RISK CONSULTING

IF'S RISK MANAGEMENT JOURNAL 1/2018

Paralyzed by flooding

Preventing e-mail spoofing

3D printing and risks

Protecting investments in emerging markets

Managing Risks Together 2.0

I'M WELL AWARE that I have talked about the theme several times before in this journal. Nevertheless, I'm going to do it again. This time in 2.0-version. Managing risks is core to our business, and even more important: Together with you.

Customer expectations are rising in every aspect, and the impact to us is indisputable. With this in mind, we recently launched several initiatives to further strengthen our services towards clients worldwide.

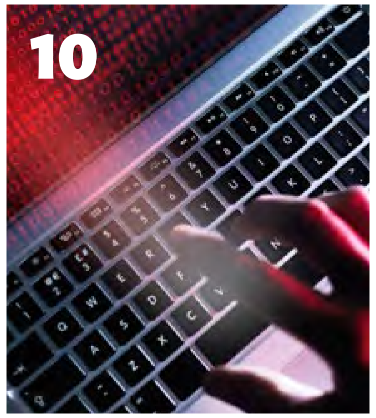
We are known in the market as the insurer who goes into partnership with our clients, to find the best solutions together. This is about the insurance solutions we provide, how we service you, how we match your needs, and how we continuously have a dialogue with you on how risks are changing. That's why we now have 'Managing risks together 2.0' as the focus of our new direction.

New technology and production methods affect which risks we insure in the future. For example, when car parts can be 3D printed within weeks, there is no need for long hauls from factories in Central Europe or Asia. This has impact on our insurance covers. We do not know how fast this development will happen and how complex the changes in different industries will be, but we will use our eyes and ears to follow the market.

We will cover the risks of the future and make things easier for you by providing seamless, digital and global services.

And maybe most important, you will notice by getting even better service.

POUL STEFFENSEN
Head of BA Industrial, If



If P&C Insurance, contact information

Finland +358 10 19 15 15 **Sweden** +46 771 43 00 00 **Norway** +47 98 00 24 00 **Denmark** +45 7012 24 24 **France and Luxembourg** +33 1 42 86 00 64 **Germany** +49 6102 710 70 **The Netherlands and Belgium** +31 10 201 00 50 **Great Britain** +44 20 7984 7600 **Estonia** +372 6 671 100 **Latvia** +371 7 094 777 **Lithuania** +370 5 210 9800
www.if-insurance.com

Publisher If, Niittyportti 4, Espoo, FI-00025 IF, Finland, +358 10 19 15 15, www.if-insurance.com **Editor-in-chief** Sigmund Clementz **Sub-editor** Carita Hämäläinen-Tallgren **Editorial board** Fredrik Holmqvist, Reija Laatikainen, Anders Rørvik-Ellingbø, Pekka Sarpila, Johan Wong, Marianne Wiinblad **Production** A-lehdet Oy **Printing** Forssa Print **Changes of address** industrial.client-service@if.fi **ISSN** 1459-3920. **Cover photo:** Getty Images

GETTY IMAGES

A CalFire helicopter makes a water drop on still smoldering remnants of Blue Cut Fire on the hilltop ridges along Hwy 2 in Wrightwood.

Spent $1.8 billion fighting wildfires

CALIFORNIA STATE AGENCIES spent nearly $1.8 billion fighting the fierce wildfires that killed dozens of people and destroyed thousands of homes and businesses last year, according to Insurance Journal. "The 2017 wildfire season in California was nothing short of catastrophic," said Mark Ghilarducci, director of the Governor's Office of Emergency Services. A series of fires killed 44 people and destroyed 8,800 buildings, prompting $10 billion in insurance claims. In December the largest blaze in state history swept through Ventura and Santa Barbara counties. California fire chiefs said drought and climate change will cause longer, more severe fire seasons. The chiefs are asking lawmakers for firefighters positioned in advance of the wildfire season in areas experiencing dangerous weather. New technology such as satellite tracking to monitor fire engines could also be part of a more effective solution for combating the wildfires. ■

Loss estimate for cyclone Zeus

PERILS, the independent Zurich-based organisation providing industry-wide catastrophe insurance data, has disclosed its fourth and final loss estimate for Extratropical Cyclone Zeus, which affected France on 6 and 7 March 2017. The revised estimate of the property insurance market loss is EUR 272 million. This compares to the third loss estimate of EUR 284 million which was issued by PERILS on 6 September 2017, six months after the event. PERILS' loss estimates are based on actual loss data collected from insurance companies.

Exploiting chips

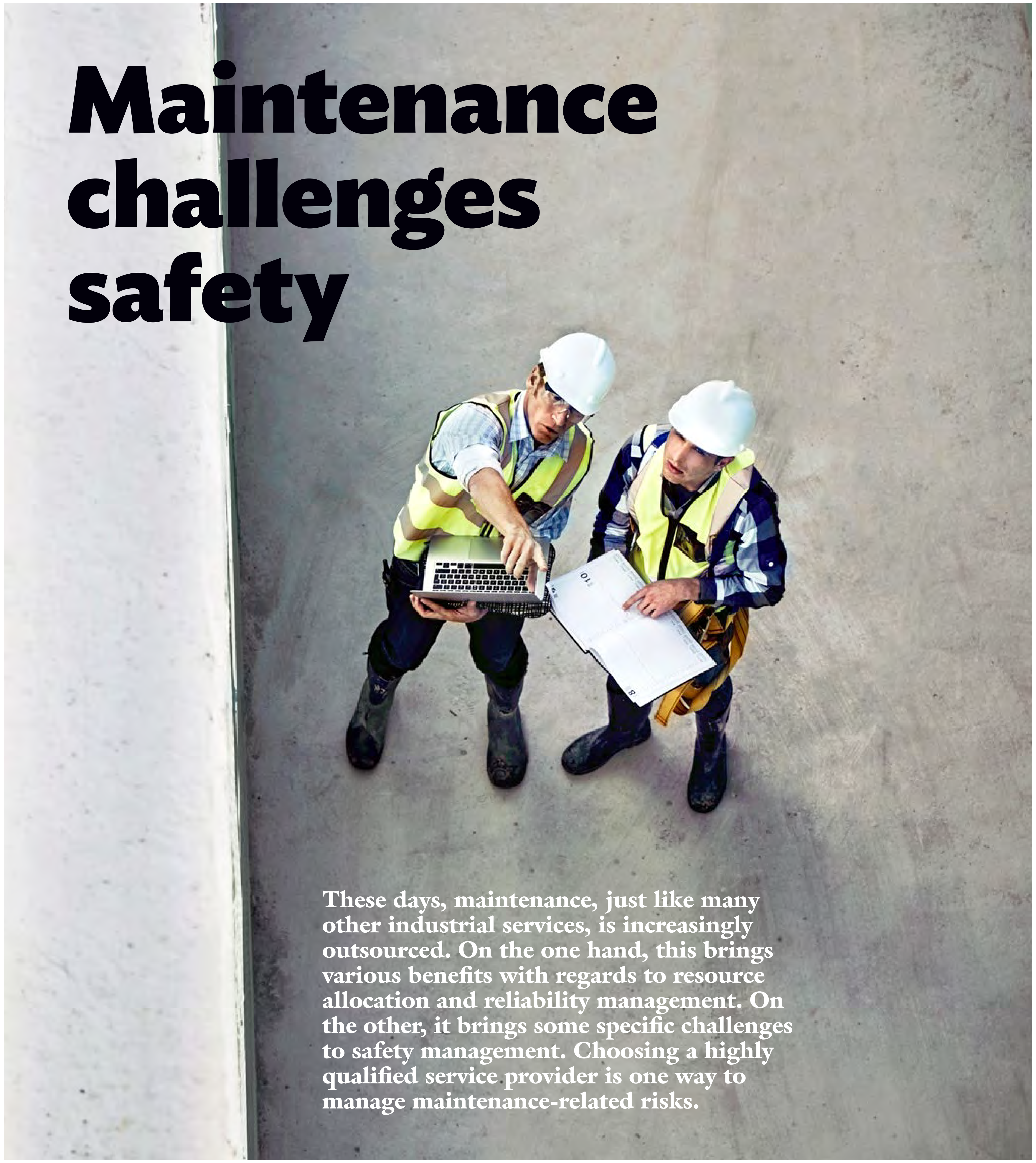
Security and risk management leaders must take a pragmatic and risk-based approach to the ongoing threats posed by an entirely new class of vulnerabilities, according to Gartner, Inc. "Spectre" and "Meltdown" are the code names given to different strains of a new class of attacks that target an underlying exploitable design implementation inside the majority of computer chips manufactured over the last 20 years.

Security researchers revealed three major variants of attacks earlier this year. The first two are referred to as Spectre, the third as Meltdown, and all three variants involve speculative execution of code to read what should have been protected memory and the use of subsequent side-channel-based attacks to infer the memory contents.

Not keeping up with cyber threats

In a global survey by Marsh and Microsoft of more than 1,300 senior executives, two-thirds ranked cybersecurity among their organizations' top five risk management priorities. The survey also found that a vast majority – 75 percent – identified business interruption as the cyber loss scenario with the greatest potential to impact their organization. This compares to 55 percent who cited breach of customer information, which has historically been the focus for organizations.

Despite this growing awareness and rising concern, only 19 percent of respondents said they are highly confident in their organization's ability to mitigate and respond to a cyber event. Moreover, only 30 percent said they have developed a plan to respond to cyber-attacks.



Maintenance challenges safety

These days, maintenance, just like many other industrial services, is increasingly outsourced. On the one hand, this brings various benefits with regards to resource allocation and reliability management. On the other, it brings some specific challenges to safety management. Choosing a highly qualified service provider is one way to manage maintenance-related risks.

As maintenance and service operations are carried out by experts who possess detailed knowledge of processes and their functions, client companies can allocate their own resources to core operations. Maintenance has several features that increase the level of difficulty when it comes to safety management. For example, property damage or business interruption resulting from errors during maintenance can be a major cost in any industry. It is also known that maintenance tasks involve various safety risks. Such challenges, and ways to tackle them, are also known by Maintpartner, a Finnish company that operates in the Baltic Sea region.

Maintpartner provides maintenance and service to various industries. In Finland, the company employs approximately 1,000 people and is constantly growing. “We want to take good care of our employees,” says Saija Pottala, who is responsible for HSEQ at Maintpartner. Due to the specific aspects of maintenance, occupational safety on client sites can sometimes be particularly challenging.

Countless ways of failing – the issue of reliability

Generally, maintenance operations are risky, both in the probability and severity of the potential consequences. This applies to both post-maintenance system reliability and to occupational safety during actual maintenance work, which are the two different aspects of safety that relate to maintenance. Reliability is typically affected by the “human contribution” which, in this context, refers to various kinds of errors and mistakes that may happen during maintenance, sometimes resulting in minor incidents or even major disasters after the work has been completed and the technical system is up and running again.

This issue has been widely touched upon by various accident investigators, reliability engineers and scientific researchers in their efforts to understand and prevent maintenance-induced weaknesses in technical systems. An excellent demonstration has been provided by James Reason with his “nuts and bolts” example (see, for example, Reason & Hobbs, 2003). In this example, he illustrates with a simple system how disassembly is practically error-free. The tricky part is in re-assembly, where there is only one way to re-assemble a system correctly, i.e. exactly as it was before it was disassembled. Conversely, there are multiple ways of doing it incorrectly. This, along with a number of major disasters with a background in unsuccessful maintenance, have sometimes been used as an example that demonstrates the human contribution to accidents and incidents, also reflecting on post-maintenance system reliability.

“Technical systems are only seldom, if ever, designed for maintenance and repairs.”

SAIJA POTTALA, MAINTPARTNER

Although maintenance may pose a risk to system reliability, it is still essential to keep technical systems up and running safely and reliably. Another, sometimes forgotten, issue is safety risks that may appear at any phase of a maintenance operation. “Technical systems are only seldom, if ever, designed for maintenance and repairs,” says Saija Pottala. “This is one of the major issues that impacts maintenance safety”. A maintenance operation typically involves multiple phases, in which repairing or replacing a part and/or re-adjustment is only one phase. The operation usually also involves system disassembly and re-assembly, preceded by the preparatory work phases and followed by cleaning up the site. Thus, there can be a wide variety of separate tasks and work phases involved in a maintenance operation.

