digital energy journal

May - July 2024

Finding Petroleum

Official publication of Finding Petroleum

digital energy journal

Issue 107 May - July 2024

Digital Energy Journal
United House, North Road,
London, N7 9DP, UK
www.d-e-j.com
Tel +44 (0)208 150 5292

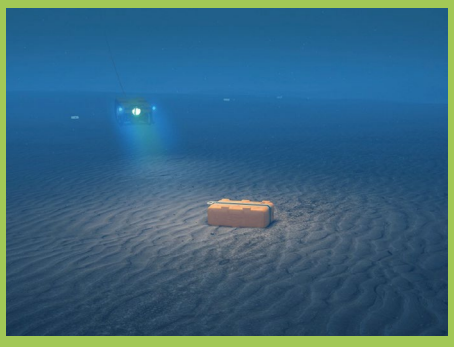
Editor and Publisher
Karl Jeffery
jeffery@d-e-j.com
Tel +44 208 150 5292

Advertising sales:
David Jeffries, Only Media Ltd
djeffries@onlymedia.co.uk
Tel +44 208 150 5293

Production
Very Vermilion Ltd.
www.veryvermilion.co.uk

Subscriptions:
£250 for personal subscription, £795 for corporate subscription.
E-mail: subs@d-e-j.com

Cover image: Viridien (formerly CGG) won a $20m contract to supply a Sercel GPR300 ocean bottom node seismic receivers for a "major customer" for a survey on the North Sea. These nodes feature QuietSeis MEMS technology, with "unprecedented" broadband signal sensing, fidelity and ultra quiet performance, surpassing conventional ocean bottom node equipment, Viridien said. It can work in water depths to 300m and is designed for easier deployment and retrieval.



Opening

AVEVA – building digital infrastructure for decarbonisation

Engineering software company AVEVA presented advice on how to build digital infrastructure to decarbonise an industrial company, based on real world use cases

Oil and gas companies and others should take a structured approach to setting up their "industrial information infrastructure" to support operational decisions for decarbonisation, alongside achieving other operational goals.

This was the lesson from a webinar from industrial software company AVEVA on April 24, "Use Cases in Strategic Alignment of a Decarbonization Strategy", presented by Craig Harclerode, industry principal for oil and gas, AVEVA

The webinar drew on presentations made by TotalEnergies staff at AVEVA events, including AVEVA World 2023 in San Francisco, and AVEVA World 2022 in Amsterdam.

Using templates to make it faster to set up digital infrastructure for specific pieces of equipment such as pumps is such a good idea it could be described as a "silver bullet," he said. It means you can set up a digital system much faster on the same type of equipment again, and the plan becomes "scalable".

Having good emissions data is the first step to finding ways to reduce them. "In my mind, what gets measured gets managed," he said.

The goal is to give tools to operational decision makers – so they can take emission factors into account alongside all the other factors when making decisions. This includes people operating equipment, process engineers and line managers.

You want digital systems which can help decision makers understand how the trade-offs work – such as how much a certain operational change will change emissions or cost, or if it may contribute to the company missing its targets.

If people have better tools to achieve targets, they will be more comfortable accepting accountability for achieving them, so more likely to work to reach them, he said.

You can make decarbonisation part of the organisational culture, and motivate people to think of innovative ways to reduce emissions.

Craig Harclerode, industry principal for oil and gas, AVEVA (screenshot from webinar)

Better tools mean that the company can make better forecasts about overall emissions and determine if the company targets will be reached. Emissions become 'manageable.'

There are many decisions to make relating to decarbonisation, including about improving efficiency, electrifying, and using decarbonised fuels.

You need to monitor whether you are making continuous improvement, and looking at the impact of the changes that you make.

To get good results, you should have integrated maintenance management, financial management, data analytics, emissions management tied together, and be able to see all the data on a single screen or "single pane of glass."

"What I find is, the devil is in the detail," he said. "It is about mapping this out, looking at data flows, looking at how a particular calculated variable is being calculated."

Basic structure

Mr Harclerode advocates building your digital infrastructure in layers, starting with data about individual 'tags' (pieces of equipment), rolling that up to provide data about assets (such as a furnace), then using that as a basis for predictive analytics and more.

"Crawl before you walk, walk before you run," he said. "I see too many companies trying to do higher level AI without this foundational capability."

The foundation of a system is the information infrastructure, the "master data management."

