StrategicRISK

SPECIAL REPORT:

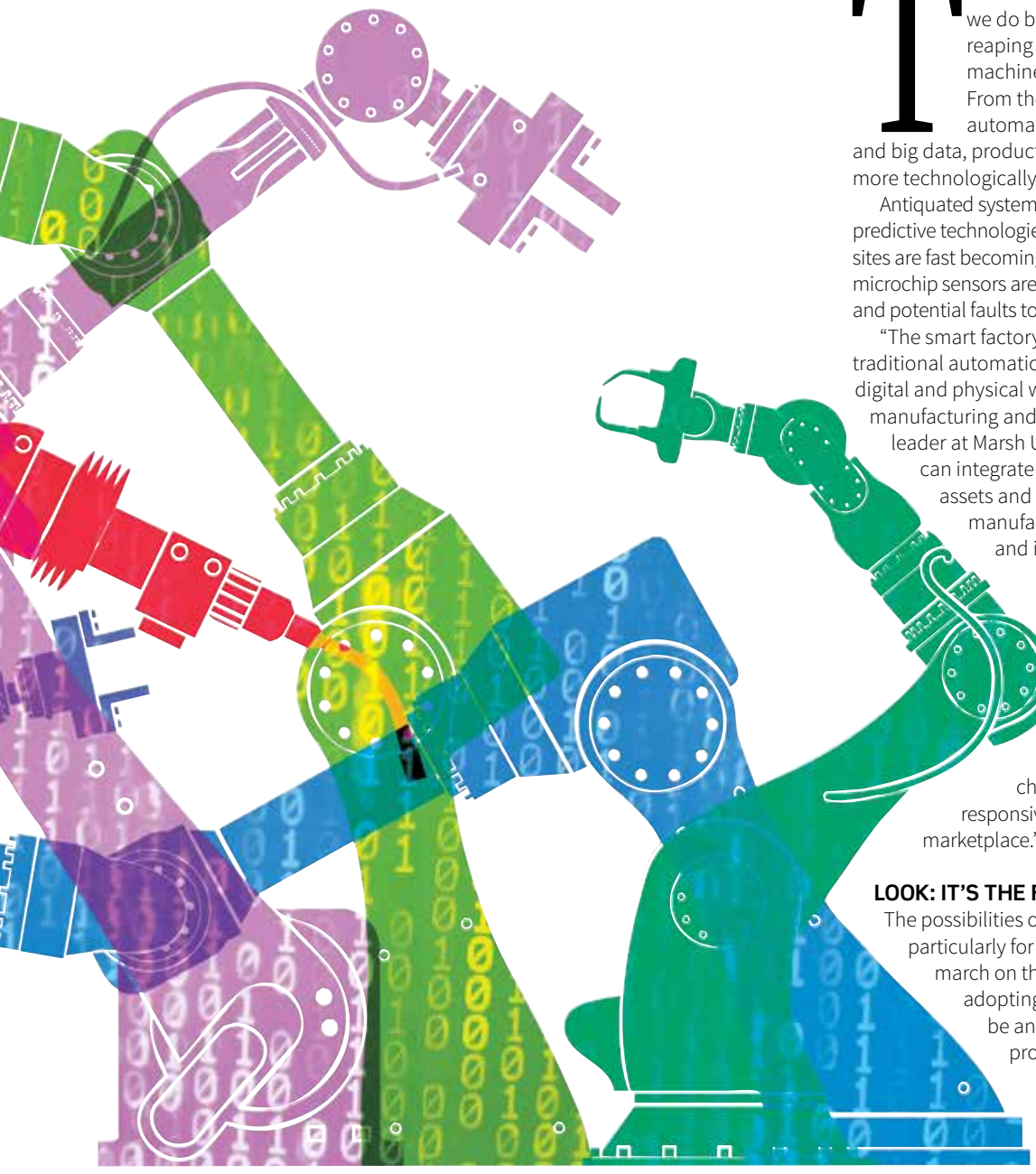
DIGITISED INDUSTRY

In partnership with:

FM Global

Heavy industry becomes agile

Production lines and power plants are now using digitalisation to predict and prevent issues before they happen, remove human error and limit costly shutdowns. Introducing: the smart factory.