Accident statistics and reports indicate that the causes of injury in maintenance vary greatly. For example, an injury can be caused by energies and substances within the system being maintained. Accidents can also be caused by the surrounding operating environment, i.e. structures and activities that do not relate directly to the maintenance task in question. Lower limb injuries are typical consequences of maintenance-related accidents, for example when something falls down during disassembly. Other typical problems are musculoskeletal injuries relating to poor ergonomics. This often relates to poor system maintainability, basically referring to the features that can make a technical system easy or difficult to maintain.

From the perspective of occupational safety, the number of tasks is one feature that makes maintenance work particularly challenging. Another factor relates to time: downtime for an industrial system is costly. Thus, preventive maintenance, not to mention corrective, unplanned repairs, must be performed efficiently. This may result in time pressure, which could increase the number and severity of risks if the work has to carried out in exceptional conditions and/or with limited information about the fault and its exact location. Saija Pottala confirms: "Defective maintainability causes safety and ergonomics to deteriorate in task execution. In preventive maintenance, the planning of safety and ergonomics can be easier to carry out, compared to repairs. As far as repairs are concerned, time pressure is particularly high". It may also be presumed that the cognitive load is high when a task includes troubleshooting under time pressure. Good maintainability can make work easier, safer and faster, while improving post-maintenance reliability. Respectively, allocating enough time and choosing a high-quality service provider is one way to manage maintenance-related reliability and safety risks.

The safety challenges of maintenance business...

As with all outsourced services, Maintpartner's employees also face various kinds of risks depending on their customer sites. The risks may relate to the operating environment and conditions and/or the actual tasks being performed.

On a task level, disassembly is particularly regarded as risky because, for example, the cause of a possible malfunction may be unknown, the failure mode may be misinterpreted and/or the energies and substances may be extremely dangerous if not securely separated from the system. Moreover, disassembly and reassembly double the number of task phases, along with the related risks. Between them, there is the actual task, e.g. replacing a part or removing a jam from a process. The tasks are sometimes completed through troubleshooting and by basically always restoring the process and cleaning the site. From the perspective of an individual employee, everyday tasks should involve inherently hazard identification and relevant, practical measures to manage risks.

Company safety management personnel must be aware of the amount and type of risks, which vary greatly between different clients and different tasks. Maintenance-related safety issues should be considered from at least three different viewpoints: 1) the task changes but the operating environment remains the same (e.g. outsourced factory maintenance with established customers sites), 2) the operating environment changes but the task remains the same (e.g. after-sales service), and 3) both vary (e.g. evening out temporary workload peaks between customer sites). While doing the actual work, each individual employee have the best possibility to impact their own safety.

> "Close cooperation between service provider and client is an effective way of promoting maintenance safety."

...and some ways of tackling them

Maintpartner's efforts in safety and health management have paid off: its accident statistics have improved remarkably in recent years. This positive progress is reflected in both the number and the severity of accidents, as the number of sick-leave days per accident has decreased. Yet, there are no quick wins: "Our commitment to safety has been systematic and long term. Each employee needs to be aware of the safety processes and commit to safety in their everyday work," says Saija Pottala. "A good safety record requires cooperation. Looking after yourself and others".

Close cooperation between service provider and client is an effective way of promoting maintenance safety. This cooperation must also include fluent information flow so that both the client and service provider are aware of the current safety-related topics. Such topics could be, for example, changes in site operations and/or procedures. In addition, the client is aware of the facilities and operations on site and has most probably conducted risk assessments and implemented safety management measures to reduce risks. This information is also of key importance to maintenance, although several risks may relate to actual maintenance operations, requiring detailed safety planning each time before an operation is started.

"When starting with a new client, we review all processes and practices together with them. We also agree on joint procedures," says Pottala, clarifying Maintpartner's practices. "In addition, we perform a safety review and assess the site-specific risks". Good knowledge and experience regarding the maintained system can help to reduce risks significantly. From this perspective, good cooperation with the operators is of focal importance.

What next?

Irrespective the ways of development in technology and industry, it is likely that maintenance will always be necessary at some points during the life cycle of a technical system. Maintenance may also be the kind of task that cannot be fully automated and requires a human contribution in one way or another.

The current and future development in industry may still influence maintenance work, for example, 3D printing or the Internet of Things. More complex and interdependent systems may also reflect on the execution of maintenance task, not to mention client expectations regarding quick and smooth system recovery and disturbance-free operation. Irrespective of the ways in which production systems are operated, there will probably always be maintenance workers with their hands on the systems, literally.

From Maintpartner's perspective, the current safety challenges are still quite practical, relating, for example, to client communication: "Client expectations regarding safety are constantly increasing. However, there are several ways of calculating and interpreting the safety figures. They may be calculated differently, although the concepts are apparently similar," says Saija Pottala. Meanwhile, technological advancements are positively expected. "Novel technologies may help to analyse information from a technical system. This can also help to plan safety more easily and effectively".

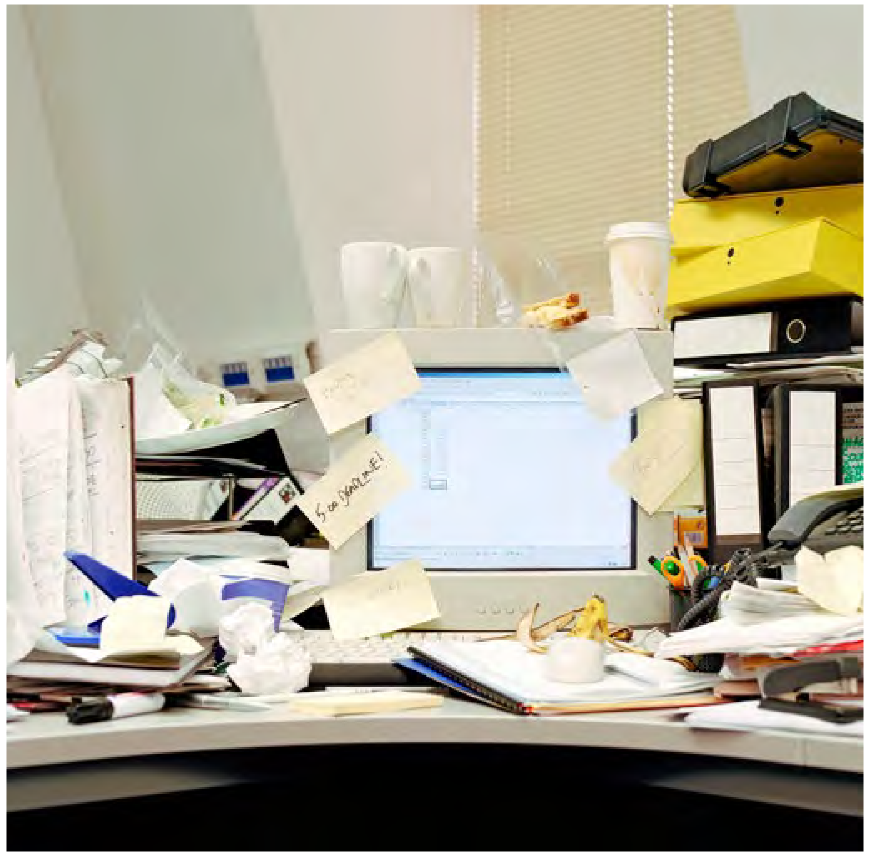
SALLA LIND-KOHVAKKA
salla.lind-kohvakka@if.fi

Further reading:

- Reason, J. & Hobbs, A. 2003. Managing Maintenance Error - A Practical Guide. Ashgate Publishing Company, Burlington.
- Lind, S. 2009. Accident sources in industrial maintenance operations. Proposals for identification, modelling and management of accident risks. Edita Prima Oy, Helsinki.

LEAN SAFETY – a concept to improve company safety culture

When Lean and Safety are combined, it will result in easier and safer working conditions.



It will also result in fewer mistakes and fewer corrective measures. Do it right the first time.

After reading the book "Lean Safety" by Bob Hafey it is more than ever clear that Lean and Safety work very well together and actually one cannot succeed without the other.

Please realise that there are other benefits to a lean programme than just saving lives, time or money, such as: quality, ergonomics, reduced search time, morale, customer satisfaction, employee satisfaction/retention, pleasant and organised workplace, etc. A well-organised workplace results in a safer, more efficient and more productive operation. It boosts employees' morale, promoting a sense of pride in their work and ownership of their responsibilities.

Lean management is a manufacturing philosophy that reduces the total cycle time by eliminating waste (it can also comprise non-value adding steps) or, in other words, by increasing efficiency. It is based on KaiZen (continuous or never-ending improvement) by means of improving the operating culture within a company.

IT IS PAINFUL to conclude that we have arrived at a point in time where we need to consciously consider management tools to help us behave in a respectful manner. But day-to-day practice shows that more complex business processes and shareholder value focus have driven us away from normal common-sense values or, in other words, common sense is not that common any more.

The top-down approach will no longer have the desired effect of rectifying this lack of safe behaviour. We are convinced that shop floor employees need to be engaged to get from compliance-based systems to proactive loss-prevention systems. Focus on safety is about respect for people. Safety is important and each of us has a responsibility for our own safety and the safety of others.

The use of a Job Safety Analysis (JSA) is a good way of performing the lean approach. It helps to identify the existing or potential hazards of a job, which can then be analysed and recorded.

A JSA, or better still, a written work procedure based on it, can form the basis of regular contact between supervisors and employees. It can serve as a teaching aid for initial job training and as a briefing guide for infrequent tasks. It may be used as a standard for health and safety inspections or observations. In particular, a JSA will assist in completing comprehensive accident investigations.

Four basic stages in conducting a JSA are:

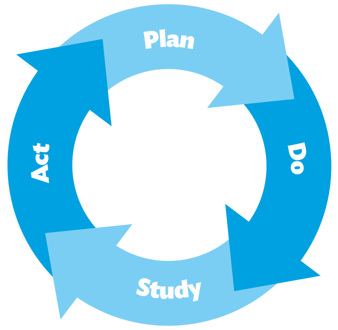
- selecting the job to be analysed
- breaking the job down into a sequence of steps
- identifying potential hazards
- determining preventive measures to overcome these hazards

More details can be found at www.ccohs.ca/oshanswers/hsprograms/job-haz.html.

A CHANGE IN mindset from Safety Compliance towards Safety Improvement is what is needed and a cultural shift from a top-down management structure to a team-based structure can facilitate this change.

Although the top-down approach will no longer work, it is executive management that must assume the role of facilitator. For effective decision making, there needs to be a flow down of Responsibility, Authority and Accountability (RAA) to the teams from the lean programme management. Organisational space has to be created to allow employees to continuously think about ways of improving their part of the process. This breaking down per sub-process or departmental approach is known as Kobestu KaiZen or Blitz KaiZen. In general, the entire focus of KaiZen is on perfecting business operations and includes the following steps:

1. Involve the people who implement the value stream or work process being improved. This allows the people closest to the problem to make an impact.
2. Focus on making improvements by detecting and eliminating waste, hazards and unsafe conditions.
3. Use a problem-solving approach that observes how the work process operates, uncovers waste. Generate ideas on how to eliminate waste, increase safety and make other improvements.



PROCESS MAPPING OR value stream mapping is used to graphically display the steps in a process. This visual method of process evaluation and improvement involves everyone. When implemented effectively it can eliminate the need for conversation to make information and ideas accessible to everyone. Activities can be merged in a standardised fashion on one A3 sheet. The following items can be combined on the front and back of an A3 form:

- Work process map
- Problem identification and solving
- Goal setting and auditing, Plan-Do-Check-Act (seven steps: define problem, analyse problem, identify cause, plan solution, implement solution, confirm results, standardise)

Both a current state and a future or desired state map should be completed during lean events. This standardisation in an A3 form helps you to be concise and to-the-point and it reduces preparation time.