Once this is in place, you can build some level of "streaming analytics," or analytics being done on data as it is generated, at a "sub second" frequency, he said. This way, the analytics can support real time decision making, and help people be more proactive in identifying and fixing any problems.

You can build visualisation tools, showing raw and analysed data, to support people in their decision making. This includes front line managers and engineers who make day to day decisions.

Then you can add in advanced analytics or machine learning, he said.

Data can be shared with other companies in the value chain, who might be using your company's emissions data as part of their Scope 3 emissions calculations.

You are unlikely to have a single 'digital twin' but a number of digital twin elements which all have to be integrated and synchronised, he said.

To make a digital twin of an asset, you will probably first need to roll up your data from "tag" level (individual equipment) to asset level. "If you are still working in a tag-based ecosystem you're going to have a lot of trouble maintaining and driving a digital twin," he said.

Using the right tools

There have been many software companies offering software for managing emissions, some making big promises of how AI can help. Mr Harclerode warned that companies should be careful to check if such software "is fit for purpose in an industrial context."

When your main data input is time series data, such as from sensors, you need digital technology which can handle this, he said. Many emissions management tools are designed for other industries not working with sensor data.

You should also be careful about getting sidetracked by the promise of generative AI. Using it requires "solid, contextualised quality data," he said.

"If you're not putting a focus on master data management and getting your data house in order, generative AI and ML are going to be problematic for you.

Too high level

A common mistake companies make is looking at emissions only at too high a level, such as the emissions for a whole facility, rather than an individual part of it, Mr Harclerode said.

Many companies are trying to calculate the emissions in separate systems to their operational technology systems, having a separate environmental calculation engine. They also set high level goals of how much they want to reduce emissions by. They publish the data and targets in their corporate sustainability reports.

This arrangement means that the data is not 'operationalised' – it is not presented to people who are operating the equipment in a way that they can use it in all of the decisions that they make. "Doing this in a higher-level system is problematic."

The higher level system is also not directly running on operational data. This means the accuracy of the greenhouse gas data may be questionable.

It is difficult to transition from higher level emissions management to a more operational / granular level, he said. It involves, in effect, "decomposing" the calculations, or pushing the calculation to a lower point in the data stack.

Templates can really help with this, he said. "If you are using templates - this can be done very efficiently and effectively with pace," he said.

Templates

Templates are proving very useful in helping you build up digital infrastructure. You can make a template for how to gather data for a certain piece of equipment such as a pump, and then use it all over the company. "That is a silver bullet," he said.

The templates can be used to generate greenhouse gas data, energy efficiency data and asset performance data, and also do analytics and calculate KPIs.

The templates also cover 'events,' the ability to notify someone if something is going wrong.

The templates can work for a whole asset class. You can quite easily adapt the template for new equipment designs, and still be able to calculate emissions in a consistent way. So, it should not deter companies from buying new equipment.

The basic data entered into the template is the sensor 'historian' data, such as gathered by AVEVA's product PI.

It means that the company is gathering data consistently all over the world. The templates ensure data has consistent units of measure.

Templates can easily work with multiple measurements, where emissions are not measured directly but inferred from several other measurements. For example, emissions from flares might be inferred from the flowrate of gas to the flare.

Data visualisation

Once data is gathered in this harmonised way with the help of templates, data can easily be rolled up, such as for an asset, for a site and for a country.

Data can be visualised, with 'drill down' tools. It can be analysed.

You can compare energy efficiency of different asset classes. For example, you can see the emissions from one hundred flares, two hundred rotating machines, twenty pieces of fuel fired equipment, with different analytic calculations performed every minute.

Data can be viewed by country, block, or site. You can see the summary of all the equipment for a site, or for a certain asset or power generation train.

You can see which are your top greenhouse gas emitters in the company. The data can show where the 'bad actors' in your equipment fleet are, and which equipment did not achieve its planned emissions. You can see projections for the future.

You can drill down to see all the data for a specific piece of equipment in different ways, such as emissions per kwh from a generator. The operators of that specific equipment can set up alerts.

The data can be used to look deeper for opportunities to minimise and optimise energy efficiency and emissions.

For example, it was used to analyse whether the company was keeping an appropriate amount of power generation in reserve. The optimum amount of reserve ensures you get the system reliability and performance you need, without wasting fuel.

Another example was to look at redundancy in use of compressors. Companies keep more compressors than they need online in case of failure, but they might be able find a better balance of reliability, performance, and energy efficiency / emissions minimisation.

Data can be generated which show people where the trade-offs are (at what level changing one factor will lead to unsatisfactory levels of another).

