OSI VOL. 16 ISSUE 1 | 2023

Offshore industry

Growing demand for low alloy steel solutions

OFFSHORE CONSTRUCTION

TU Delft Wind AI Lab

WIND TURBINES

By the industry, for the industry

WINDEUROPE COPENHAGEN

Image courtesy of Adobe Stock.

How to deal with cyber crime?

In the offshore industry, automation and digitalisation contribute to higher efficiency, sustainability, operability, and safety. However, there is a downside because the increasing digitalisation also entails a growing cyber security risk, which might ultimately also impact safety. This is of specific interest in times of geopolitical tensions.

ALL PHOTOS COURTESY OF SECURA UNLESS STATED OTHERWISE.

In order to prevent offshore assets to be a target of cyber crime, their owners should take appropriate security measures and security specialist Secura (a Bureau Veritas Company) can help companies in their efforts.

Digital security

"In the past two decades, the development of automation and digitalisation have been taking large steps in most productions processes", says Sjoerd Peerlkamp, Director Industrial Market Group at Secura. Secura acts as an independent, specialised security expert. The company helps organisations improve their cyber resilience from a people, process, and technology perspective. Secura is active in all sectors and has a specific group focusing on industrial companies including critical infrastructure and renewables.

The company provides security advice, testing, training, and certification services.

Mr Peerlkamp continues, "The end of this development is not in sight yet as in this digitalisation, artificial intelligence (AI), big data, and autonomy are becoming increasingly important, also in operational technology. This has many advantages for the industry, however it also offers a new opportunity for bad actors to intrude offshore assets. And although this intrusion is only virtual, damage can be serious and even impact daily life."

EU NIS 2 Directive

The fact that cyber crime is something to be taken seriously, is recognised by the European Parliament. As a result of this, the EU NIS2 Directive was approved and will come into effect in Q4 2024 in all member states. The NIS2 Directive is

the EU-wide legislation on cyber security. It provides legal measures to boost the overall level of cyber security in the EU. The EU original cyber security rules introduced in 2016 (NIS Directive) were updated by this NIS2 Directive. It modernised the existing legal framework to keep up with increased digitisation and an evolving cyber security threat landscape. By expanding the scope of the cyber security rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities, and the EU as a whole. The NIS2 Directive on measures for a high common level of cyber security across the Union provides legal measures to boost the overall level of cyber security in the EU. Businesses identified by the member states as operators of essential services (energy, transport, water, banking, financial market infrastructures, healthcare, and digital infrastructure) will have to take appropriate security measures and notify relevant national authorities of serious incidents. A new key aspect is that this also covers the supply chain of companies within scope. According to

Sjoerd Peerlkamp is Director Industrial Market Group at Secura.

"To keep assets hack-proof, it is also important for companies to know what measures their suppliers and (sub)contractors are taking to keep their products and processes secure"

Sjoerd Peerlkamp – Director Industrial Market Group at Secura.

Mr Peerlkamp, the EU NIS2 Directive certainly is a good step towards digital security in the energy industry. "However," he says, "the restriction (and power) of this Directive lies in the words 'appropriate security measures', as this can be interpreted in many ways. What exactly is appropriate? You can only determine this with appropriate risk assessments relevant for your specific company. If done well, this is a very powerful way. However, we also see that the competency for appropriate risk assessments is not widespread yet and it should include people, process, and technical aspects."

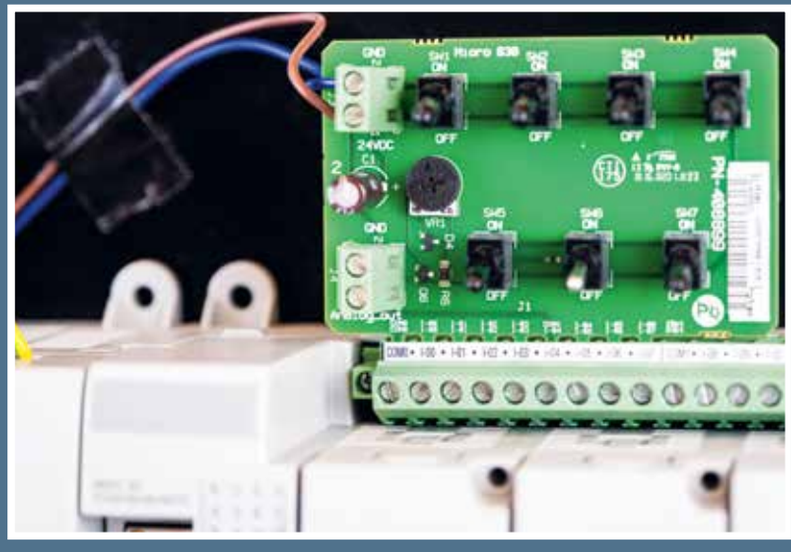
Reasons for hacking

Mr Peerlkamp continues, "When looking at the energy industry, several motives for threat actors can be described. First of all, criminals want to gain financial profit, for example by deploying ransomware. A recent example of this is the Vestas case in 2021. This company discovered a cyber security incident which involved external attackers gaining unauthorised access to some of their IT systems. During the attack, data was illegally retrieved and the attackers threatened to publish the stolen data. In this case, we assume that money was the main objective of the hackers. The result of being hacked was that Vestas had to shut down various IT-systems which had a negative impact on its operation." Another motive for hacking is geopolitical. "In the case of geopolitical reasons, hackers are trying to disrupt daily life as a form of digital warfare. For this purpose, hackers tend to take higher risks and put more efforts in the intrusion", Mr Peerlkamp elaborates. "The highly knitted European electricity network for example is a possible target. When intruded successfully, hackers can completely shut down the power supply by disrupting sufficient capacity. Taking the right measures is not easy because of the extensiveness of the network and the many parties and institutions involved to balance the grid. From grid operators, to production companies like offshore wind farms, to even domestic solar inverter manufacturers. If an attacker can control sufficient capacity at once, this could potentially result in a blackout. An important question in this matter is how to limit the effects of a potential breach. By isolating critical systems from commodity systems in the right way, the potential impact on your core business processes will be reduced for example."