Learning from losses and accidents is a very important part of any improvement process. Lean thinking can turn every incident into a safety improvement. Learning from losses should never be a blame game, but a process review and an improvement initiative. Facilitators should have the right questions, not the right answers. Focus on the process as the problem, not on the operator. Operators do not come to work to do a bad job or get injured, but they often have to work with poor processes, which yield poor results. Try to identify the root cause of the problem. Use tools such as "the 5 Whys".

Another strong element of the lean approach is Good Housekeeping. Here there is a choice between two methods:

1. Tuttava® as developed by the Finnish Institute of Occupational Health.
2. The more disseminated and popular 5S (five S), an effective system of risk control in the workplace.

Tuttava® is easy to apply to virtually every workplace or situation and If engineers have been familiar with this approach for many years.

THE TERM 5S is a reference to five Japanese words that describe standardised clean up and they stand for: Sort, Straighten, Shine, Systemise and Sustain. It is a structured programme to systematically achieve total organisation, cleanliness and standardisation in the workplace.

The overriding idea behind 5S is that there is "a place for everything and everything in its place". Every item that is used in a business process should be clearly labelled and easily accessible. Discipline, simplicity, pride, standardisation and repeatability as emphasised in the Five Ss are critical to the lean enterprise in general and flow implementations specifically.

CLEANING MUST BE carried out by everyone in the organisation, from operators to managers. It is a good idea to have every area of the workplace assigned to a person or group of persons for cleaning. No area should be overlooked. Everyone should see the "workplace" through the eyes of a visitor – always considering if it is clean enough to make a good impression.

Many companies fail in their efforts to sustain for several reasons:

- Too broad an approach
- Not implementing mistake-proof devices (poka yoke = fail safe)
- Lack of preventive maintenance activity
- Lack of accountability for follow through and follow up. Process ownership must be clear. Each defined business process should have an individual assigned to monitor and direct that process.

With the focus on safety, the chances of success increase. Another benefit from focusing on safety rather than only cost-saving is that it makes it less threatening and more acceptable to those who do not understand the true meaning of lean and have only heard that it is a management tool for down-sizing organisations.

Lean Safety, transforming Your Safety Culture with Lean Management, Robert B. Hafey, CRC Press, ISBN 978-1-4398-1642-4

MAK OLIEMAN
mak.olieman@if.se
SALLA LIND-KOHVAKKA
salla.lind-kohvakka@if.fi

Flood risk management must be stepped up

As the climate is warming, companies must think more carefully where they carry out their operations. Thanks to its partner network, If can offer up-to-date information about flood risks and their management.

Flooded banks of the river Seine with the Bir Hakeim bridge in the background are seen after days of almost non- stop rain on January 29, 2018 in Paris, France.

Modern finely tuned subcontracting and supply chains are extremely susceptible to disturbance. These cause customers bigger and bigger losses, and often the root cause is weather phenomena. For example, flood damage to a subcontractor may cause serious problems to a company.

Senior management should be very much aware of not only the flood risks of their own production plants but also those of their subcontractors. Finding out about dependency risks is part of good risk management, although it may require a fair amount of effort.

Property and business interruption losses caused by weather phenomena are an increasing problem, the effects of which can be reduced with proper risk management.

Server and back-up serve in the same cellar

If's International Claims Manager Mike Freeman told at the Risk Management Day for major corporations in March in Helsinki about a case that raised some eyebrows.

"The control systems of a fully automated giant logistics centre had been outsourced to a subcontractor who had in turn outsourced this contact to another contractor. The servers that controlled the logistics centre were located in a basement. During heavy rain the server room flooded which paralysed the information systems and the entire logistics centre for quite some time. Surprisingly the back-up server was also located in the same basement causing a much more extended interruption period.

The same may also apply to your own premises that are exposed to flood and earthquake risks but also to any subcontractors and their subcontractors.

"It is crucial for If's major customers that they can trust If's ability to obtain the best information about flood risk and to assess the risks in each location. This will enable us to assess together what an optimal insurance package should contain," says Reinsurance Manager Tommi Valkama of If.

Contingency plans more and more important

The insurance business operates only under certain conditions. Insurance companies cannot do better than their customers in the long run.

"Climate change will increase flood areas."

"It is a great advantage for us that we have companies like Munich Re as reinsurance partners. They keep a close look on rainfall changes regionally and also over time."

However, just recording rainfall data is not enough. As the climate changes, contingency plans become more and more important, because also the subcontractors and their subcontractors must have such plans.

"Every sector must be ambitious to bring their contingency plans up to date. The need for them increases steadily," said Valkama.

Weather phenomena and dependency risks used to be local

When Carl von Linné visited a copper mine in Falun, Sweden in early 1734, he observed with interest and concern that the air was polluted. A thick sulphurous smoke hovered over the small town and its coughing inhabitants.

However, he did not have to go far to breathe clean air again, because the pollution was very local.

Researchers of today are concerned about two long-term global problems. One concerns the depletion of the ozone layer and the other an increase in carbon dioxide content in the atmosphere.

For example, the climate is forecast to warm up faster in the Nordic countries than the global average. The winters will probably be warmer and rainier. The sea level rise is also forecast to accelerate.

Heat records have been broken in recent years in the Nordic countries, elsewhere in Europe and around the world. The south is suffering from drought, threatening food production and causing, among other things, extensive forest fires.

When rainfall increases in the north, flooding is more common, spring floods start earlier, accompanied by coastal flooding, related to rising sea levels. Elsewhere in the world, fiercer hurricanes and tornadoes are forecast, as are floods affecting wider areas.

Business interruption caused by flooding more common

"When the weather gets warmer, nature will react to it, and the lives of people and businesses change. Vegetation and animal territories move further and further north. Conditions for food production in the Nordic countries, northern parts of Russia and Canada will improve," said meteorologist Lea Saukkonen of the Finnish Meteorological Institute who spoke at the Risk Management Day for major corporations.

"However, the challenge is how the plants will adapt to new climate conditions. Forestry, for example, may be challenging, because the tree sapling planted today should cope with climate change right up to logging," she added.

Climate change will increase flood areas, as a result of which many companies will have to re-asses the location of their production plants already in relatively short term.

Plans concerning production and storage buildings may assume, for example, that the risk of flooding is low on a mountainous highland area, although higher rainfall will increase landslides considerably.

Local changes may be very painful.

"Whenever a flood takes a major production plant by surprise, many jobs will be lost. The plight to the people who lost their jobs is often increased by loss of their homes to the same flood and the fact that once the flood is over, the same or similar company is unlikely to be built in the same place," said Mike Freeman.

As the example told by Mike Freeman showed, building a storage building outside the flood zone is not enough if the servers of a highly automated storage facility and also their back-up systems are located in a flood-risk area even in the same building and, to top it all, in the cellar.

Image of the world's sources of carbon dioxide becoming clearer

Some sceptics still claim that this global warming is quite natural. "Such a view is totally opposite to scientific research findings," says meteorologist Lea Saukkonen.

She says that carbon dioxide molecules in the atmosphere can be subjected to isotope analysis to determine accurately the extent it derives from fossil fuels.

Fossil carbon is released into the atmosphere when people use fossil fuels, such as oil, natural gas or coal. Fossil carbon has been buried underground for millions of years and has therefore not been subjected to cosmic radiation. Carbon found in nature, on the other hand, has been under cosmic radiation all the time. These two types of carbon can be told apart.

"It makes very little difference in terms of atmosphere and climate change where the CO_2 comes from. Only its amount is significant," said Saukkonen.

The objective of the Paris Agreement is to slow down climate change so that the planet warms by less than two per cent. The plan is that the agreement that was signed in 2015 will be applied after 2020.

The image of the world's carbon dioxide sources and carbon sinks are getting clearer all the time. By 2020 we should have reached the stage where new satellites will chart large areas at a time, instead of the current measurements taken only in specific locations.

New observation methods and increased calculation capacity will enable us to collect and process a much larger amount of data.

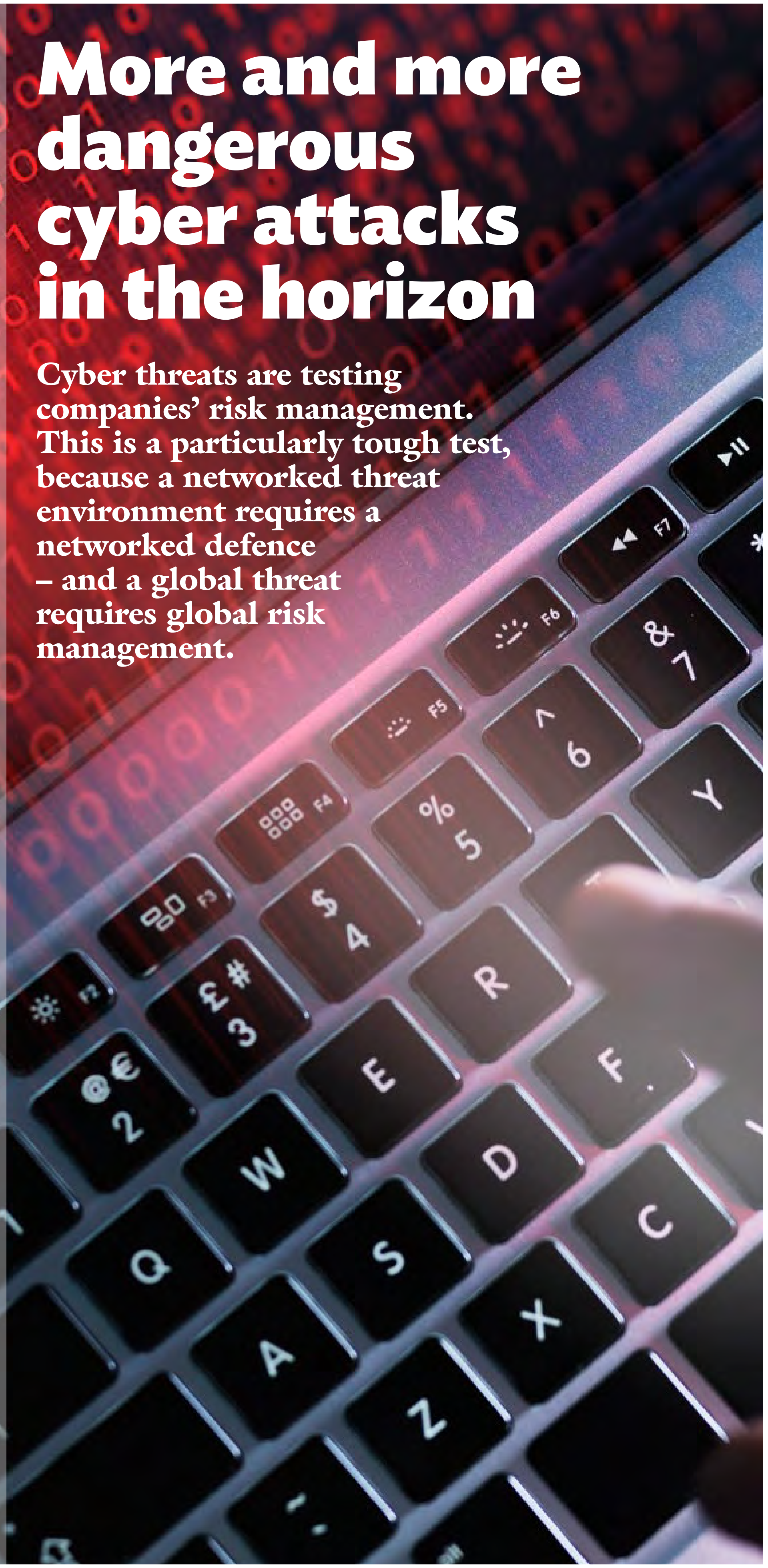
Good to remember when things go wrong

During extreme weather, the damage usually extends to traffic connections and other infrastructure, for example. This means that connections are lost, preventing you from getting to the plant or storage facility, even of the plant itself was functioning.

