagged as a warning or a priority then this is also counterproductive.

The emergence of the ability to integrate big data has provided opportunities to better predict and manage warship availability and the safe to operate envelope through the automation of data. The topic of this paper is the development of a model for an availability and safe to operate risk tool which could be used to enhance understanding of the impact on sustaining readiness and cost implications on scheduling decisions and the delivery of high-quality safety and capability data to guide decisions. This paper proposes an initial model, prioritised and weighted against mission criticality, with thresholds set at which a capability is lost. It integrates available data sets to deliver a better understanding of complex warship availability and safety.

2. *The emergence of Big Data*

'Data is the new oil.' (Humby, 2006)

The volume of data produced in the modern word is mind-bogglingly vast; in 2022 alone there were 2.5 exabytes of data created each day (Wise 2022). Moving forward and data creation is predicted to increase to 180 zettabytes by 2025 (Statistica 2022)! This has resulted in a worldwide phenomenon known as the 'Data Deluge':

'the sheer volume of new data, "the Data Deluge", is overwhelming the capacity of institutions to manage it and researchers to make use of it.' (United States Government 2007)

Whilst the 'Data Deluge' impacts the business world, it also has a significant impact on military decision makers, for example, in deciding where to focus resource for the best result.

Despite the challenges posed by big data, the emergence of tools giving an ability to integrate it provides opportunities to better predict and manage warship availability and the safe to operate envelope through the automation of data and through 'datafication'. The term 'datafication', first coined by Mayer-Schönberger and Cukier (2013), is the process of capturing any aspect in a digital format. Arguably anything may be subject to 'datafication', and this had led to the emergence of digital twins.

3. *Digital Twins*

'A digital twin is a virtual representation of an object or system that spans its lifecycle, is updated from real-time data, and uses simulation, machine learning and reasoning to help decision-making.' (Armstrong 2020)

Digital twins were first conceptualised in 2002 (Grieves and Vickers 2017 cited Grieves 2002) and are now emerging as commonplace in industry, as digitalisation is embraced. They provide a method to digitalise systems for analysis, and this technology is also useful for militaries. However, there are subtle differences between the requirements for industry and military use. If the reader firstly considers a civilian use of digital twin technology in a wind turbine.

Digital twin technology could be incorporated at the design phase to model the wind farm using cloud-based technology. This enables different components and configurations to be tested in simulation to select the optimal solution based on the real-life characteristics of the wind flow and topography of the wind farm. Once commissioned, embedded sensors would gather real world system performance data which could be analysed to enable the system to be optimised as well as monitored for efficiency of maintenance and defect repair. This has the potential to optimise performance, reduce down-time and also expenditure on unnecessary work.

All of these things we would aspire to be able to do with our warships, however, unlike a warship a wind turbine will only have a limited number of independent variables in comparison, such as the angle of the blades or indeed how windy it is. Also, unlike a warship it will have been mass produced with large volumes installed throughout the world from which to gather meaningful statistical data. For the wind turbine sensor data may be analysed and, with a relatively minimal number of parameters, machine learning methods may then be applied which will look at similarities and trends.

4. *The complexity of Military Capability*

And now if the reader considers why applying the same methodology to a combat system or military capability poses significant challenges for the techniques that work well in many civilian applications. A combat system or capability is termed as 'a set of human and technological resources which comprise the fighting capability of a platform.' (UK MOD 2018). Arguably, this definition could be extrapolated to encompass every resource, both organic and inanimate, that comprises a warship; whilst warships are used for other purposes, their expense is justified solely in their fighting capability/survivability.

There are scale differences in complexity when considering the military use of a capability or a combat system as opposed to a civilian use of an equipment. The base equipment of, for example, a destroyer, could be considered as equivalent to the wind turbine. However, to make this into a usable capability all the Defence Lines of Development (DLoDs) as well as arguably the entire military support organisation must be integrated which presents a much greater magnitude of complexity; ‘complex data’ instead of merely ‘big data’. When calculating both the cumulative risk to capability and for safe operation the DLoDs, in Figure 1, must therefore all be considered:

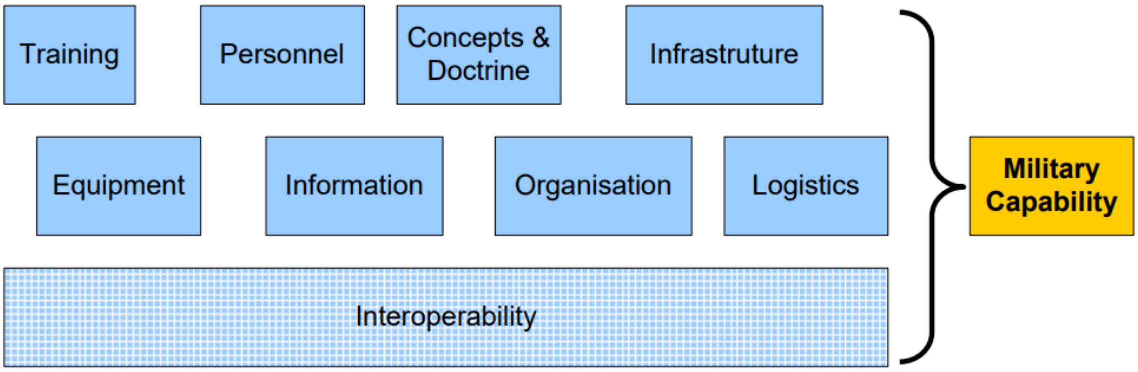

Figure 1 – Defence Lines of Development (UK Gov 2009)

Relating Figure 1 to the civilian use referred previously, and to highlight the scale difference in complexity, the wind turbine would be the ‘Equipment’ block. An equivalent ‘value generating’ asset in the military might be a naval destroyer. Noting that modern naval destroyers are already entitled complex warships due to their integration, this in itself indicates the challenge ahead.

5. *The sub-Components of Military Capability and Safety*

Using the example of a typical naval destroyer, Figure 2 represents a non-exhaustive list of possible capabilities:

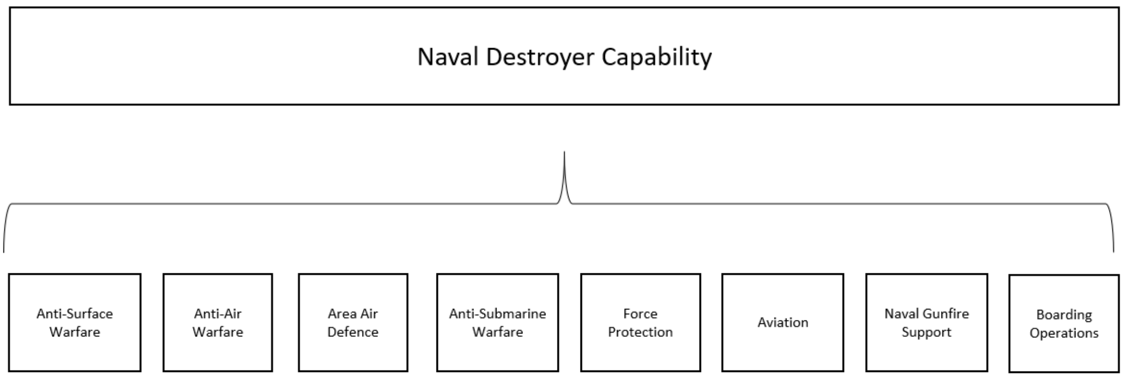

Figure 2 – Naval Destroyer Capability

The capabilities within Figure 2 may be broken down further to the next level to the grouping of equipment that forms the capability. Whilst, in the real world, significant redundancy is designed into complex warships, for the purposes of this paper a simplified grouping of equipment comprising area air defence is shown at Figure 3:

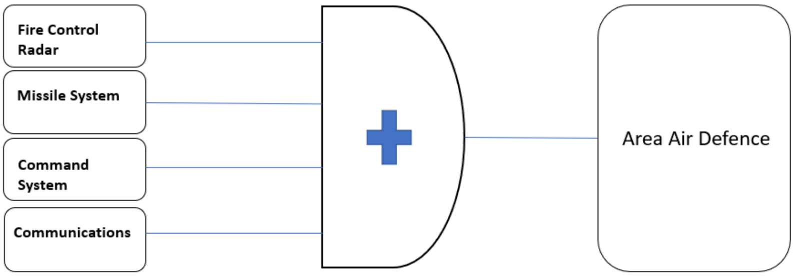

Figure 3 – Area Air Defence Equipment

If all equipment comprising the area air defence capability is at the specified performance (green), then the capability is also determined to be available to the operators as shown in Figure 4:

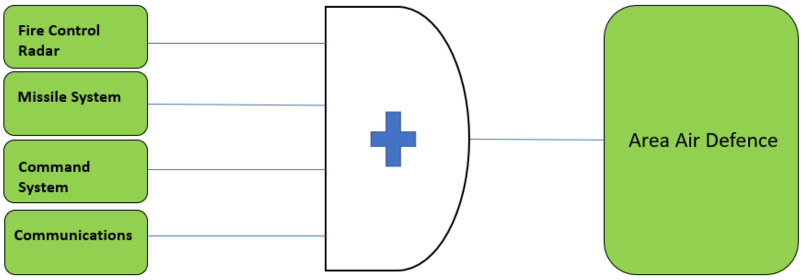

Figure 4 – Area Air Defence Capability Performing Correctly

However, changes in availability of the sub-components may affect the assessment of the overall capability. A total failure of the missile system, for example, would mean area air defence could not be completed, as per Figure 5:

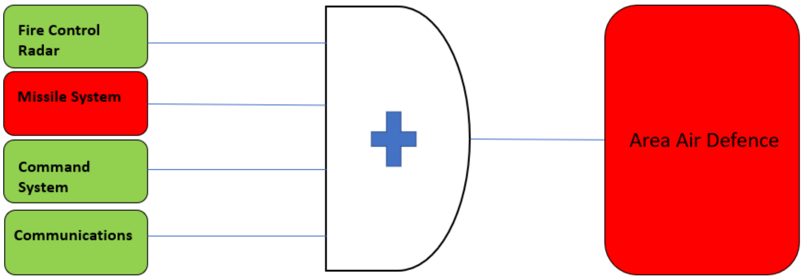

Figure 5 – Area Air Defence Capability Inoperable

Alternatively, there may be an equipment fault in the fire control Radar, but it could still be used in a less capable reversionary mode, as per Figure 6:

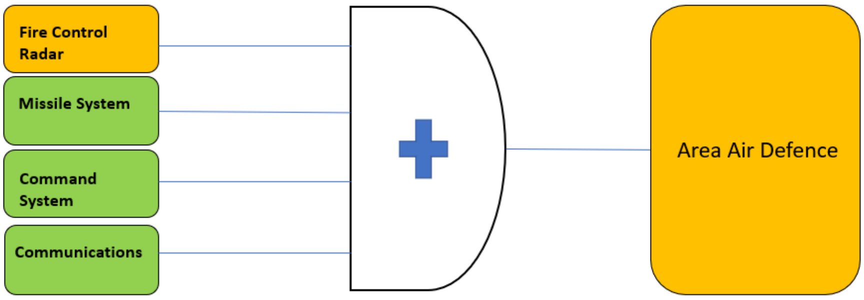

Figure 6 – Fire Control Radar Degraded

Moving down a level further, each of the equipment comprising a capability may also be mapped for sub-components. One key sub-component here is the availability of competently trained maintainers and operators. If accurate competence data is available then it is a key indicator of both the sustainability of capability and the ability to make a safe to operate declaration. A (non-exhaustive) basic analysis of other sub-components impacting the availability of a fire control radar is at Figure 7:

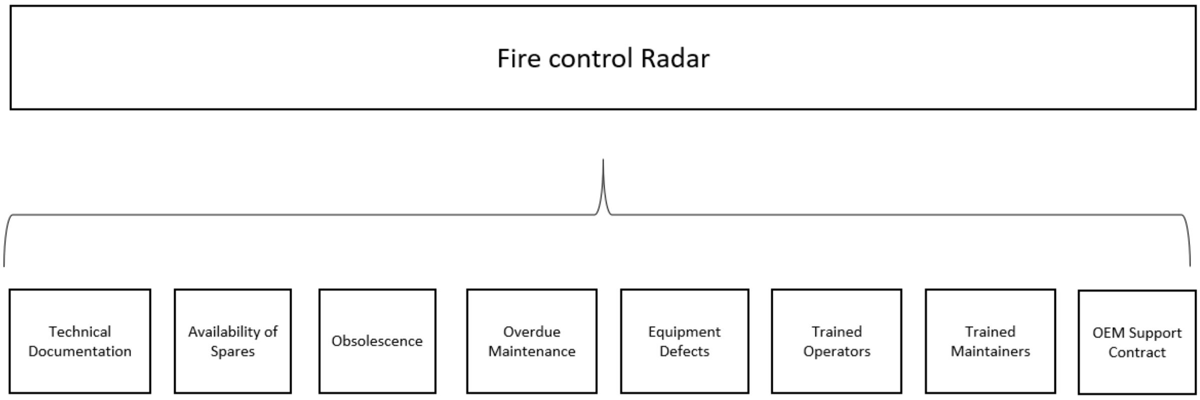

Figure 7 – Factors Impacting Fire Control Radar availability

Whilst this paper will not analyse to the next lower level as the methodology has been highlighted with the examples given, each of the factors in Figure 7 could also be broken down further to sub-components continually, providing greater granularity as necessary. To complete the model of the destroyer, a digital representation of each component would be required, gaining in accuracy but also complexity as more granularity is introduced. This could come from data within existing databases or from new 'datafication'.

Figure 8 integrates Figures 2, 3 and 7 to show a very basic dependency map. Whilst a simplified example has been demonstrated, if the reader begins to mentally extrapolate Figure 8 to encompass all of the systems integrated to a typical naval destroyer, then this rapidly becomes more challenging to interpret, and highlights the need for a digital solution:

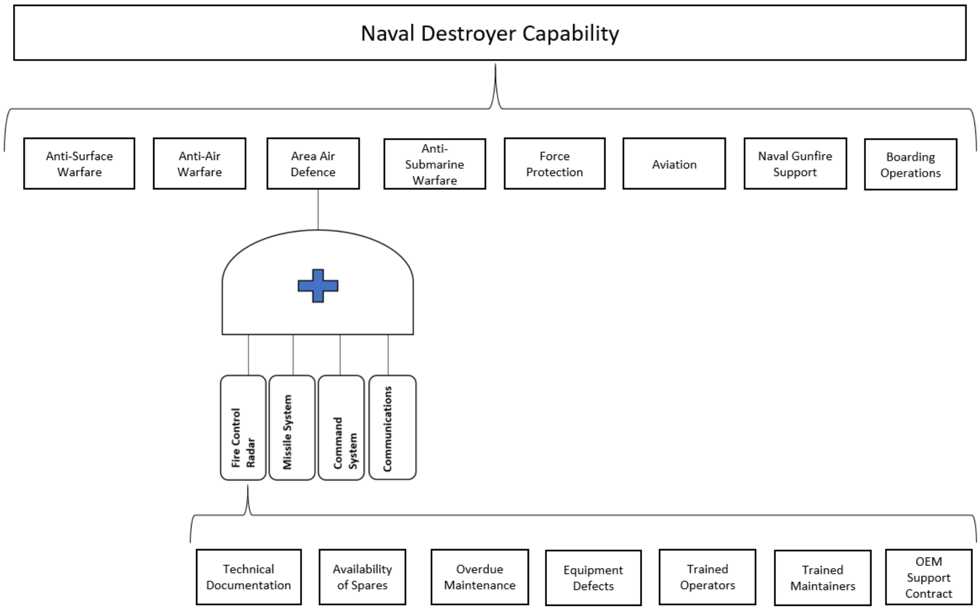

Figure 8 – Overall Assessment of Capability

6. *Other Uses*

Having introduced the concept through the lens of availability of capability, the model could provide a digital representation with uses to a broader user community. This includes being used to determine whether a warship is safe to operate.