TotalEnergies approach

TotalEnergies decided to develop templates for its various asset classes with the help of subject matter experts, which could then be used all over the company. They can be then adapted to the individual needs of specific sites.

TotalEnergies first developed templates for all asset classes which involve combustion, including heaters, furnaces, and flares. This meant it had covered 80 per cent of the greenhouse gases emitted in a typical manufacturing site.

TotalEnergies also made a template to understand chemical reactions at a molecular level, to work out the output of different greenhouse gases.

The company did not have a large dedicated team building the templates. They were built by the IT department, working together with subject matter experts who understood the various equipment types such as pumps, heat exchangers and furnaces, working part time on the project.. There were 3 or 4 experts in working with PI sensor data.

The role of the IT staff was making the systems work, such as networks and operating systems.

TotalEnergies developed 50 different displays to visualise emissions data, he said. Hyperlinks take the user from one screen to another.

Like most oil and gas companies, Total reports emissions for the whole company, and has decarbonisation targets, such as for reducing methane leaks, flaring, and the use of fuels in production.

Achieving this requires a well-understood baseline (starting point) and then a clear understanding of how much improvement is happening. You need to ensure calculations are consistent with regulatory norms and standard methodologies.

"I see Total as one of the leaders in the industry, how they treat information management, how they approach greenhouse gas determination, how they support their overarching strategy, he said.

Robin Sutherland - exploration in Southern Africa

Robin Sutherland, who is working with four different exploration companies in Southern Africa, gave an overview of exploration activities in Namibia, Zimbabwe, South Africa and elsewhere

South Africa is still subject to frequent power outages, which could be fixed if more gas was available. The power shortage is hampering mining operations, extracting materials being used to make solar panels, wind farms and batteries. So even if you are a fervent supporter of moving away from oil and gas, there are good reasons to continue exploration in Southern Africa.

Robin Sutherland, who is working with four different exploration companies in Southern Africa, gave an overview of activities, speaking at a Finding Petroleum webinar on Feb 9.

Robin Sutherland, who is working with four different exploration companies in Southern Africa (screenshot from webinar)

Mr Sutherland is former head of Tullow Oil's exploration team for Africa, where he led its well-known discoveries and field appraisals in Ghana,. These were the Jubilee, and the Tweneboa, Enyenra and Ntomme (TEN) fields.

Today he holds a number of roles including technical lead with Monitor Exploration of London, South African adviser to Searcher Seismic from Australia, non-executive director of ASX listed Invictus Energy, and chief operating officer with Anglo Eurasia Power Africa in Cape Town.

The region is attractive for explorers, with many countries prepared to offer attractive production sharing agreement (PSA) terms, without big work programme requirements in the initial phase. So, operators can have options rather than obligations, he said. Another benefit is that you can often find there isn't much competition for onshore licences.

Namibia

In Namibia, exploration is happening in the Owambo Basin in the North, which extends into Angola, and the Nama Basin in the centre.

The most active explorers in Namibia are Mr Sutherland's company Monitor Exploration Ltd (MEL) and ReconAfrica.

Other companies holding acreage in the Owambo Basin are Babecca, Exito, Elephant Oil and Apprentice, he said.

ReconAfrica started exploring the region expecting it to be a "pure Permian play. "That's not what it is. It has been interesting to see what it really is," he said.

Monitor Exploration is a UK privately held company operating solely in Namibia. Monitor holds 55 per cent of the "PEL 93" block in the Owambo Basin, size 18,500 km2.

In the Nama Basin, in the centre of the country, Monitor Exploration is about to sign a petroleum agreement with two blocks. "We've negotiated very favourable terms," he said.

A number of other areas around the country are "under application" for exploration licenses by other companies, but there hasn't been much movement since at least August 2023, he said.

Owambo Basin

The Owambo Basin region is on a rail line and has good roads and electricity transmission connections, while being far from "populated and wildlife areas", he said. "We have numerous potentially large hydrocarbon bearing structures."

An Australian operator 88 Energy Ltd is funding a 2D seismic program and will receive 20 per cent ownership in MEL's project in return.

MEL explores through its sister company Geodynamics Worldwide, which has the same majority shareholder. This company specialises in onshore exploration techniques other than conventional 2D and 3D seismic – so remote sensing, passive seismic, magnetotellurics and geochemical techniques.

The Owambo Basin is "not your normal tertiary cretaceous West African play," he said.