IEC 62443

When looking at cyber security, governmental regulators are asking for more appropriate and fitting measures >>

Cybersecurity Demo kit used by Secura in for example, the two-day Operational Technology Cyber Security Fundamentals training.



and, according to Mr Peerlkamp, companies in the offshore industry also depend on suppliers and (sub) contractors for this. "To protect your assets, it is also important for companies to know what measures their suppliers and (sub) contractors are taking to keep their components and processes secure", Mr Peerlkamp says. "For this, certification according to the IEC 62443 standard can help as this is very extensive on product level as well as on system level. Secura can support companies in getting certified. The first step we take is to assess the current security maturity. The next step would then be a roadmap to improve the most relevant topics. We are a strong advocate of taking the right security measures already in the design or procurement phase of a product or system instead of taking measures afterwards. This way, you do not have to take additional measures in later stages. And with IEC 62443 certified components or systems, vendors can even differentiate themselves in the landscape where cyber security is becoming more and more important, like the offshore assets."

Offshore risks

According to Mr Peerlkamp, one of the biggest differences between working onshore and offshore is the remote operations of assets and how this influences cyber security. "When something wrong is noticed at an onshore asset," he voices, "it is easy for a technician to go to the location to see what is wrong and to take the right measures. You can also disable the remote programming mode on various types of devices as you hardly need it and can send an engineer on site in emergency situations. Offshore, this is very expensive and also more dangerous. This is why more and more offshore assets are monitored and fully operated remotely from onshore control centres. The more you can control remotely, the higher the risk and impact of a successful attack. When looking at cyber security, this is a potential risk which demands for higher security measures compared with onshore operations. Remote offshore operations also are dealing with limited network capacity which makes software updates and security monitoring more complex. Another risk in offshore operations lies in the fact that offshore assets are sold relatively often, which

One of the biggest differences between working onshore and offshore is the remote operations of assets and this influences cyber security.

Photo courtesy of Iberdrola.

requires integration and interconnecting different systems and vendors. In case of buying or renting an offshore asset, one should not only look at the technical condition but also at the state of the cyber security measures. cyber security should be part of the technical due diligence process."

Purdue model

Secura has ample knowledge in helping companies to be better protected against cyber crimes. "When looking at our customers' operations, we often use the so-called Purdue model from the IEC 62443 standard", Mr Peerlkamp explains. "This model was designed as a reference model for data flows in computer-integrated manufacturing (CIM), where a plant's processes are automated. It came to define the standard for building a network architecture in a way that supports OT (operations technology) security. The Purdue model is a structural model for industrial control system (ICS) security that concerns segmentation of physical processes, sensors, supervisory controls, operations, and logistics. For a long time, this has been regarded as a key framework for ICS network segmentation to protect operational technology (OT). Implemented correctly, it helps establish 'barriers' between ICS/OT and IT systems. There are also more specific measures to be applied to offshore wind. One of those measures is that wind turbines are no longer connected individually to the internet but connected to a central control room. Also, anomaly based security monitoring can help identifying potential security breaches. Among other things, it makes visible what has been changed, removed or added and if uncommon activities are taking place."

Threat Modeling

Another method used by Secura is Threat Modeling. "When securing an application, system or the complete chain, it is important to know from which perspective threats arise and how a system can be attacked by hackers", Mr Peerlkamp says. "Threat Modeling gives a complete picture of the threats and possible attack paths. During threat modelling, you not only look at the regular 'use cases', but also how an attacker could abuse this functionality. We call that the 'abuse cases'. So instead of thinking 'what should we be able to do', people should learn to think 'what do we not want the attacker to be able to do', which indeed is quite a change of mindset. These attack paths can subsequently be used for instance to create efficient penetration testing scenarios, design adjustments, or to define additional mitigating measures."

Security training

When looking at security, human behaviour is of course also an important aspect. Therefore, Secura organises various forms of training to stimulate secure behaviour. This ranges from very broad programs targeting secure behaviour across various employee groups to more technical and security specific training like a training on the IEC 62443 standard. "One of top-rated trainings is the OT Cyber Security Fundamentals training which is an eye opener for many engineers and asset owners. It even contains a small real industrial control environment where concepts like threat modelling and real-world attacks are applied during the training. All in all, we see that cyber security is getting more and more traction, at the legislators and regulators, as well as at the various companies we serve", Mr Peerlkamp states. "Digitisation unlocks a world of potential, but also introduces new risks. Cyber security became a board room topic and is a critical success factor for any digitised business. As part of Bureau Veritas, Secura is shaping a world of trust."

i. secura.com