The model could provide a decision-making tool confirming whether the predetermined threshold for a safe system had been met. This would take inputs from certification and other related databases, considering the equipment and assets that are required to safely operate a platform, as in the non-exhaustive diagram of the requirements (equipment only for simplicity noting there would also be a significant personnel competence element unrelated to equipment) to safely sail a warship at Figure 9. Of note, each of the individual equipment feeding the safe to sail analysis would also have underpinning analysis of sub-components as per the previous fire control radar example in Figure 7:

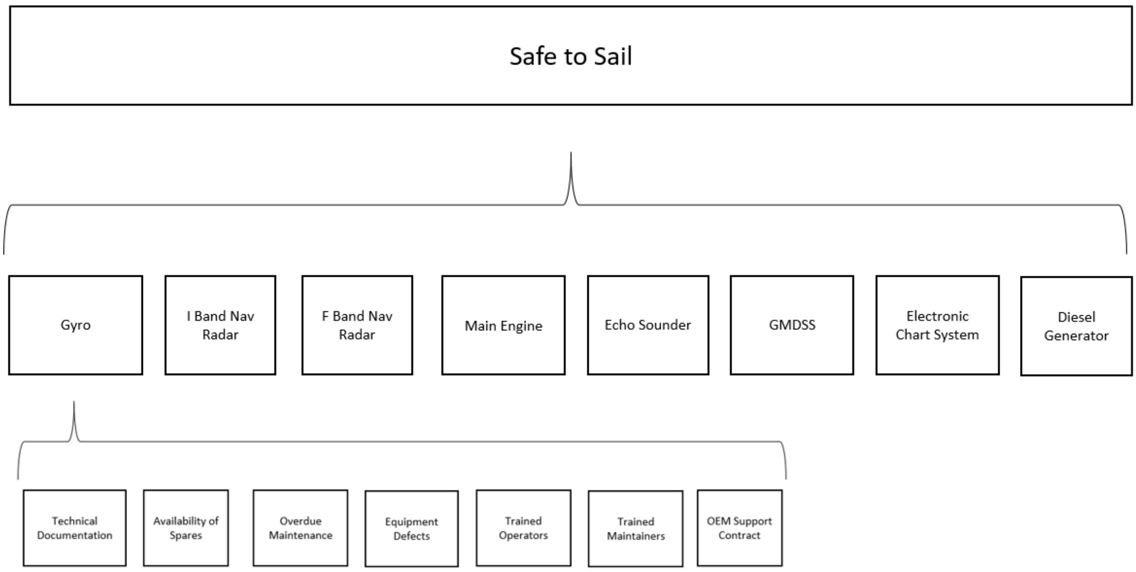

Figure 9 – Safe to Sail

While the capability example previously looked at a single warship, feasibly any capability could be modelled, providing Operational Commanders with an automated analysis of the availability of the assets at their disposal, or readiness for particular tasking. This would also provide a single point of truth across the organisation, with the removal of personnel driven ‘optimism bias’, due to the automation. For example, the risk to availability of capability across a task group comprising an aircraft carrier, two destroyers, two frigates, support vessels and a submarine. Whilst this is done through human analysis at present, this would just be an extension of the model. However, with the number of different taskings that may be performed, all with different capability requirements, it may be necessary to create or modify existing models to suit.

7. *Trip Wires*

Having considered the broad concept of digitised availability and safety modelling, the real ‘so what’ is related to forecasting the emergence of risk and mitigating it well in advance of it becoming an issue. The cumulative effect of low-level defects and other impacting factors can present an unseen threat. In Figure 10, the known risk is obvious, as the visible part of the iceberg. This might be, for example, a defective missile system. However, beneath the surface lies a staggering amount of unquantified risk. Consider a platform that has four diesel generators and requires two diesel generators to be functioning to be able to sail. There may be two functional diesel generators, but a large volume of low-level defects on one of them, or maintenance that is subject to concessions and has been deferred. How well is the overall picture understood?

Figure 10 – The Risk Iceberg

This is where trip wires could be built into the model, to forecast risks which could then be mitigated before they became issues. Noting the significant challenges that would be faced by programmers in building a fully integrated warship digital twin due to their sheer complexity, an ‘expert’ system with rules built in may be imminently more achievable.

8. ***Expert Systems***

'An expert system is a computer program that uses artificial intelligence (AI) technologies to simulate the judgment and behaviour of a human or an organization that has expert knowledge and experience in a particular field.' (Peterson 2016)

'Expert-systems' are often described as 'automated' rather than 'autonomous'.

