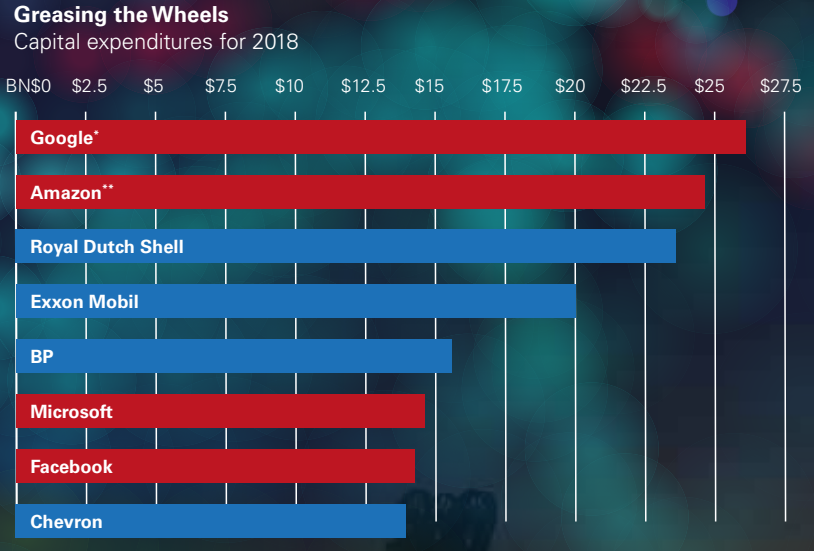
THE ROLE OF BIG DATA IN AUTOMATING PROCESS INDUSTRIES

Data is becoming increasingly vital in support of modern industrial processes. Gerard Ward, Cyber & Technology Loss Adjuster at Integra Technical Services, looks at how the oil of the new economy – 'big data' – is supporting the Oil & Gas and Petrochemical industries in optimising their operations and considers how insurance and risk management strategies need to evolve to remain relevant.

In March 2019, the Wall Street Journal published an article titled 'Data Really Is the New Oil' in the context of how the capital expenditure of tech companies was beginning to exceed that of traditionally capex intensive industries. As the diagram opposite shows, in 2018 the combined investment by the tech companies totalled USD77.7 billion, compared with USD71.5 billion spent by oil and gas majors Shell, Exxon Mobil, BP, and Chevron.

Among the biggest tech spenders was Amazon investing approximately USD22 billion in assets that include data centres supporting cloud delivered services, such as data warehousing and high-performance computation for algorithms that power Artificial Intelligence (AI). And let's not forget that the chart fails to really illuminate the extent to which the Oil & Gas and Petrochemical industries are themselves investing in big data in their drive for automation that can create new competitive advantages.



Ranking of capital expenditure (capex) by firm

IMPORTANCE OF DATA ANALYTICS

GE and Accenture published a research report in 2016 highlighting that 81% of Oil & Gas and Petrochemical executives considered big data analytics as one of their organisation's top three priorities. It's a point that was brought into focus again in April 2019 when the President of the oil services company, PUMPCO, observed that to boost efficiency the Oil & Gas and Petrochemical industries need unique technological differentiation which in the "new normal includes the adoption of big data as operators work with Google, Amazon and Microsoft to gain information about improvement of field operations, equipment, and well management."

Highlighting the journey of these sectors in using big data, in 2015 Shell reduced its cost of oil extraction by partnering with Hewlett-Packard and Amazon Web Services (AWS). Using HP fibre optic cables and storing the enhanced data sets acquired in AWS's cloud facilities, the resulting insights provided a more detailed vision of what lay below the ocean floor enabling geologists to more accurately determine where to drill.