If's global network consists of local insurance companies that are the best in their respective countries.

In each loss and especially after serious dangerous situations, If always works in close cooperation with local service providers.

HARRY NORDQVIST
harry.nordqvist@if.fi



More and more dangerous cyber attacks in the horizon

Cyber threats are testing companies' risk management. This is a particularly tough test, because a networked threat environment requires a networked defence – and a global threat requires global risk management.

This is the period when it will be decided which companies can protect against cyber criminals' attacks.

"This has become an unprecedented security problem," says cyber risk engineer Peter Granlund of If's Risk Management.

This was a view shared by the world's economic leaders at the World Economic Forum. Information systems are a critical part of any company's operation, and threats against them have grown. According to studies, cyber risks are considered by many major companies as the most serious threat to operations.

Companies are becoming more and more networked. Robots are controlling robots. New factories and production plants are fully automated. Operations are controlled by means of information systems and their backup systems.

"Understanding the effects of cyber threats on our own business is one of the main priorities of our large customers. In order to meet our customers' security needs, we have plenty of information in our Competence Center on what companies should take into account to improve their cyber safety," says Matti Sjögren, If's Nordic Liability Risk Management Specialist.

Alarming example

Recent years have begun with big questions about corporate cyber safety. These have been followed by one nasty surprise after another.

Cyber risk engineer Peter Granlund gives us an example, which will be discussed in details in another article, Maersk Line attack, in this magazine.

"For few days they had to return to handle everything by paper or Excel spreadsheets. At some of their container terminals it was impossible to handle goods. The financial impact was 300 million dollars in Q3".

According to Peter Granlund, companies' key jobs in our modern fast-moving world is to ensure that they have the right partners to fight against cyber threats. He also thinks every organisation should be able to respond to following questions about cyber securities:

- What processes and assets are important to protect?
- Have you considered the impact of a cyber attack?
- Do you know your cyber threats or weaknesses?
- Do you know what you'd do if you're attacked?
- Do you know what cyber insurance can cover for you?

"Companies must also raise their personnel's readiness to fight cyber threats. The human factor must never be forgotten. When talking about cyber security, people often only focus on technology and forget about human activity," says Senior Risk Engineer Erik Van Der Heijden of If's Risk Management.

Chief Information Security Officer Erka Koivunen of F-Secure Corporation said in the Risk Management Day event organised by If in March in Helsinki that previously hackers were motivated by the challenge of whether they could work their way in. If you could break into the information system of a major company, your prestige among your peers was guaranteed.

"One of the key factors is risk identification."

This is no longer the case today. Today's cybercriminals (states, criminals and terrorists) are skilled, have sufficient resources, and patience to perform highly successful attacks on consumers, businesses and governments around the world.

Cybercrime is today Big Business, while the risk of attackers being traced and prosecuted is low.

It all begins with risk identification

One of the key factors is risk identification. By a thorough assessment of risks and wise channelling of measures to stave off attacks you can improve security quite significantly without any major extra costs. Any resources thus saved can be used, for example, to make the personnel aware of any risks.

And besides, few organisation have endless resources to improve their cyber safety. On the other hand, nobody can promise 100 per cent security.

"Organisations should first find ways to reduce risks for example by acquiring competences and services which would be too expensive to develop in their own organisation. The new phase requires new systems and efficient protection solutions. To fight cyber threats, you need reliable partners," says Erka Koivunen of F-Secure Corporation.

As cyber threats increase in number, frequency and complexity, it is more and more important to identify, understand and manage all aspects of cyber safety. It is a matter of ensuring continuity of your own operations.

The attitudes of those who decide about investments may be one thing, but the risks may be of quite another nature.

"Many can be under the misapprehension that a virus protection program bought 5–6 years ago can take care of the entire cyber safety issue, but the truth is something quite different."

Managing Cyber Risks Together

If's Risk Management's target is to do everything that its clients can find an optimal way to keep a variety of cyber attacks at bay.

For this purpose, If's Risk Management has come up with a 25-point survey questionnaire to find out how companies deal with data security. The aspects focused on include Cyber Risk Management Organisation, awereness training, defence in depth, parch management process and business continuity plan.

Once a company's data security is sufficiently high, we can help manage the remaining risk.

"Cyber security is extremely important and managing it has become a profession in itself with strategic, tactical and operational requirements to consider. The IT department is not the most likely candidate to handle cyber risk management", says Peter Granlund.

If can provide insurance solutions supporting our client's management of risk.

"Once a company is sufficiently prepared against cyber threats, we can insure the remaining risk. A key product for industry is property and business interruption cover as part of property insurance which, if a cyber risk is realised, covers financial losses caused by business interruptions. Our comprehensive cyber insurance also covers, thanks to its various modules, losses caused to both yourself and third parties. EU's General Data Protection Regulation (GDPR) will enter into force in May 2018, and the risk for compensation about loss of customer data will increase," says Sjögren. ■

HARRY NORDQVIST
harry.nordqvist@if.fi

Global trade disrupted by cyberattacks

As an insurer we are well aware of so-called "Black Swan" events, i.e. events that are deemed so unlikely that they are not really taken seriously when calculating risks. For many years this has been the case with cyber risks. Imperceptible. Unlikely. Intangible.

Until just recently, that is.

In June last year, global shipping giant Maersk Line, which handles one in seven containers shipped globally, was hit by a ransomware attack. With a fleet of more than 600 container vessels, Maersk is the world's largest shipping company. The company handles around 25 percent of all containers shipped on the key Asia–Europe route and transports about 16 percent of the world's seaborne manufactured trade. Hence, this cyberattack had a real impact on global trade.

In the week following the cyberattack Maersk's loading volumes dipped from typical levels of around 210,000 forty-foot containers to 160,000. The attack came at a time when Maersk had rolled out a new digitisation strategy to modernise an industry in which most orders were still placed via phone. Maersk was forced to return to manual operation and had to handle a backlog of orders. However, just two days after the attack, Maersk Line was able to take orders from existing customers and things gradually got back to normal over the following week and returned to normal by the middle of July, according to its CEO.

The cybersecurity risk was also highlighted as a major risk in the World Economic Forum's Global Risk Report, and the World Economic Forum mentioned it in their Executive Summary:

"Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace. The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack—which affected 300,000 computers across 150 countries—and NotPetya, which caused quarterly losses of US$300 million for a number of affected businesses. Another growing trend is the use of cyberattacks to target critical infrastructure and strategic industrial sectors, raising fears that, in a worst-case scenario, attackers could trigger a breakdown in the systems that keep societies functioning".

THE MAERSK ATTACK infected computers through ransomware that encrypted the hard drive – with the so-called NotPetya virus. It started due to a breach in the Ukraine and impacted the systems of Maersk's parent companies. The breakdown affected all business units at Maersk, including container shipping, port and tug boat operations, oil and gas production, drilling services and oil tankers. The cyberattack mainly impacted Maersk Line, APM Terminals (which reported that some 17 shipping container terminals run by APM Terminals had been hacked) and Damco, as well as negatively affecting business volumes for a couple of weeks in July last year. Maersk's APM Terminals unit, which operates 76 port and terminal facilities in 59 countries around the globe, was impacted at a number of sites, including the Port of New York and New Jersey, the largest port on the U.S. East Coast, and Rotterdam in The Netherlands, Europe's largest port.

The attack, similar to the WannaCry virus, reached Asia after spreading from Europe to the U.S. overnight, hitting businesses, port operators and government systems. Hackers told their victims to pay USD 300 in cryptocurrency (Bitcoin) per infected computer to unlock their systems.

The ransomware took advantage of certain security vulnerabilities in Windows that Microsoft patched after they leaked. It was a previously unseen type of malware and updates and patches applied to both the Windows systems and antivirus were not an effective protection in this case, according to Maersk.

"The Maersk attack infected computers through ransomware."

Not only Maersk was affected but also Ukraine's central bank also said a number of Ukrainian commercial banks and state and private companies had been hit by cyber-attacks via an "unknown virus". It is important to remember that Maersk was more likely than not collateral damage of an attack on the Ukrainian government. To that end it is exceedingly likely we will see a repeat. Shipping company Maersk Line has said that the June cyber-attack could cost it up to USD 300 million in lost revenue.

Maersk Line managed to stay in profit despite the attack. Maersk Line reported a net profit of USD 220 million in the third quarter, compared with a loss of USD 122 million in Q3 16. Turnover at Maersk Line increased year-on-year by 14% to USD 6.1 billion, boosted by a 14% hike in its average freight rate to USD 2,063 per feu[1]. The star performers were the carrier's Asia–Europe and transpacific east–west trades, where average rates jumped almost 20% to USD 2,186 per feu. Maersk's operating profit before depreciation and amortisation (EBITDA) of USD 2.06 billion was in line with the USD 2.05 billion forecast by analysts.

THE 2017 CYBER ATTACK proved extremely difficult for Maersk Line and they have since revised and invested in their system architecture to reduce cyber risks to ensure that its operations do not get impacted by any such global breach in the future. You can build up your cyber fortifications, but partners in trade and container supply chains need to develop contingency plans, as it is a near certainty that the industry will be hit by another cyber-attack. The question is not if, the question is when.

Every cloud has a "silver-lining" and for Maersk it was how all its key stakeholders, including customers, authorities and employees reacted to the attack. Overnight, the company switched over to manual operation from its computer-based systems, while some customers supported the company by increasing their orders. Whilst Maersk had business continuity plans, it was not prepared for the total impact and has since put in place new, different and further protective measures following the attack.

As a risk manager – always expect the unexpected. Even though cybersecurity risk awareness is currently high and on the agendas of all risk-conscious companies – as shown above – having the right insurance could prove valuable. Literally. ■

TONY SCHRÖDER
tony.schroder@if.se

[1] Forty-Foot Equivalent Units. Refers to container size standard of 40 feet. Two 20-foot containers or TEUs equal one FEU.

Companies are being forced to re-examine their approach to digital risk management.

Managing risks in the digital age

The unplugged company is history. Should businesses be worried about their own products?

Being connected to the internet is another day at work. Nothing special at all. But...

Kristine Birk-Wagner is Head of Casualty & Marine Cargo at If. She has headed the development of the new cyber insurance and is heading If's Cyber Competence Centre. She talks about the challenges faced by the interconnected company.

Kristine Birk-Wagner

You deal with businesses from all industries. What is the most important change you have noted in recent years?
Like others, I think the shift from a physical to a more connected or digital world is one of the major changes. This shift has consequences we have not yet grasped. Not only do we transfer data and knowledge across international borders, but also through methods and across media that we have not thought of as being communicative before. Now someone can use – or misuse - your own interconnected products to carry out a DoS (Denial of Service) attack on your company website. Such a scenario, I would assert, had not been considered by many people five years ago.

In what way are digital risks or disruptions a challenge?
Actually, they are a challenge from different angles. Companies face disruption to their production because of criminal acts such as hacking – as we saw last summer with NotPetya – which led to multinational companies being unable to process orders for parts of their business for several days. Another angle is disruption due to errors that are not related to criminal acts. Right now we are seeing disruption to the supply chain, where we experience companies or their suppliers not being able to deliver or deliver on time due to Denial of Access as a consequence of natural hazards or bankruptcy.

Why is communication between physical products a risk to businesses?
Companies have to focus on securing communication lines not only between people, but also between products – an example is your mobile phone communicating with the heating system in your cabin. Products are often tested for their intended purpose and are proved to work. However, we must also focus on the misuse and vulnerability that is uncovered long after the product was made. It is a challenge to ensure that products communicate and interconnect safely and that we have a long-term commitment to maintaining the security during a products' life cycle. We have understood that we need to secure our communication with people, but will we be good enough at ensuring the security of the communication between products that are active on a global market in five years? ■

MARIANNE WIINBLAD
marianne.wiinblad@if.dk

How to prevent e-mail spoofing

Do you know how your company can reduce the volume of phishing e-mails that target your company and brand?