'The decisions made or actions taken by an automated system are based on predefined heuristics. An autonomous system, on the other hand, learns and adapts to dynamic environments, and evolves as the environment around it changes.' (Matteson 2019)

This is relatively simple for a wind turbine operator to achieve, with minimal complexity built in for redundancy and the ability to schedule maintenance periods that are never changed or postponed due to operational requirements.

However, it will be highly complex to achieve for warships as there is a lot of redundancy built in to enable reversionary modes allowing battle damage to be absorbed. Moreover, the complexity of risk due to the redundancy builds in a cushion for the operator which is also a part of their consideration as it is still highly possible to safely operate a warship with a large volume of defects when used for benign tasking. In a military context, a 'benign' tasking can change to a 'high intensity' tasking overnight. An illustration would be the re-deployment of units to support operations in Libya following the Arab spring. Thus paradoxically the imperative to meet short-term lower intensity demands and the ability to do so using in-built redundancy creates a form of moral hazard where the consequences of eroding redundancy materialise at greater cost in the future.

Maintaining a sufficiently detailed picture to understand cumulative risk with constantly changing information is time consuming and challenging for the programmer, so, dependent on the desire, an initial triage could be completed using a criticality analysis to identify the primary systems of interest in buckets as Priority 1, 2 or 3. An example of a Priority 1 system might be a diesel generator, whereas a Priority 3 might be the satellite TV system.

For the systems identified as critical, rules could be included. Consider the example of the diesels, a rule can be added whereby:

a. Low level alert = 3 of 4 diesels operating

b. Medium level alert = 3 of 4 diesels operating AND > 1 low level defect on at least 1 of 3 remaining diesels

c. High level alert = 3 of 4 diesels operating AND > 1 low level defect on at least 2 of 3 remaining diesels

Such trip wires could be provided across all systems. Although the example of the diesels is very simplistic, this would provide meaningful alerts from within the 'data deluge'. It would also enable a more accurate targeting of resource towards potentially previously hidden cumulative risks.

9. ***Moral Hazard***

'Moral hazard' occurs when 'people behave differently if they do not face the full costs or risks of their actions' (Balafoutas et al. 2017). This might include an individual facing risk changing one's behaviour depending on whether one is insured. For example, a person may drive a hire car in a different manner to how they drive their own car, as somebody else is taking the risk -the hire car company and insurance company. If the reader considers that a warship may have a 30 year or even 50 year life the organisational imperative to incentivise the long-term strategic consequences of today's actions becomes clear. The ability to more accurately understand all aspects of risk and redundancy may encourage short term risk taking through the deferral of maintenance and the development of 'technical debt'. Whilst this would increase time on task in the short term and reduce costs (which may be very welcome), at some point somebody else would be responsible for paying the cost in time and resource which may not be the present operator. One of the highest profile incidents of 'moral hazard' may be the global financial crisis, 2008, where it has been argued that elements of the global finance industry made significant sums of money making high risk bets that were subsequently underwritten by unwitting worldwide governments and hence the public (Dowd 2008).

This also means there may be a deferral of when the negative points collide which would make it harder to train an algorithm. If the reader considers the wind turbine company which will be focussed on their financial balance sheet; a failed wind turbine may lose them £100k per day, and so on. The company would therefore be incentivised to spend £50k at the earliest point to fix the system as they would want to maximise reward long term. Accordingly, an algorithm would be written to identify when they needed to make interventions and they would make them in a timely manner.

However, if one is only looking at short term gain and somebody else is responsible for the payment in the future then the algorithm could become subtly different. It may therefore be difficult to train an algorithm to do reinforcement learning with conflicting goals.

10. *Challenges*

There are other challenges associated with a digitalisation proposal such as outlined within this paper, although these are primarily associated with difficulties in digitalising legacy information technology infrastructure. Firstly, unless the systems are inbuilt with monitoring sensors, then data entry friction poses a significant challenge. A lot of this will rely on onboard teams to input vast amounts of data which may then enable automated analysis. This may not be possible depending on the available personnel resource and the volume of the data required to be input using existing databases. Furthermore, whilst the quality of existing data may be cleaned up, it may also present an issue, if it is inaccurate or not complete. Finally, as alluded, the greatest challenge is to build a digital infrastructure over existing organisations and process, although this is faced across industry and not just militaries.