MACHINE LEARNING

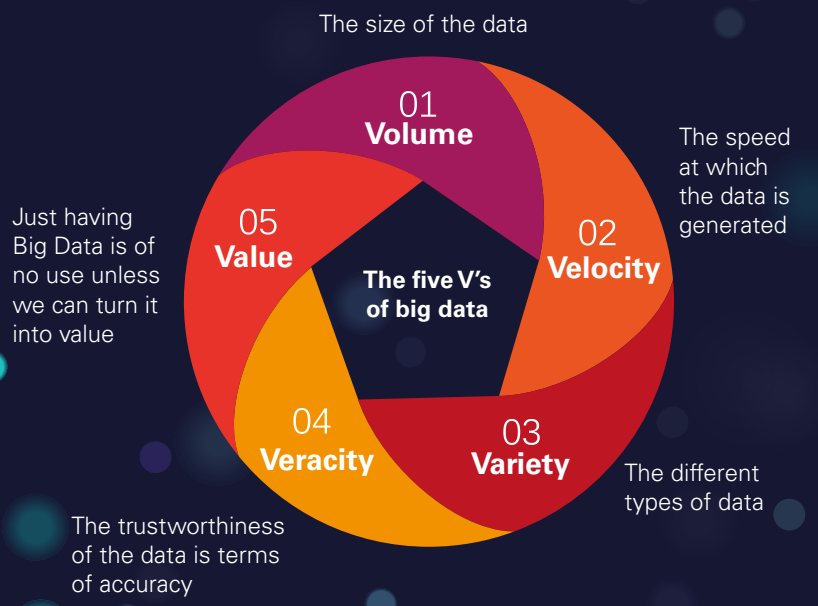
Big data is the foundation of industrial automation, and a critical first step in implementing AI. Providing a foundation for its data sets, the Oil & Gas and Petrochemical industries rely on Industrial Control Systems (ICS), Programmable Logic Controllers (PLC), and Supervisory Control and Data Acquisition systems (SCADA) to both control and report on the operating state of industrial assets.

In the world of big data the information captured by ICS and PLC and aggregated by SCADA has a much more expansive application. For example, Shell now uses machine learning to assist operator control of drilling equipment. Machine learning is a technique that utilises algorithmic classification of data sets so that patterns can be identified and used to inform automated decisions. It requires data in large enough quantities and of appropriate quality to train the algorithms.

The control data that was historically used for real-time monitoring now takes on new value. It's use in training machine learning forms a cornerstone of AI, so what was once temporal data is now an enduring asset for many organisations. Not just within the Oil & Gas and Petrochemical industries but across many different sectors, including for example retailers and airlines.

THE FIVE V'S OF BIG DATA

The Oil & Gas and Petrochemical industries have long incorporated control data into process flows, with much of the equipment deployed having sensors and actuators for regulating valves, for example flow meters, submersible pumps, and other downhole monitoring systems. While historically this control data supported monitoring and operator directed intervention to assist the big data attribute of 'velocity', this time continuous data is being combined with other organisational data such as risk, asset and project information, to derive near real-time actionable intelligence.



Introducing the AI controlled smarts is increasing implementation of Cyber Physical Systems (CPS). These are meshed networks comprising nodes of sensors and actuators coordinated by edge computing and cloud hosted big data to create a new paradigm in connectivity. Edge computing is a technical term referring to computation being completed as close to the device as possible. For example, in the Oil & Gas sector using well data AI can identify kicks in the well and then determine actions that avoid destructive blow-outs.

SCALE OF RISK

These developments are undoubtedly fuelling advancements and creating new advantages, but they require a complete refresh of risk modelling, rethinking the propensity for scale events.

The tragedy of the two Boeing 737 Max air crashes illustrate the consequences of bad sensor data informing an algorithm. The MCAS system (a CPS) was introduced by Boeing to eliminate the need to retrain pilots following the installation of larger engines that changed the aircraft's aerodynamics. The engines were designed to improve safety, but the implementation and use of AI resulted in greater complexity. This has led to the grounding of all Boeing 737 Max aircraft, with the delay in the manufacturer implementing a fix illustrating the risks of complexity overlaid on the limits of technology.

While the media is full of articles about enterprises adopting AI, and technical white papers talk to successful case studies, wringing productivity gains from big data and AI does involve a progressive layering of complexity.