E-mail scams have increased rapidly in recent years. For example, in 2016 a Swedish manufacturer lost SEK 25 million due to this kind of scam. In such cases, criminals impersonate a company executive and send a fake e-mail message to selected employees, tricking them into wiring funds.

DMARC (Domain Message Authentication Reporting and Conformance) can protect you from this. DMARC is an internet protocol specification that provides visibility into e-mail flows and can tell receiving servers to delete spoofed messages immediately when received, thereby ensuring that only legitimate e-mails are delivered to inboxes. Approximately 70% of consumer inboxes worldwide are protected by DMARC – that is more than 2.5 billion mailboxes worldwide. However, many organisations are still not aware of DMARC and its benefits and only one-third of businesses and other organisations have implemented DMARC as part of their validation process.

Within If, we think that every organisation with a domain name should consider using DMARC to help reduce spam and phishing attacks that target their brand.

How does it work?

A DMARC policy allows the sender to indicate that their messages are protected and advises the receiver what to do – nothing, quarantine, or reject – if a received message does not match the DMARC policy. Because the specification is available with no licensing or similar restrictions, any interested party is free to implement it.

What are the benefits?

DMARC benefits both recipients and senders. E-mail recipients are warned if an e-mail is fraudulent or harmful and don't have to guess what to do with e-mails that fail the DMARC authentication. Senders can now identify how much e-mail is coming from their own domain (or claiming to come from their domain), where it originated, and how recipients are handling the e-mails.

Can DMARK combat all types of e-mail attacks? No, DMARC can only provide protection against direct domain spoofing. If the owners/operators of example.com use DMARC to protect this domain, it would have no effect on example.eu (note the ".eu" vs. the ".com").

How do you get started?

Although it can technically take less than an hour to build and publish a DMARC record, it is smart to first involve all teams that have a stake in e-mail security (security, marketing, fraud prevention, service desk, system administrators, and others) and then consider deploying DMARC in three steps:

Monitoring mode: In monitoring mode, you advertise to the internet that you want all DMARC-compliant e-mail receivers to send you reports on who is sending e-mails from your domain. No e-mails will be flagged, blocked, rejected or quarantined.
Quarantine mode: In quarantine mode, suspicious messages are flagged for review. This allows you to identify all internal and authorised e-mail servers and ensure they have been configured properly.
Reject mode: In reject mode, spam and phishing messages are deleted by DMARC-protected e-mail servers. This enhances the trust relationship between e-mails sent by you and received by DMARC-protected mailboxes.

As a final step, DMARC should be leveraged to detect and mitigate threats since it provides valuable reporting information about the amount and structure of phishing attacks and can help to improve fraud intelligence around targeted attacks on your brand. ■

For further information, visit the Global Cyber Alliance's website
https://dmarc.globalcyberalliance.org/

PETER GRANLUND
peter.granlund@if.se

Protecting our investments in emerging markets

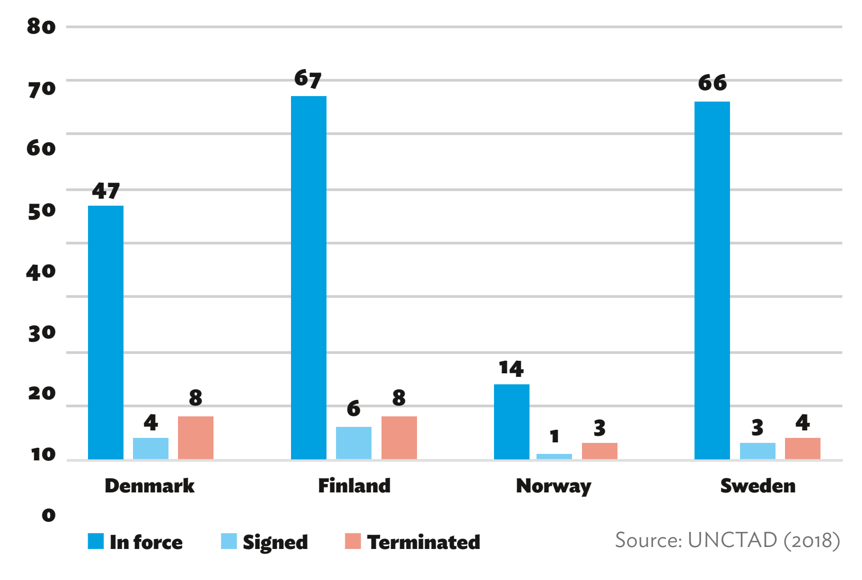
Data from the statistical service of Norway, Sweden, Denmark, and Finland in the past years show that Emerging Market countries have become an interesting investment destination for Nordic companies.

When executives of multinational enterprise (MNE) decides to expand the operations of their firms into foreign countries in emerging markets, they are faced with several important strategic decisions, including, which operation form to establish adapt i.e. start the operations from scratch (build of facilities) or through acquisitions (buy equity share in an existing foreign entity). They are also faced with whether to do it alone (to establish a wholly owned subsidiary) or to involve a local partner (to establish a subsidiary with shared ownership), in addition to financial, HR, and operations considerations.

As such, supposedly negative discussions are paid rudimentary attention. How would Nordic executives reach if years after expansion and operation in a country, the host government decide to increase taxes on profit by 100%? How would you react if the local authorities in a destination country decide to put a cap on l repatriation of profits? Or raise local requirements? Collectively, these are called political and regulatory risks. That is, the probability that a host government/authorities will discretionary change laws, regulations, or contracts terms governing an investment or refuse to enforce them in a way that reduces a foreign investor's returns on that investments. To most executives, these will obviously go against their legitimate expectations.

Emerging markets are characterized by underdeveloped institutions and frequent environmental shifts (Khanna and Palepu, 2014). This brings uncertainties to investments that can have a huge consequence for Nordic companies expanding into these places. Ex-post modifications of the legal framework in force at the time when the investment was made or interference with the investment in response to external pressures such as public opinion leading to (in)direct expropriation of assert from investors. The nature of these risk is not static – they change over time. For instance, a recent study by the Wharton School found that although outright expropriation of foreign assets by host countries in emerging markets have largely disappeared (Henisz and Zelner, 2014). As investors interest in developing countries/emerging markets grow, some host governments have learned, that more value can be extracted from foreign enterprises through the subtler instrument of regulatory control rather than outright seizures. This new risk is the main concern of today's investors. In this article, I would like to introduce our cherished Nordic clients how are to prepare their investment and maneuver these risks when expanding their businesses overseas.

Figure 1: Number of investment Agreements signed by Nordic countries as of January 2018



The good news is that political and regulatory risks can be managed. Almost all (Nordic) governments have been very active in helping investors from managing these risk in emerging markets by signing various International Investments Protection Agreements (IIAs) with most emerging markets governments. Today, there are 3,000 IIAs in existence around the world. Among the Nordic countries, Finland has the most investment agreements, with 67 agreements in force[1], followed by Sweden with 66 investment agreements in force[2], see Figure 1.

Below, I discuss some of the ways investor can mitigate against such risks and protect their investments in emerging markets.

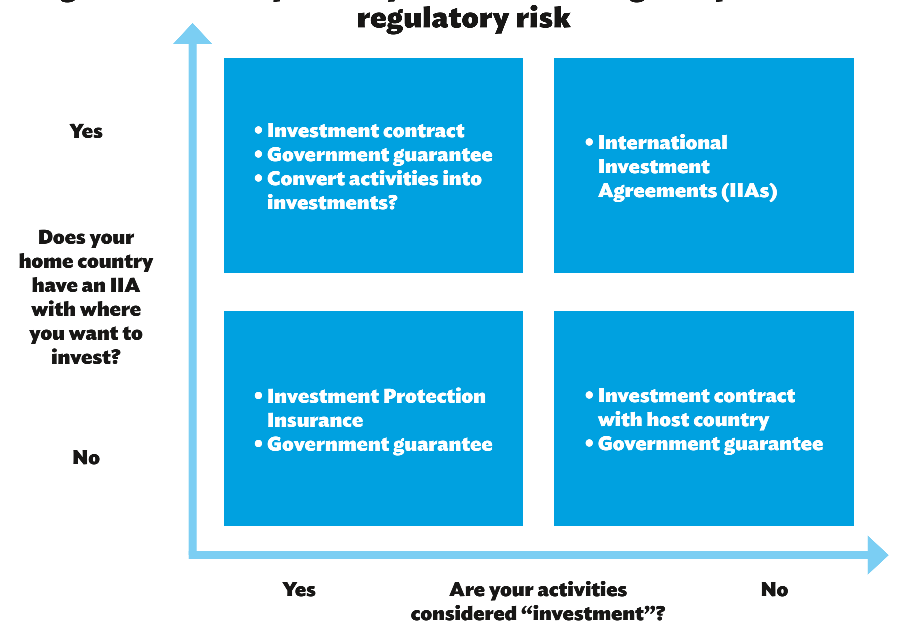
Are you really making an investment?

"In order to qualify as an investment under this Agreement, an asset must have the characteristics of an investment, such as the commitment of capital or other resources, the expectation of gain or profit, or the assumption of risk"

Norway's model Bilateral Investment Treaty (2007)

International investment Agreements protect investments. Research shows that most executives wrongly assume that once they are doing business in other countries, they are investors doing investments in that country. It is important to point out here that this may not necessarily be correct. Not all economic activities abroad qualify as investments. As such, to be eligible for protection, you must make sure your activities qualify as "investments". What is an investment varies from between countries, for instance, between Denmark and Argentina, an investment is defined as: "… every kind of asset connected with economic activities…" However, between Finland and Argentina, investment is defined as "…every kind of asset invested by

Figure 2: How to protect your investment given political and regulatory risk



an investor of one Contracting Party in the territory of the other …"

We will not go into the legal interpretations here in this article, however, the point I want us to arrive at is that what executives may consider an investment, may in reality not be investments since definitions vary. Historically, investment disputes resolved by the International Center for the Settlement of Investment Disputes (ICSID), under the auspices of the World Bank, have adopted a "unified" definition of investments with four key elements: a contribution of money or assets, a certain duration, an element of risk and a contribution to the economic development of the host state. This is the so-called "Salini test". It is only after it is determined that one is making an investment that the benefits ascribe under IIAs applies to you and your investments.

The mechanisms available to investors

Suppose you are involved in investment in emerging markets. How do you ensure that those investments are protected against volatile political and regulatory risks? Broadly speaking, there are four mechanisms available to investors:

1. International Investment Agreements;
2. National investment legislation;
3. Investment contracts; and
4. Oversees investment insurance

Let me explain how each of these mechanisms works.

Investment Agreements

International Investment Agreements (IIAs) are effective mechanisms for protecting Nordic investors' investments against political and regulatory risk. International Investment Agreements are government-to-government treaties that provide legally binding, (usually privately) dispute settlement and enforceable rules regarding one country's treatment of investment from another country that is party to the agreement. Investment agreements usually come in three forms:

1. Bilateral Investment Treaties (BITs) signed by two states;
2. Regional Investment Treaties signed by groups of states within a single region;
3. Chapters of integrated trade and investment agreements that can be signed at the bilateral or regional level.

> "Investors must be aware that National investment legislations are made voluntarily by national parliaments."

Investments covered by such IIAs such as Bilateral Investment Treaties (BITs) enjoy protection against direct interferences such expropriations (direct or indirect), and unfair and discriminatory treatments[3]. Investors whose investments are covered by BITs in most cases have the privilege of investor-host state dispute settlement systems in case of authority's actions are interference and against their legitimate expectation. Investment treaties when signed between more than two countries are called Multilateral Investment Treaties (MITs), examples of MITs are the North American Free Trade Agreement (NAFTA) signed between the USA, Canada, and Mexico, or the Energy Charter Treaty (ECT) signed or acceded to by fifty-two countries including the all EU countries, Australia, Norway, and Russia.