There is also the challenge of generating statistically meaningful sets of data to enable machine learning from the complex data generated by an integrated combat system. Using the analogy of identifying imbalance in a coin, if this is tossed then the chance of heads or tails is 50% if it is fair. The coin would need to be tossed hundreds of times to determine any imbalance. If, however, the coin is only tossed a few times then any imbalance would not be recognised as there would be no pattern. Now consider the complexity of an integrated Combat System which has a vast number of statistical relationships which would require a huge number of rows of data to infer probabilities. This makes many machine learning techniques unsuitable, as unless there are failures (and enough of them repeatably); the sort of techniques that work well on a wind turbine may not work as well on a warship. In technical terms the Navy's support data is characterised by being largely unlabelled, high-dimensionality with more noise than signal. Therefore, more sophisticated hybrid models are required to pre narrow the range of data using domain expertise combined with ML techniques.

11. *Goodhart's Law*

One of the other challenges is Goodhart's law which states; 'any observed statistical regularity will tend to collapse once pressure is placed upon it for control purposes.' (Manheim and Garrabrant 2019). This is a particular issue for measuring performance in defence in peacetime as all measures are proxy measures with the real reference measure rarely tested. Proxy measures are therefore vulnerable to gaming whether by humans or algorithms. This can be illustrated by an anecdote from the Soviet era when nail factories were instructed to increase the quantity of nails they manufactured, with the focus being on the number. It is alleged they switched to produce millions of very small, useless nails. The criteria for the weight was then changed to generate larger nails so the managers initiated the production of large, but equally useless nails (Coy 2021).

This effect has important implications for the metrics used to train and measure the effectiveness of decision support algorithms. Considerable care needs to be taken to ensure that the recommendations to improve hard-to-measure complex and sometimes conflicting outcomes like 'safety', 'availability' or 'capability' actually improve the overall outcome and not simply the metric.

12. Conclusion

There is presently a significant drive towards digitalisation as large organisations, including militaries, seek to capitalise on the benefits it enables. In a military context, this provides the potential to better monitor and analyse the availability of capability, safety, as well as deliver an enhanced understanding of cumulative risk and its mitigation. Harnessed correctly, this has the potential to deliver significant benefits to the user community.

Firstly, through the identification of specific areas to target it could enable the saving of financial and time resource, as well as signpost previously unidentified risk, reducing threats to the availability of capability and reducing the risk to a safe to operate position. It also would provide a single point of truth across the entire user community which may be used for coherent decision making.

When considering the military application versus the civilian application, as demonstrated by the digital twin of the wind turbine compared with the naval destroyer, there is a scale difference in complexity. What might be relatively simple to achieve for the civilian sector may be significantly more challenging in the military context. This means that a complex warship digital twin may be too difficult to develop. The complexity of the data may make it challenging to implement machine learning, and an 'expert' system may be more suitable, notwithstanding the complexities of programming a complex warship with the redundancies built in.

This paper has proposed a model for an 'expert' system which would enable the monitoring and forecasting of availability risk, safe to operate status and other uses. It would enable a far more accurate forecast based on data, although with different ways to use the resulting data, there would need to be consensus on the desired output of any algorithms designed, noting the arising of a possible moral hazard based which may mean short term and long-term goals conflict. Other associated challenges, including data entry friction and accuracy of the source data, also may need to be overcome. Despite the challenges, however, digital tools may be developed, with the methodology proposed within this paper, to provide an analysis of risk to availability of capability and also an assessment of risk in a safety context.

13. Recommendations

This paper makes the following two recommendations:

1. An 'expert' system is better suited to understanding holistic risk for complex warships due to the complex data and small statistical sample of data available which may pose challenges to other methods.

2. An agreed consensus should be gained amongst relevant users of digital risk tools as to the aims of the output and of the underpinning algorithms to prevent both unintended consequences and the emergence of moral hazard.

References

Anzil, F., 2022. *Goodhart's Law*. Economicpoint.com. Available from: https://economicpoint.com/goodharts-law [Accessed 22 June 22].

Armstrong, M., 2020. Cheat sheet: What is Digital Twin? IBM. Available from: https://www.ibm.com/blogs/internet-of-things/iot-cheat-sheet-digital-twin/ [Accessed 22 June 22].