As the Boeing 737 Max situation shows remediating CPS implementations is complex and can involve millions of sensors and actuators controlled by thousands of central processing units (CPUs). The ability of the crisis teams to comprehend the full extent of the problem may diminish proportionate to the systems complexity.

This may provide a perfect warning for risk managers of asset fleets in Oil & Gas and Petrochemical, and potentially other industries. The implementation and reliance on AI may support more consistent utilisation of assets compared to using human operators, but human error is usually contained whereas the deployment of an algorithm creates a greater potential for scale events.

RISK MANAGEMENT IMPLICATIONS

Just how can risk managers determine and model the potential outlier risks that exist in algorithms? Particularly as they are largely software problems the test cases may not envisage and the big data that informed the decisioning in the first instance may not have encountered the combination of events that give rise to the outliers.

In considering scale risk, if a single asset crashed or exploded following an algorithmic error, would the balance of that fleet be stood down while root cause investigation and remediation ensued? If the fleet was idled significant business interruption losses then flow from that decision, but would these be insured under a traditional Property Damage policy?

In circumstances such as faulty sensors that inform algorithmic decisioning, and for which historic data sets had not encountered that

combination of circumstances, liability on the part of the machine learning trainer or sensor manufacturer may not be clear. How will a smart building be impacted if the algorithm interprets warning data as a false negative and ignores it, will a Property Damage policy still be triggered if the building catches fire as a result?

What if that fire had originated from the malicious interference of a bad actor through tampering with those systems in that smart building, does the Property Damage policy still respond?

RAMIFICATIONS

These questions and others have been vexing insurance market practitioners and regulators alike. It's led to much debate about silent cyber risks and transparency about what is covered and what is not covered.

In January 2019 the UK regulator, the Prudential Regulation Authority, called on Lloyd's and the wider UK (Re)Insurance market to ensure more effective management of silent cyber exposures. They ordered firms to work towards developing an action plan in the first half of 2019, and to set out clear milestones and dates by which action would be taken.

Following this Lloyd's consulted with the market and announced that from 1 January 2020 Lloyd's Underwriters will be required to clarify whether first-party Property Damage Policies affirm or exclude Cyber Cover.

While the cyber debate aims to bring certainty to (Re) Insurers and Insureds, achieving that outcome may not be so easy. The increasingly pervasive nature of big data supported CPS in industries like Oil & Gas and Petrochemical means qualifying the data and AI cannot be done in broad cross-industry terms. It will likely need to be more targeted, challenging the use of industrial special risks wordings and positioning standalone Cyber Insurance as being best placed to approximate the needs of rapidly evolving technology and data dependent businesses.

Just as a reliance on data is both challenging and changing the Insurance industry, Loss Adjusting also needs to change. Adjusters cannot rely on their traditional Property and Liability claims experience to guide them in the investigation, mitigation, adjustment and settlement of Cyber and Data related insurance claims.

Without understanding the composition of information flows, data and its role in supporting modern business models it is difficult for Loss Adjusters to qualify and attribute loss or support recovery strategies.

MEET THE AUTHOR

Gerard Ward is a cyber insurance specialist with deep knowledge of the technology industry. He understands data driven business processes, the financial models that data informs, and applies that knowledge to cyber and technology related insurance claims.

Since joining the insurance industry, Gerard has adjusted cyber and technology claims on behalf of (Re)Insurers for SME's through large corporates. Prior to that, he managed Information Technology (IT) projects focused on process and data security across Australia and Asia for clients operating in banking, insurance, retail, transport, and aviation. Following the Christchurch earthquake series in 2011, he joined a New Zealand Loss Adjusting firm as a Financial Lines Adjuster to primarily manage technology related losses. His ability to drive claim outcomes draws on his experience as an IT project manager, supported by his having started his career as a management accountant.

Complementing Gerard's professional experience is specialist IT qualifications. He holds a Master's in Information Security & Digital Forensics, is a certified project manager and a certified information systems security professional. And he is advancing a PhD around risk in cyber physical systems and is the recipient of a doctoral scholarship from the University of Auckland Business School.