Technology is revolutionising the way we do business, with heavy industries reaping the full benefits of digitalised machinery and production processes. From the internet of things (IoT) and automation, to artificial intelligence (AI) and big data, production lines and power plants are more technologically advanced.

Antiquated systems are being replaced with predictive technologies, manufacturing and production sites are fast becoming automated factories, and microchip sensors are beginning to predict maintenance and potential faults to machinery before they happen.

"The smart factory represents a jump forward from traditional automation to the convergence of the digital and physical worlds," says Anthony Monaghan, manufacturing and automotive industry practice leader at Marsh UK & Ireland. "A smart factory can integrate data from physical and human assets and operational processes to operate manufacturing processes, maintenance and inventory tracking."

Monaghan continues: "This increased connectivity can result in a more efficient and agile system, less production downtime, reduced human elements, and an ability to predict and adjust to changes in the manufacturing supply chain, which can lead to a more responsive operation in a competitive marketplace."

LOOK: IT'S THE FUTURE

The possibilities of such advances are endless, particularly for companies that want to steal a march on their competitors. The benefits of adopting technologies such as these can be anything from more streamlined processes to higher quality products and even better decision making. For instance, good data analytics can help an organisation predict customer

demand better, meaning there's less chance of too much stock when there's low demand or not enough when there's a surge.

Another core advantage is the ability to spot problems before they become a reality. Tiago Dias, EMEA cyber consultant at FM Global, gives the example of how one client is using new innovations to help predict and prevent faults on the factory floor. "We have a customer that is looking for increased automation, but also machine learning where the quality process is based on robots that are able to inspect the product along the production line and detect defects during that process," Dias says.

"This customer is looking at 80 control points for a single product, which means there is extreme complexity involved. The difference between using these technologies and having human intervention is the level of complexity that is involved and the ability to learn using a trial and error approach. The machines are able to be taught to evaluate for certain things that have been missed previously and ensure a continuous improvement in that process."

It's not just manufacturing that is reaping the rewards of digitalisation, either. The defence and security sector is using cyber solutions like intrusion detection systems and intrusion prevention systems to minimise the significant threats it regularly faces.

Meanwhile, organisations that rely heavily on boilers find themselves able to avoid outages that could otherwise shut down entire plants.

Dias continues: "We will definitely see more and more industrial control system devices connected. Failures in these devices can lead to an entire plant shut down, so we need to be able to anticipate issues. By using predictive analysis we can detect possible equipment failures in critical time. This is crucial."

WHEN TO GO ALL IN

Of course, some companies are faster than others when it comes to adopting new technological approaches. Indeed, many are still dipping their toes in the water, weighing up the pros and cons before they go fully native.

Hans Læssøe, principal consultant at AKTUS and former risk manager of The LEGO Group, says that the use of AI, robotics and predictive analytics is only going to grow. "I am certain more and more uses and methodologies and integration will materialize in the years to come. The more fragile or dependent on 100% uptime a process is, the greater the need for smart technologies, predictive analytics and so on."

"I foresee a higher degree of autonomy in this equipment, enabling it to detect upcoming issues before they become issues (that is, predictive analytics) and automated adjustment, optimisation, and call for maintenance."

Clearly, from a risk management perspective, being able to use predictive analysis or natural language processing to not only react quickly to interruption – but also to stop it before it happens – is a powerful new weapon in your armoury.

Danny Wong, founder and CEO of Goat Risk Solutions, says: "Big data and AI has helped to advance our understanding of how materials and combinations of materials behave, their resilience and attributes to make better quality products – this can be seen in continued improvements in batteries and reducing size of electronic devices."

As well as automation helping to reduce downtime, big data can also be a useful tool for risk managers who want to better understand their exposures and plan to mitigate against them.

Læssøe says: "Big data is just another source of facts, and predictive analytics was formerly in the risk management area known as Early Warning Indicators. These tools can improve the validity, thoroughness and timeliness of processes already established."

Wong adds: "Data and analytics can be used to model risk-adjusted outcomes, forecasts and decisions. When clients' data maturity is ready and the appetite is there, we will introduce artificial intelligence/machine learning and robotic process automation so that business decisions can benefit from the collective wisdom of internal and external data, success drivers, considerations and risks. It sounds complicated, but the technology already exists."

Of course, as with any new advancement, there are challenges alongside the opportunities, and risk managers will have to add these to the long list of factors that need their attention.