National investment legislations

In addition to International investment agreements (IIAs) such as Bilateral Investment Treaties (BITs) and MITs, many emerging market countries, in their attempt to attract foreign investments have enacted legislation to guarantee protection for foreign investors. The content of such legislation varies from country to country. However, generally, they contain guarantee or exemption from taxation regimes or provide a specific fiscal regime for investors in a particular industry or service sector. Just like BITs, these unilateral actions are binding[4]. However, investors must be aware that National investment legislations are made voluntarily by national parliaments, as such any protections contained in such legislation may be subject to revocation by a subsequent government. As such, relying solely on investment agreements might not be the best kind of protection for a long-term investment.

Investment contracts

Nordic companies can also enter into an investment contract with a host government of a country they would like to invest. Host governments in emerging market countries are willing to sign investment contract particularly when investments projects are considered critical for the nation, such as infrastructure projects. These contracts will specify the legal rights and obligations between the investor and the host government. The advantage of investment contracts is that it is binding on subsequent governments. However, a contract with a local government will in most cases be subjected to laws of that country. This means that any dispute arising out of the contract will be resolved through the local court system. Do not enter into an investment contract with a country authorities if you do not trust the legal system in that country.

Insurance to mitigate risks

Many governments and private insurance companies offer offers foreign investments protection insurance and other insurance products to protect investors against losses on overseas investments resulting from political and regulatory actions by host governments. In Norway for example, the Garantiinstituttet for eksportkreditt (GIEK), under the Ministry of Trade, Industry and Fisheries issues guarantee on behalf of the Norwegian State to private firms to cover political and regulatory risk, in addition to credit enhancement guarantees to protect investors assets against non-commercial risks at a fee. Other private organizations such as the Multilateral Investment Guarantee Agency (MIGA) of the World Bank Group offer insurance for private investors.

As one might recognize, the above options are not mutually exclusive, executives can combine several mechanisms to ensure that their investments are fully protected against political and regulatory risk, as the optimal mechanism depends on your situation as an investor.

> "Succeeding in these markets is learning to manage risks."

For instance, it will be prudent to rely on IIA if there exists an investment treaty between your home country and the destination country for your investment. Insurance or an investment contract will be your choice if no IIAs exist between your destination country and your home country. In figure 2 I present a summary "option card" for executives depending on whether there is an IIAs between your home country and your host country, and whether your activities are considered "investments" or not.

The above is only a suggestion, as such, there may be a better alternative depending on one's situation. But, whatever the case, make sure your investments are protected. Investing in emerging markets may be risky, however, they may be the most effective means of diversifying your portfolio in the long term. Succeeding in these markets is learning to manage risks. We hope that this article provides you with some of the options available to you as a Nordic investor interested in emerging markets on how to ensure that your investments are protected against political and regulatory risks in your chosen countries. ■

GILBERT KOFI ADARKWAH
gilbert.kofi.adarkwah@if.no

References

Henisz, W., & Zelner, B. (2014). The hidden risks in emerging markets. IEEE Engineering Management Review, 42(2), 27-34. http://dx.doi.org/10.1109/emr.2014.6823807

Khanna, T. and Palepu, K. (2014). Winning in Emerging Markets. Boston: Harvard Business Review Press.

Regjeringen.no. (2018). Norway Common Model Agreement for future investments 2007. [online] Available at: https://www.regjeringen.no/contentassets/e47326b61f424d4c9c3d470896492623/draft-model-agreement-english.pdf [Accessed 1 Feb. 2018].

UNCTAD - Bilateral Investment Treaties. (2018). Investmentpolicyhub.unctad.org. Retrieved 25 January 2018, from

Grabowski, Alex (2014) "The Definition of Investment under the ICSID Convention: A Defense of Salini," Chicago Journal of International Law: Vol. 15: No. 1, Article 13. Available at: http://chicagounbound.uchicago.edu/cjil/vol15/iss1/13

[1] As of January 2018, Finland has investment agreements in force with: Albania, Algeria, Argentina, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Bulgaria, Chile, China, Croatia, Czech Republic, Dominican Republic, Egypt, Salvador, Estonia, Ethiopia, Georgia, Guatemala, Hong Kong, China, Hungary, India, Indonesia, Iran, Jordan, Kazakhstan, Kenya, Korea, Kuwait, Kyrgyzstan, Latvia, Lebanon, Lithuania, Macedonia, Malaysia, Mauritius, Mexico, Moldova, Mongolia, Montenegro, Morocco, Mozambique, Namibia, Nepal, Nigeria, Oman, Panama, Peru, Philippines, Poland, Qatar, Romania, Russian, Serbia, Slovakia, Slovenia, South Africa, Sri Lanka, Tanzania, Thailand, Tunisia, Turkey, Ukraine, United Arab Emirates, Uruguay, Uzbekistan, and Vietnam. There were six agreements signed but not in force yet. These were with Brazil, Costa Rica, Cuba, Kazakhstan, Nicaragua, and Zambia.

[2] Sweden active investment agreements are with the following countries: Albania, Algeria, Argentina, Armenia, Belarus, Bosnia and Herzegovina, Bulgaria, Chile, China, Côte d'Ivoire, Croatia, Czech Republic, Ecuador, Egypt, Estonia, Ethiopia, Georgia, Guatemala, Hong Kong, Hungary, India, Indonesia, Iran, Kazakhstan, Korea, Kuwait, Kyrgyzstan, Lao, Latvia, Lebanon, Lithuania, Macedonia, Madagascar, Malaysia, Malta, Mauritius, Mexico, Mongolia, Morocco, Mozambique, Nigeria, Oman, Pakistan, Panama, Peru, Poland, Romania, Russia, Saudi Arabia, Senegal, Serbia, Slovakia, Slovenia, South Africa, Sri Lanka, Tanzania, Thailand, Tunisia, Turkey, Ukraine, United Arab Emirates, Uruguay, Uzbekistan, Venezuela, Bolivia , Vietnam, Yemen.

[3] Through provisions such as the Fair and Equitable treatment (FET), most-favored-nation (MFN) treatment, as well as National treatment. Meaning that these firms or investment must be afforded the treatment that is equal to the best any other investment or firm in their industry can enjoy.

[4] See ICJ judgement in Australia v. France.

Supply Chain Insurance

A new insurance product by If

What do you do if your supply chain breaks down?

The risk of a supply chain glitch is a threat that has risen with the increased demand for just-in-time delivery, higher storage costs, and hazards beyond the company's control. This risk is ever present – without there having to be any physical risk of damage to any of the insured party's interests.

Modern supply chains may be flexible and cost-effective, but they are also more vulnerable to disruption. Whilst business interruption insurance products are governed by a physical loss within the remit of the insured party, supply chain insurance is not. For many businesses, comprehensive business interruption coverage is increasingly being seen as an essential part of today's insurance policy.

Supply chain – what is it?

Definitions of "supply chain" almost universally encompass the following three functions: supply of materials to a manufacturer, the manufacturing process, and the distribution of finished goods through a network of distributors and retailers to a final customer. Companies involved in various stages of this process are linked to each other through a so-called "supply chain".

To facilitate the flow of products, information is shared up and down the supply chain, i.e. with suppliers and clients. This sharing of information enables all parties to plan appropriately to meet current and future needs. The more that companies within a supply chain can integrate and coordinate their activities, the more likely they will be to optimise the flow of goods from supplier to customer and react effectively to changes in demand.

Causes of disruption loss

Global supply chains are increasing the severity and frequency of business interruption claims, with the average large business property insurance claim rising to millions of dollars and many thousands of claims per year. Increased interconnectivities and interdependencies between companies, as well as lean production processes, have contributed to both the rise in business interruption claims and new risks to businesses. The main causes of business interruption loss globally are adverse weather, unplanned IT or telecoms outage, transport network disruption, earthquakes/tsunamis, as well as volcanic ash clouds, insolvency, civil unrest and fire.

No physical damage

As mentioned briefly above, Business Interruption (BI) and Contingent Business Interruption (CBI) insurance products have been on the market for many years. But in order to trigger cover, there needs to have been physical damage – such as an industrial fire – that triggers the BI loss. When it comes to Supply Chain Insurance it will rather be triggered by an external event, beyond the control of the insured party.

The If touch

What sets the If product apart from other Supply Chain products currently on the market is that If has simplified the calculation of the Business Interruption loss by having a pre-agreed daily indemnity that will be paid out (less pre-agreed deductible days) – up to a number of pre-agreed maximum number of days (which can be, for example, 90 days or 180 days). As this is all pre-agreed, there is no need for what are usually quite complex and time-consuming business interruption calculations.

The product is targeted to work as a supply chain disruption (financial) safety net so that disruptive events will not completely ruin a business. Whilst it might be a tool that produces a rough estimate, it will ease the most severe and imminent business/supply chain-related (financial) concerns.

If has already seen a keen interest in this product and hopes it will be an attractive solution for medium to large enterprises to safeguard their continued business operations. ■

TONY SCHRÖDER
tony.schroder@if.se

Consolidating expertise

If establishes competence centres within several areas.

As the largest general insurance company in the Nordic countries, If wants to give its industrial clients good advice in the area of risk management, amongst others. Thus, the collaboration between the specialist communities of the different countries is now being strengthened to provide clients with better access to expertise within business interruption, natural hazards and cyber risks, among other areas.

Cross border

"Through competence centres we utilise the best resources and skills without having borders," says Jukka Forssén, Head of UW Property Nordic at If Industrial.

"The best of our expertise and knowledge from If Industrial is gathered and transferred to practical services, tools and products, which improve our ability to provide optimal solutions for our clients. We are a truly Nordic company, which is our strength. We have underwriting specialists, as well as claims, risk management and other specialists in all Nordic countries and also in the UK, Netherlands, France and Germany. Most of our clients are international and operate in multiple countries. Working across borders we can utilise the best of our expertise and skills to the benefit of our clients," says Forssén.

Clients will benefit from improved services, such as risk management tools and lessons from losses – and enhanced insurance products that are better tailored to meet client needs. The knowledge is shared through client seminars, articles in If News and Risk Consulting, and, of course, through direct client service and interaction with If's specialists.

> "Working across borders we can utilise the best of our expertise and skills to the benefit of our clients."

International network

One area under rapid development is cyber risks.

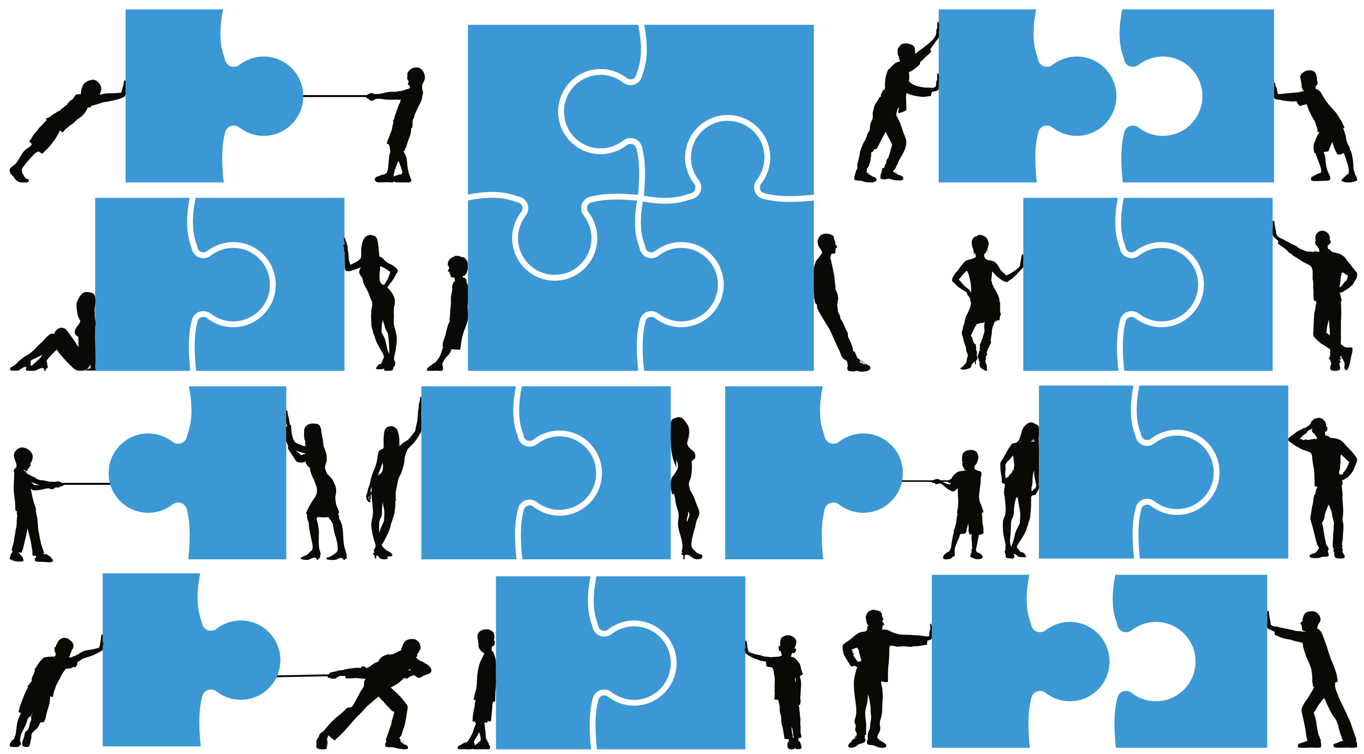
"We must therefore be able to constantly adjust our understanding of our clients' need. It is obviously important that decisions are made on the most optimal basis and aligned throughout the Nordics. This will be ensured through the competence centre," says Kristine Birk-Wagner, Nordic Head of Casualty & Marine at If Industrial.