Balafoutas, L., Kerschbamer, R., Sutter, M., 2017. *Second-Degree Moral Hazard in a Real-World Credence Goods Market*. The Economic Journal. Available from: https://www.economist.com/finance-and-economics/2017/03/02/second-degree-moral-hazard [Accesses 22 June 22].

Brummer, A., 1986. *Programme in turmoil after shuttle tragedy*. The Guardian. Available from: https://www.theguardian.com/century/1980-1989/Story/0,,108275,00.html [Accessed 22 Jun 22].

Coy, P., 2021. *Goodhart's Law Rules the Modern World. Here Are Nine Examples*. Bloomberg. Available from: https://www.bloomberg.com/news/articles/2021-03-26/goodhart-s-law-rules-the-modern-world-here-are-nine-examples [Accessed 22 June 22].

Cullen, W., 1990. *The Public Inquiry into the Piper Alpha Disaster*. Department of Energy. Available from: https://www.hse.gov.uk/offshore/piper-alpha-public-inquiry-volume1.pdf [Accessed 22 June 22].

Dowd, K., 2009. *Moral hazard and the financial crisis*. Nottingham University Business School. Available from: https://www.nottingham.ac.uk/business/who-we-are/centres-and-institutes/gcbfi/documents/cris-reports/cris-paper-2008-6.pdf [Accessed 23 Jun 22]

Grieves, M., Vickers, J. (2017). *Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In: Kahlen, J., Flumerfelt, S., Alves, A. (eds) Transdisciplinary Perspectives on Complex Systems*. Springer, Cham. https://doi.org/10.1007/978-3-319-38756-7_4 [Accessed 22 Jun 22].

Haddon-Cave, C., 2009. *The Nimrod Review*. Crown Copyright. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/229037/1025.pdf [Accessed 22 June 22].

Manheim, D. and Garrabrant, S., 2018. *Categorizing variants of Goodhart's Law*. *arXiv preprint arXiv:1803.04585*. Available from: https://arxiv.org/abs/1803.04585v3 [Accessed 22 June 22].

Mayer-Schönberger, V., & Cukier, K. 2013. *Big data: A revolution that will transform how we live, work, and think.* Houghton Mifflin Harcourt.

Manheim, D. and Garrabrant, S., 2018. *Categorizing variants of Goodhart's Law*. *arXiv preprint arXiv:1803.04585*. Available from: https://arxiv.org/abs/1803.04585v3 [Accessed 22 June 22].

Matteson, S., 2019. *Autonomous versus automated: What each means and why it matters*.TechRepublic. Available from: https://www.techrepublic.com/article/autonomous-versus-automated-what-each-means-and-why-it-matters/#:~:text=Autonomous%20and%20automated%3A%20Defined&text=The%20decisions%20made%20or%20actions,the%20environment%20around%20it%20changes [Accessed 22 June 2022].

Peterson, S., 2016. *Definition expert system*. Techtarget. Available from: https://www.techtarget.com/searchenterpriseai/definition/expert-system [Accessed 22 June 22]

President's Council of Advisors on Science and Technology, 2007. *Leadership Under Challenge: Information Technology R&D in a Competitive World.* United States Government. Available from: https://www.nsf.gov/geo/geo-data-policies/pcast-nit-final.pdf [Accessed 22 June 22].

Statistica Research Department., 2022. *Total data volume worldwide 2010-2025*. Statistica. Available from: https://www.statista.com/statistics/871513/worldwide-data-created/#:~:text=Over%20the%20next%20five%20years,to%20more%20than%20180%20zettabytes. [Accessed 22 June 2022].

United Kingdom Government, 2009. *How MODAF Supports the Defence Lines of Development*. Publishing Service. Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/951622/20090210_MODAFDLODAnalysis_V1_0_U-withdrawn.pdf [Accessed 22 June 22]

United Kingdom Government, 2018. *Defence Standard 21-059 Issue 3*. Ministry of Defence.

Wise, J., 2022. *How Much Data is Created Every Day in 2022*. Earthweb.com. Available from: https://earthweb.com/how-much-data-is-created-every-day/ [Accessed 22 June 2022].