THE ROUGH WITH THE SMOOTH

One core risk is that of cyber interruption. As businesses connect more and more devices to each other, to headquarters and even to the internet, there is an increasing concern that attackers could gain access and cause real physical damage.

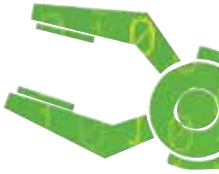
There are other new risks on the horizon. For instance, as more companies start to introduce technologies such as facial recognition or voice recognition (both of which have garnered attention for the airline industry recently), there are significant privacy concerns. And a connected world means that businesses need to be careful of GDPR legislation, too.

Dias explains: "Understanding data flows, understanding where data is being processed, understanding the interdependencies of systems and organisations processes and so on means it is very challenging to keep track of the huge changes that we see in a digital world."

SR

"FAILURES IN [BOILERS] CAN LEAD TO AN ENTIRE PLANT SHUT DOWN, SO WE NEED TO BE ABLE TO ANTICIPATE ISSUES. BY USING PREDICTIVE ANALYSIS WE CAN DETECT POSSIBLE EQUIPMENT FAILURES IN CRITICAL TIME."

EMEA cyber consultant, FM Global **Tiago Dias**



Rampage against the machine

Heavy industries may now be embracing the digital world. But physical, as well as reputational and financial, damage from a hack can be severe. This is where the risk manager must come in.

It's not just consumer data that is at risk from hackers, and when power plants, machinery, production lines and turbines come under fire, the consequences can be even more severe.

Unsurprisingly then, as more of the heavy industries embrace the digital world, connecting machines both to each other and to the head office, using the internet of things and AI and even letting robots run the production line – the concerns about cyber interruption are growing ever more serious.

"Increasing connectivity using automated control, and connected systems in the manufacturing process inevitably bring cyber risks to the fore," says Anthony Monaghan, manufacturing and automotive industry practice leader at Marsh UK & Ireland. "Unauthorised parties or hackers could capture data or alter records or interrupt the manufacturing process, creating a new dimension to business interruption."

It can be hard to picture the damage that can be done by cyber attacks levelled at the manufacturing industry. But beyond the breach in the first place, the physical damage can be extreme.

For instance, Tiago Dias, EMEA cyber consultant at FM Global, explains how a cyber attack on a turbine could have severe consequences. "The main concern is the physical resulting damage of a cyber attack. For example, a cyber attacker could increase the operating speed of a piece of machinery, such as a turbine, and as a result trigger a fire due to overheating oil."

Other possible risks include business interruption, supply chain disruption, systems failures and factory failures. Danny Wong, CEO and founder of Goat Risk Solutions, says: "Cyber attacks in heavy machinery sectors can take many forms and have serious implications for the confidentiality, integrity and availability of systems and data, impacting operations, customers, employees, shareholders, suppliers and more, and result in significant regulatory fines, lost revenues, extra costs, and reputation damage."

BUT WHY YOU?

There are plenty of reasons that hackers might want to target a manufacturing plant, defence company or other machinery-related business. Both the defence and the airline industries are obvious targets for security reasons. Equally, manufacturers are ripe for IP or corporate espionage-based hacking. But there are less obvious triggers as well. For instance, sometimes criminals will target a company not because of what it is making, but because of its processing power.

Dias says: "The reason can be simply access to systems or the ability to use their processing power for operations that an attacker wants to process. For example, using those systems for mining crypto currencies. So the motivation is the monetisation of that processing power and may not be related to what is being manufactured by that organisation. It can be just the ability to manage more systems."

Any industry that relies heavily on machinery is also at significant risk from ransomware attacks. This software allows criminals to block

EXPERT VIEW: SMARTER THE DATA, BETTER THE BUY-IN

The smart tech now being used in heavy industry brings risks as well as rewards. But these risks actually give the risk manager what they need – more data on what can go wrong and quantitative information to take to the C-suite, says FM Global's Philip Johnson.

Industry and commerce are in the midst of profound transformation perpetuated by super smart technologies that are wirelessly connecting one piece of equipment to another; and where complex procedures are being automated through the use of AI and the IoT.

Businesses that operate and rely on heavy and critical machinery are beginning to reap the commercial and operational benefits. Control systems are being optimised by remote control, enabling temperature and speed adjustments to be made more quickly; and real-time data to be accessed at any time, from anywhere in the world.