The clients will benefit in various ways: "They will have access to our highly-specialised experts who have the expertise to support their IT security. They will be ensured products that are continuously evaluated and improved and, as always, a specialised claims team," says Wagner.

Sirpa Peura is Nordic Head of EB & Motor Underwriting at If Industrial. She emphasises how knowledge and knowledge exchange will benefit the client.

"The competence centre for travel and expats has a strong cooperation with If's international network, and knowledge is shared in various forums with other underwriting units in both If Industrial and If Commercial business areas. It ensures the quality of our work for clients and brokers," says Peura. ■

SIGMUND CLEMENTZ
sigmund.clementz@if.no



EXPLOSIONS in boiler fuel infeed

Damaged building due to overpressure from CO-explosion in a chain conveyor inside.

The number of explosions in fuel systems in direct connection with various types of boilers seems to have increased in recent years.

The cause of the increase is unclear but may be partly due to changes in fuel. The explosions are caused by unburned gases being forced backwards from the furnace due to disturbance of combustion. With few exceptions, the root cause can be attributed to a design flaw in the boiler fuel infeed. The consequences can be quite serious and cause extended outages, depending on the time required to repair physical damages as well as to investigate the matter and make rectifications in response to findings. The Swedish Work Environment Authority often requires that a full investigation of the accident must be performed before the facility can be put back into operation. Incidents often lead to unease and a sense of insecurity among personnel, which can have a negative impact on operating safety.

In order to prevent explosions, existing systems can be analysed in order to identify any weaknesses. Often, relatively simple measures can be taken to reduce the probability of an occurrence. Alternatively, or in combination with such measures, actions reducing the consequence can be employed to reach a tolerable risk level.

Background

In recent years, P&B has investigated a number of explosions in fuel infeed equipment for boilers. Though it has not been possible to establish statistically, our perception – and that of our customers – is that the frequency of this type of incident has increased. It has been possible to establish with high probability that all these explosions were caused by unburned gases from the boiler being forced backwards in the fuel system, primarily causing a gas explosion.

There is no unequivocal proof that the incidents are directly linked to a certain type of boiler or fuel. Explosions have occurred in connection with circulating fluidized bed (CFB) and bubbling fluidized bed (BFB) and gate boilers and ovens fired with dry fuel such as pellets and briquettes, but also wetter fuels such as recycled wood chips, forest fuel and waste. There is however a certain predominance of incidents in connection with simpler, smaller grate boilers in the <10 MW class.

The consequences of the explosions investigated varies from minor deformations of the fuel system to more extensive damage both to the equipment and buildings. From a purely technical perspective, however, all of these explosions can be categorised as relatively weak in relation to a worst-case scenario. The combustion speed and thereby the speed of the rise in pressure is normally deemed to have been a maximum 5–10 % of what the effect would be with an optimal gas/air mixture. Should ignition occur with a more optimal mixture; a scenario which cannot be ruled out, the effect can in the worst case impact a considerably larger part of the system than normal and the explosion may result in overpressure even in larger sections of a building, entailing a risk that parts of the building structure will be destroyed. The consequence of the explosion also depends heavily on the magnitude of the risk that dust layers inside and outside of the equipment are swirled up, aggravating the primary explosion.

Luckily, none of the incidents investigated by P&B have led to personal injury, but in several cases the effects have been so severe that injuries could have occurred if personnel had been exposed. In most cases, the personnel have perceived the explosions as serious and this has resulted in varying degrees of anxiety and a sense of insecurity for those working in the facilities affected.

Backfire protection, no guarantee against gas dispersion

All combustion facilities are equipped with some type of protection and monitoring to prevent backfire in the fuel system. The basic protection always consists of monitoring and control in order to ensure the furnace has an underpressure in relation to its surrounding environment, including the fuel system. Normally, monitoring is carried out through pressure transmitters that controls the underpressure regulator via a flue gas fan, and in some cases in combination with combustion air control in the event of greater deviations. In addition, there is normally an overpressure switch that shuts down the boiler if the pressure exceeds the set level during a given time interval.

As a complement to the pressure monitoring, there are e.g., rotary valve feeders, shut-off valves and various methods of ensuring that the fuel creates a barri-

Signs of heating from back-fire and hot gases in stoker screws and bin.

Hybrid explosion (gas and dust) in a chain conveyor to BFB boiler.

er in chutes or fuel bins. The temperature in the fuel system is monitored continuously and controls activation of the extinguishing systems in the form of steam or water extinguishing, as well as interlocking of the fuel infeed, rotary valve feeders. Simpler facilities with grate boilers normally feature a thermomechanical sprinkler which does not send a signal to the control system, often supplemented with a temperature sensor that triggers an alarm at temperatures lower than the activation temperature for the sprinklers. The temperature sensors are virtually always mounted on the outside of chutes, bins or feeders.

In most cases, the backfire protection is effective against fires that start in the fuel directly adjacent to the boiler and spread backwards. In cases where for various reasons an overpressure is created in the furnace, however, the protection is limited or non-existent when it comes to unburned gases, and flue gas can be forced back through the fuel system. Nor does the fuel barrier provide reliable protection but potentially offers a certain limitation which depends on the design of the system and the fuel fraction. Rotary valve feeders allow gases to pass backwards without any major limitation than volume capacity, as long as they are in operation. Slide gate valves normally do not form a tight enough seal to guarantee that gases cannot leak through. Temperature monitoring in direct proximity to the boiler, where the sensors are normally positioned, is far too slow in this type of scenario and heating is often very limited due to the quick gas flow, low energy content and large mass to be heated. Even if the sprinklers were to be triggered, for example, this does not affect the quantity of gas forced backwards.

Normal course of events

The consequence of gases being forced backwards over an "extended" period (several seconds) or in short pulsing sequences due to disruption is that the hot gases quickly heat smaller particles in the fuel and inside the fuel system. It is quite probable that red-hot particles will also be brought along with the gases from the boiler. The environment is normally inert initially, due to the fact that the gases have forced the air out of the system, which means that no fire or explosion is triggered at first. Rapid cooling of the gases creates an underpressure which draws air into the system again. The unburned gases, primarily CO, are ignited by the heated particles as soon as the concentration of gas/air is within flammability limits. This is likely the reason for the explosions' relative weakness in normal situations; combustion close to the flammability limits is slow, which results in a lower explosion effect. In some cases, however, the gas explosion is caused by dust inside the equipment and the fuel being swirled up, intensifying the explosion if the concentration is sufficient. This type of hybrid explosion has more serious consequences than pure gas explosions.

Fuel handling systems normally tolerate very limited pressure increases without parts rupturing or opening up, which means that the explosions appear to be very severe. Flames and pressure emitted can result in damage and/or injury and in the worst case result in dust being swirled up causing a secondary explosion, potentially with very serious consequences.

> "Fuel handling systems normally tolerate very limited pressure increases."

In most cases, explosions have occurred in facilities which have been in operation for a long time with no previous incidents. So what is causing these incidents?

Causes of overpressure and gas dispersion

Naturally, the causes vary, and it has in any case not been possible to identify them with full certainty. There are examples of cases where boiler house ventilation has been affected resulting in that the differential pressure between the building/fuel system and the boiler shifting, whereby regulation of the boiler no longer functions as normal. Problems with heavy agglomeration of the fluid bed have in one case been the probable root cause. However, the predominant root cause established has been design flaws in fuel infeed systems and shortcomings in the control of these systems. This phenomenon is found primarily in grate boilers/ovens where the infeed often consists of either a fuel chute with so-called "stoker screws" or hydraulic pushers with varying configurations of fuel volume as a buffer and a barrier adjacent to the pushers.

The flaws in the fuel systems' design often leads to uneven and unreliable fuel infeed and poor distribution of fuel across the grate. This is compensated through the regulation of combustion air and flue gas fan, which allows the boilers to function with no serious deviations but hardly optimal combustion. However, in certain operating conditions or during certain sequences, it is likely a close call in terms of the limit before the furnace– whether all of it or a small, localised section – which entails a risk of gases being forced backwards in the fuel system. The cause for the threshold being passed may for example be

- Changes in the fuel, new fuel or e.g., increased amounts of fine fractions, change in fraction distribution, change in moisture content, etc.
- Changes in control systems, reprogramming, changed parameters, adjustment of regulators, etc.
- Malfunctioning sensors or guard switchers
- Wear and tear on the fuel infeed equipment
- Malfunctions, insufficient monitoring of levels in the fuel buffer bin

Risk identification and Risk assessment

What can be made to get in control of the risks? How can the risks be managed?

Assessment of the risks associated with this type of incident requires an survey of the design of the fuel system in relation to which fuels are being handled. It is also necessary to review how the facility is controlled, as well as alarm threshold values and automatic functions in the event of deviations. Interviews should be conducted with operating personnel regarding previous deviations, "normal" problems and experiences. Based on this, it may be possible to identify weaknesses which could entail a risk of explosion and to assess the consequences of such an event.

Risk reduction measures

The first priority in reducing the risk of explosion should be to reduce the probability of unburned gases being forced backwards to any considerable extent. This may require concrete measures such as the rebuilding of fuel infeed equipment, installation of barriers, replacement of protection and sensors, etc. It may also entail the adjustment of alarm threshold values and the need to improve control of the fuel infeed and combustion.

If it is not possible to assess whether the risk level will be tolerable following implementation of these measures, consequence reducing measures such as installation of explosion protection components, venting, explosion suppression systems and audio/visual alarms to warn personnel may be necessary. ■

GÖRAN JANSSON
g.jansson@pob.se

ABOUT THE AUTHOR
Göran Jansson, is a risk consultant at P&B and has some 25 years' experience of risk management in the processing and manufacturing industry. In recent years, Göran has conducted a large number of explosion cause investigations after explosions and "backfires" in boiler fuel infeed systems. P&B is one of Sweden's oldest Fire and Risk consultancies.

If occasionally uses consultants to support its Risk Management Services in special and niche risk areas.
This article has earlier been published in Swedish in 2017 by P&B.

3D printed spare parts – a potential risk?

What are the risks associated with 3D printed spare parts?

3D printing has been around for quite a while already but only in recent years has the technology developed and expanded into various new industrial areas. Spare parts management is an important and complicated element of the maintenance programmes of industrial companies. Industrial machinery constitutes a long-term investment and may need to be maintained, repaired and updated for decades to come. Doing this cost effectively and reliably is a challenge.

3D printing

The Digital Spare Parts Project by Aalto University and the VTT Technical Research Centre of Finland show how digitalisation and 3D printing provide opportunities to industries to streamline their business processes. However, the many changes also mean there is a possibility of new risks.

