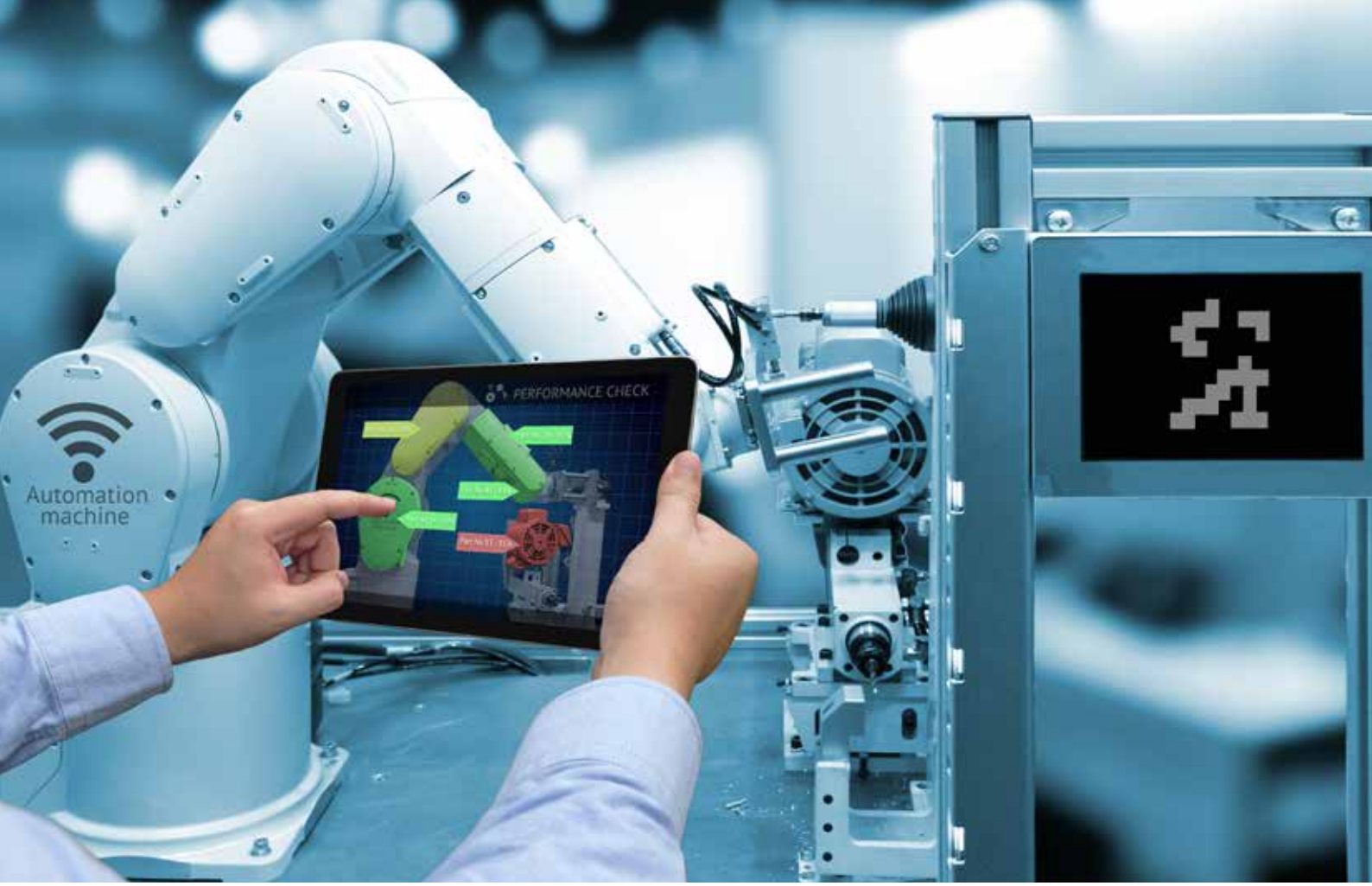

Industry 4.0 | Revolution in manufacturing and production

The Smart Factory: Increased vulnerability to cyber-attacks?

The Smart Factory allows production to take advantage of a fully integrated value chain enabling an increase in overall efficiency. Based on the Internet of Things, this revolution comes with increased risk for producers and customers. The increased risk exposure primarily needs to be mitigated by defining and strictly following appropriate internal IT security standards. Manageable residual risk may then be covered by innovative insurance products.

Digitisation has become a global process affecting the lives of consumers and producers in societies across the entire globe. A major positive effect of digitisation is the huge up-side potential in resource efficiency across processes in any given industry. Once digitised processes that, until today, had required a specific quantity of resources (e.g. time, financial or physical resources) can now achieve the same results at far lower overall costs than before. As a consequence, Industry 4.0 with digitisation as it's core will create enormous new value potential especially for industrial companies and not least the global economy in total.

A key element of Industry 4.0 is the concept of the "Smart Factory" which merges the physical and virtual worlds in production by applying artificial intelligence, machine learning, augmented reality, automation and machine-to-machine communication. The Smart Factory will fundamentally change the way products are invented, manufactured and shipped.

In it's most sophisticated version and based on the Internet of Things (IoT) the Smart Factory will emerge as a totally interconnected production facility with robots, machinery, supply chains and even inventory and produced goods communicating with one another for controlling and delivering the targeted output in the most efficient way. Supply chain management will be raised to another level with machines self-reliantly reporting the need

for new materials or for logistics involvement to deliver any necessary part or material for production as well as the ability to report critical wear and tear limits through predictive sensor-based maintenance thereby limiting the possibility of unplanned downtime of the assembly line. Intelligent and communicating production devices will further reduce inventory, spoilage and expiration of products in stock based on just-in-time delivery and increase stock efficiency. Smart Factories will be connected to one another scaling efficiency across their entire value chains on regional and global levels.

With all the benefits of interconnectivity in Smart Factories, however, comes their vulnerability to factors such as technical failure, operating errors and, with increasing importance, external incidents like cyber attacks. In the US alone, reported cyber attacks on industrial control systems have increased by 20% to 295 incidents in 20161. Again, these are reported figures only. As enterprises often tend to not report cyber attacks for reputational or strategic reasons, overall incidents are believed to be higher. The more devices in production facilities are connected to the internet for communication purposes, the more potential gateways are created for possible cyber attacks. Data theft such as customer information, intellectual property including design blue-prints and performance data (such as on the efficiency and profitability of different stages in the value chain) may be at risk. According to former FBI Director Robert Mueller „There are only two types of companies: those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again“.

Just as with any new technology benefits, it’s application are accompanied by risks and uncertainties. The price for efficiency gains of Industry 4.0 is the risk exposure that comes from the production facilities being connected to the internet. While risk exposure cannot be eliminated when trying to leverage the opportunities of Industry 4.0, a comprehensive cyber risk governance for the organisation may serve to successfully limit exposure to cyber risk and mitigate critical incidents to the production facility. Specific measures for increasing IT security need to be taken in companies and production facilities of any size. Companies need to identify their intangible assets to be protected and determine areas that could be open to attack. IT security standards need to be implemented and observed at every level of the workforce, in management and in production. This includes access to internal networks, regular programme updates and strict rules for the use of mobile devices and continuous IT security training for the workforce. As with any previous industrial innovation, the insurance industry will support innovative manufacturers in moving towards the Smart Factory with advice on risk mitigation and, if necessary, cover any residual risk through sophisticated cyber insurance products.

ERGO