Of course, as businesses rely more on these smart technologies, they grow more vulnerable to cyber risks. It is easy to imagine a scenario where a criminal gains access to and takes control of critical systems – increasing the temperature in a power plant or the speed of a wind turbine – which can lead to loss in revenue, market share and shareholder value, as well as the damage to physical property.

But AI, IoT, sensors and automation are also boosting risk management capabilities. As this tech gains momentum, it is generating critical data points – information that can used to make more incisive risk management decisions. In fact, insurers are using big data and predictive analytics to build new risk management tools. This is precisely what we have done – created a new suite of predictive analytics capable of identifying locations that are predisposed to loss, relative likelihood and environmental factors.

There is, of course, a big difference between data and good data: we conduct approximately 100,000 location visits every year and this has resulted in more than 7 million individual data points. This means that we can provide more accurate loss scenario predictions. For instance, our predictive analytics tool has told us that of the top 1,000 locations likely to suffer a loss, 43% of these locations did suffer a loss. This rate is 15 times more frequent than the median location on the list.

In a volatile economic environment, where it is tough to obtain budgetary sign-off for losses that have yet to occur, critical information such as this provides risk managers with compelling data to present to the C-suite on where time, money and resources should be prioritised. It helps risk managers convey the potential loss scenario and the associated financial implications.

We pride ourselves on helping risk managers make more accurate decisions, using data and tech to develop tools. For example, we've worked with our clients to build a total financial loss model. This helps risk managers take a quantitative approach to prevention.

We take a proactive approach to helping our clients prevent, manage and mitigate risks because we believe resilience is a choice.

Philip Johnson is senior vice-president, EMEA division manager, at FM Global.

"UNAUTHORISED PARTIES OR HACKERS COULD CAPTURE DATA OR ALTER RECORDS OR INTERRUPT THE MANUFACTURING PROCESS, CREATING A NEW DIMENSION TO BUSINESS INTERRUPTION."

Manufacturing and automotive industry practice leader, Marsh UK & Ireland
Anthony Monaghan

access to a system until a sum of money is paid. It can be levelled against individuals, but organisations such as the NHS have been targeted, too. FM Global says 41% of cyber losses this year have been ransomware based.

Even though machine or boiler-reliant industries are rising rapidly up the hackers' agendas, these sectors are somewhat behind the curve when it comes to protecting themselves.

Generally speaking, the operations technology world has lagged behind the information technology world on the identification and mitigation of cyber threats. This is unsurprising, but definitely a cause for concern. This means risk managers need to make sure cyber risk is firmly on the corporate agenda. Risk professionals need to understand the board's appetite for risk and translate this into tangible actions that can minimise exposures.

Dias suggests that risk managers should take these pre-determined steps to managing potential cyber exposures. "For risk managers, any significant change to the operating model, such as a merger or acquisition, should serve as a red flag for a potential increase in cyber exposure. An immediate reassessment of this risk, across all operations, business units and equipment, should be a priority, with appropriate resilience building steps taken where required. Insurers should be notified as soon as possible so that existing policies can be adapted to the changed model, ensuring continuity of coverage and protection for the business."

TREAT LIKE ANY OTHER RISK

Of course, risk managers must also identify and contextualise the risk in a way that the board can understand, as well as educating leadership about how digital opportunities can be taken in a way that also keeps risks under control. Usually, this means working with other departments, particularly IT and security.

Hans Læssøe, founder of AKTUS, says: "The more dependent the industry/company is on 100% uptime of equipment, the more vulnerable they are to any cyber issue – be it an attack or accident. Process-wise, risk managers can do to these risks exactly what they do to all other risks. Ensure the relevant people address the issues and take appropriate steps to ensure risk taking does not exceed risk tolerance. The actual management of the risks lie in the hands of the business." **SR**

BE EXPOSED TO RISK **OR** ENGINEER IT OUT?

With specialised Boiler and Machinery services, our loss-prevention engineers evaluate the integrity and reliability of your equipment, identifying hazards and deficiencies to help prevent breakdowns. **Choose to be resilient today. Visit fmglobal.co.uk/boilerandmachinery**

RESILIENCE IS A CHOICE.

Proud partner of

FERMA
EUROPEAN RISK MANAGEMENT
FORUM 2019

FM Global®
Commercial
Property
Insurance