The basic idea of 3D printing was invented as early as the 1980s. It is also known as "additive manufacturing" as 3 dimensional objects are produced by adding material layer by layer from a printer. The objects can be virtually any shape based on a digital data model. The technique is being applied to an increasingly broader range of areas from the production of spare parts, components, medical devices based on a patient's own measurements, clothing, toys and pharmaceuticals up to large building materials.

The technology has developed to support serious high-tech applications in the manufacturing industry, even in quality-critical industries like the automotive and aerospace industry. A digital file is created in computer-aided design (CAD) software and stored in a file format from which the 3D information can be sliced into hundreds or thousands of 2D layers. The printer understands the file and prints the slices as layers on top of each other and produces the three-dimensional object.

The materials used in 3D printing are mostly plastics, metals or ceramics. The chemical and physical characteristics of the materials and their bonds vary. The choice of materials has increased rapidly enabling ever wider applications. However, the amount and quality of materials suitable for processing through traditional manufacturing technologies such as forging and moulding are even greater.

Industrial spare parts

The maintenance of machinery requires systematic service and available spare parts. The Original Equipment Manufacturer (OEM) is the natural manufacturer and supplier of the parts. This means that production is centralised on site at the manufacturer. The client's urgent need to have a specific spare part at hand depends on the equipment and process. In just-in-time conditions, even the slightest error or unexpected incident may disrupt operations and delay the availability of a spare part, consequently jeopardising the continuity of the operation.

To manage the risk, plant operators need to strike a balance between their own warehouse carrying a range of spare parts and the manufacturer's ability to quickly supply the required parts. However, maintaining large spare part warehouses ties up capital and is counter-productive from a business perspective.

This is where the benefits of 3D printed parts enter the picture. They can be produced locally and quickly on site by the customer or on site by the maintenance service provider. Besides offering availability, the method also enables updated versions and other modifications. This requires, of course, the digital information for the design to be available.

Quality assurance

3D printing technology does not produce precisely similar materials to traditional methods. This does not mean that the spare parts wouldn't be as durable as the original parts. But it is important to adapt quality control to ensure the product is suitable for its purpose.

Typically, the parts will also need post-processing and there are numerous parameters that must be controlled to ensure quality. This is more challenging as there are currently no uniform quality-control procedures. The lack of standardisation and possible certification poses further challenges.

Supply chain

The more parties in the supply chain, the more contractual relationships. Managing supply chain risks may involve dealing with the OEMs and manufacturers of printers and suitable raw materials, digital modelling, software, testing equipment, etc.

Liability

The manufacturer and seller of a spare part is liable if the part is defective and causes injuries to personnel or damage to property. Between commercial enterprises the liability is based on the sales contract. In the contract, the parties agree on the product specifications, delivery and consequences of any breach of contract such as a defect. The Sale of Goods legislation complements the sales contracts with default regulations if something has not been specifically agreed. Usually, sellers are liable for direct damage without their own negligence and for consequential losses through negligence, but these can be freely agreed upon.

> "We see that spare parts management requires a complex balance between risks and costs."

When users of the part produce the part themselves, several liability issues arise. The user is the manufacturer so there is no seller. But what about the seller of a 3D printer? Again, it depends on the contract whether there is any liability. Very easily the damage caused by the products would be outside of the printer producer's contractual liability as indirect damage. A digital file may be developed in various ways from the original CAD file or by measuring or scanning the original part. There could be alternatives for the liable party. Other potential parties include the material manufacturers or sellers and the software providers. Contractual relationships form a wide and complex matrix. Quality control of the parts by the user may remain the essential safeguard against damage.

Liability for bodily injury caused by defective physical products is based on strict liability of the manufacturer according to Product Liability Law. This applies also to accidents caused by heavy machinery or their components at industrial sites. When producing parts through 3D printing, even this becomes complicated. Who the manufacturer is in the legal interpretation may be unclear.

IPRs, Cyber

There are risk issues that are not handled further here including the use of patents and other IPRs and cyber risks. Anything digital may be hacked one way or another.

Risk management

Spare parts are important to continuity of the operation. Their availability may dramatically impact downtime and risk of Business Interruption. Thus, an industrial company must have a sound risk management programme that addresses all factors that expose the company to machinery breakdowns and consequential business interruptions. This includes the management and supply of spare parts. The criticality of each part to the process should be assessed. Critical parts need to be available, which usually means they are stocked by the plant. This can be achieved through VED classification – Vital, Essential and Desirable. It is important for vital parts to be available even if they would be improbable to wear out like the consumable parts such as bearings.

We see that spare parts management requires a complex balance between risks and costs. The availability and delivery times vary. Besides these issues, risk management may include follow-up of indicators in the use of machinery that anticipates future risks, thus giving more time to arrange parts to become available when needed.

Liability issues mean that there may not be any liable party to claim damages from in the event that the spare part does not fulfil its function or breaks. Managing liabilities means assessing contractual relationships and using contractual terms and specifications systematically.

Business Interruption

Property insurance for an industrial policy holder covers accidental physical loss, destruction or damage to insured property, which was not intended by the insured or could not have been foreseen by the exercise of reasonable care and skill on the part of the insured. Insurance coverage also supports any well-maintained property when 3D printed spare parts are used. Naturally, there may be safety regulations or other requirements. However, in the standard terms, 3D printed parts do not receive special attention.

The same applies to Business Interruption insurance. The coverage is tied to the insured events covered by the Property insurance.

Liability

As explained in this article, liability relations may be complex when industries start producing their own spare parts. But whenever there is liability, liability insurance is valid. Product liability policies offer protection to the manufacturer if 3D printers or raw materials are defective and cause damage or injury. General liability policies offer protection, for example, in the event of errors during assembly.

Consultant's liability covered by Professional Indemnity insurance may cover design errors. ■

MATTI SJÖGREN
matti.sjogren@if.fi

The digital spare parts project

Risk Consulting magazine has interviewed senior scientist Sini Metsä-Kortelainen from VTT on the results of the digital spare parts project.

Sini Metsä-Kortelainen

You were part of the Digital Spare Parts project conducted by Aalto University and the VTT Technical Research Centre of Finland Ltd in conjunction with some industrial companies. Could you tell us about the project's targets and methods?
The main goals of the project were to create a business concept for digital spare parts and to lay the foundations for a functional ecosystem, analyse the current and future performance and competitiveness of spare parts manufactured using a 3D printing process, increase the efficiency and speed of spare parts production and distribution with the new operating model, and create a roadmap for digital spare parts. During the project we collected information on the current situation of the companies and their future prospects by organising one-on-one and group interviews, workshops, seminars, visits, international research scientist exchanges and surveys. In addition, many demonstration parts, which were original parts of companies participating in the project, were manufactured and analysed.

What are the essential developments in 3D printing technology that enable its increased use in industrial spare part production?
At the moment, there are certain issues that must be developed before a wider implementation of 3D printing in the manufacturing of spare parts can start. Technologically and economically-feasible 3D printable spare parts should be identified from spare parts libraries in a systematic way, and methods should be developed for automation of both order-delivery processes and the different phases of the manufacturing chain related to 3D printing.

The stages of development necessary for and directly linked to 3D printing technologies mainly relate to materials and the quality of the parts. It should be noted that 3D printing differs from traditional manufacturing methods and, for example, produces a unique microstructure and surface finish. Material selection for 3D printing is quite limited when compared to the materials available for traditional processes. Thus, the digitalisation of spare parts and their further manufacture utilising 3D printing may lead to the use of substitute materials. It is essential to gather more information on 3D printing materials, the effects of different post-treatments and compare the properties with traditional materials. In addition, quality-assurance methods, general rules for IPR protection, and methods for safe data storage and transportation must be developed.

What are the main benefits of 3D printing applied to industrial spare parts production?
The main benefits are making spare parts service businesses more efficient and achieving significant cost savings: availability of spare parts is improved, customisation of parts is enabled, delivery times will become shorter and the manufacturing of individual parts or small batches will become cost effective. In addition to manufacturing and warehousing or transportation costs, it is also important to be aware of the costs of downtime that can become so significant that the price of the spare part itself becomes insignificant. 3D printing enables new spare part concepts like smart spare parts: different kinds of small objects can be embedded into parts during the manufacturing phase. Smart spare parts are suitable for condition-based monitoring, tracing and part identification.

Did you identify or assess risks that stemmed from 3D printing methods in spare parts production?
In the project we did not focus on the risks but some risks were certainly brought up, especially in the company interviews and workshops. These risks were related to materials and quality, IPR, ownership of 3D models, data storage and transportation, lacking standards and certificates, different 3D printing processes and information flow between the different parties.

Do you consider that the risk management framework of this production method requires reassessment for industrial production equipment and machinery? What kind of changes are needed?
3D printing should be seen as a new supplementary manufacturing method alongside many conventional manufacturing methods. The materials and the processes related to 3D printing have not been extensively standardised but, in the future, the situation will be different, particularly in industrial 3D printing. The rules regarding digital data ownership and use must be formulated and included in the contracts between the OEM company and the 3D printing service provider, for example.

How widely used is 3D printing in production industries? Is the potential understood and are the industries already accustomed to using 3D?
3D printing technologies have attracted the interest of the manufacturing industry and the general public more than ever before. Many companies are currently evaluating the feasibility of adopting 3D printing technologies into their business, whereas some companies did this decades ago. The sale of 3D printed products and services has grown year on year and was close to USD 6.1 billion in 2016. It is expected that growth will accelerate and the size of the industry will be USD 26.2 billion by 2022 according to Wohlers report 2017.

Currently, 5% of company spare parts are suitable for conversion into digital spare parts and it is expected that the proportion of digital spare parts will increase to 10% in 2028. ■

MATTI SJÖGREN
matti.sjogren@if.fi

Microplastics – a global risk

Waste material being discharged into the environment through human activities is a common source of global risk. We depend on the environment. Recently, pollution resulting from plastic has been hotly debated. This is not a new problem – the plastic littering the oceans was noticed decades ago – but the focus has shifted to all the sources and waste degradation in the oceans and in other environments.

It is no longer a question of local pollution. The resulting microplastics are ubiquitous. Through major mechanisms of the globe such as rivers, ocean currents and winds, microplastic particles end up in the food chain. In recent studies they have been found in all kinds of bottled water, in spring water pumped from the ground, in fish and other animals and in the soil that produces our food. And it is not only waste that is spreading and disintegrating. Many products like cosmetics contain microbeads that are washed directly into drainage systems. This also includes the particles released from synthetic materials in ordinary washing machines.

It was estimated last year that the volume of microplastics added over a 12-month period to the farmlands of Europe would be between 63,000 and 430,000 tonnes.

The effects on wildlife, soil and on humans have been researched but this research is at an early stage. There is no direct evidence of the short- or long-term effects on human health. But there are many worrying signs indicating that microplastics are not supposed to be in the digestive organs of humans or animals. Microplastics cause clear changes in the functions of microbes, insects and other small animals and then continue through the food chain.

This is not a risk that can be directly addressed by individual companies or persons. The risk is systemic and is about the way we use plastics in products, packaging and for other use purposes. Globally, about 300 million tonnes of plastic is produced annually meaning that about 8% of oil production is used for this purpose. Most of it is discarded as waste. Plastic is a very stable material and will stay in the environment for centuries.

It is still difficult to say how the problem of plastic in the ocean will be addressed as there is controversy surrounding the most suitable approach. ■

MATTI SJÖGREN
matti.sjogren@if.fi

TRYM HAUGE
Risk Engineer, NO

JAMES MORRELL
Risk Engineer, UK

STEFAN RASMUSSEN
Risk Engineer, NO

Tech scams on the rise

Microsoft said that email scams, fake websites, illegitimate phone calls and malware are getting worse, according to Forbes Magazine. Microsoft said it received 153,000 reports in 2017 across 183 countries from customers that came in contact with scammers. This is up 24 percent from 2016. In December 2017, Microsoft received a report of a scammer emptying a bank account of €89,000 during a tech support scam in the Netherlands.

“Whenever a flood takes a major production plant by surprise, many jobs will be lost.”