The reservoirs are formed in the neo-Proterozoic era (from 1000 to 538 million years ago).

It is not common for rocks of this age to have produced oil, but it has happened, with oilfields of this age in Oman and in the Szechuan basin of China, he said. "It's a bit more risky, because oil has to have stuck around for quite a while."

It is a very deep basin. There are a number of potential reservoirs. There are source rocks, some of which can be seen in outcrops.

There has been limited exploration to date due to a thick layer of sand above the reservoirs known as the Kalahari Formation.

There has already been a discovery in the basin (well Etosha 5-1A, drilled between 1965 and 1970 by the Etosha Petroleum Company, found a barrel of oil in the wellbore post suspension for operational reasons). ReconAfrica were exploring what they thought was a Permian (298mya to 251 mya) layer of the subsurface and drilled a well and "found hundreds of metres of oil shows," drilling through the base of the Permian and into the neo-Proterozoic section.

This was drilled as a stratigraphic well (only for understanding subsurface geology), on a site identified using aero gathered magnetic data.

You can see source rocks, reservoirs, seals, and structure, that formed about 550m years ago.

The first 700m of rock comes from the late Cretaceous, Jurassic, Triassic, and Permian. "Then we get to interesting stuff," he said.

There is black shale, which used to be thought Cambrian. "Recent work suggested this could be Silurian hot shale, seen all over North Africa, Europe and the Middle East," he said. "It's a very good source and seal."

Moving further down, there is the Damara, which is "good reservoir [rock]".

"The Etosha-5-1A well intersected this zone which flowed 1000 barrels a day of water on test without any stimulation," he said.

Further down, you come to tillites (large, detached rock bodies), and basinal shales, "which are good source rocks."

The well which found oil was linked to a carbonate source, which could only have come from here, he said.

There are two repeats of this, layers of shales followed by a layer of potential reservoir rock, "creating a perfect scenario," he said.

For exploration, the area has coverage of "very good quality" gravity and magnetics surveys taken by aeroplane, "which is a great start."

There have only been two 2D seismic surveys done, and they are quite old, done in 1969 and 1990. These have been used together to identify structures.

There has been one geochemistry survey, which found ethane concentration in the soil, with geochemical anomalies.

Passive seismic has been used. Monitor is looking at how passive seismic waves are impacted by hydrocarbon bearing reservoirs they pass through, modulating the frequency of the waves.

"It allows you to calculate probability of hydrocarbons at a specific point in the sur-

face," he said.

With this technique, Monitor has determined a high probability of hydrocarbons in some of the structures which have been mapped using gravity and seismic data.

Monitor is building on this with further 200km of 2D seismic surveys later in 2024. It has 3 areas of interest identified with the passive seismic.

One structure covers 144km2 area, so it could be a very large oil reserve if it contains hydrocarbons. Geochemical analysis of soil provides good support to the possibility of hydrocarbons, he said.

"If we were able to acquire thousands of kilometres of 2D seismic, we might get more definition on that."

Analysis shows that there could be "un-risked" recoverable oil of 7.6bn barrels, or 37.2 TCF.

There is some disruption to the data quality where there is shallow lava and layers of calcrete, he said.

"We're not exactly sure whether any hydrocarbons we find will be oil or gas. We think we've got a good chance of finding oil based on what Recon have seen. We will see," he said.

ReconAfrica has been exploring further Eastwards in the basin, and they have more seismic in their block. Some of it shows very clear imaging. There are some igneous intrusions in the area which "have some impact on reservoir quality."

ReconAfrica say they have 28 TCF of gas in place, or 2.3bn barrels of oil in place. They are planning a multi-well drilling program in the second quarter of 2024.

"We're very interested in the results because it has a direct impact on us [Monitor Exploration]," he said.

"We have a collaborative relationship with Recon. The new management are very realistic. They've got a believable story, and we wish them every success."

Nama basin

Monitor's block in the Nama Basin is on the edge of the basin, where there could be good source rock. There is a clear migration route where oil could have come from the central Nama basin.

There is not much coverage with seismic surveys. "It's a function of this enormous country and how much it would cost to cover everything in seismic," he said.

"We believe this has a very similar chance of success as the Owambo, but slightly different," he said. "It's a diversification of our risk."

The rocks have the same age, and there is evidence of a carbonate source rock from samples on the surface. There are multiple reservoir-seal pairs.

Southern Africa – interesting opportunities to develop gas production? (photo – Bigstock)

"We'll use the same exploration techniques to advance exploration - remote sensing, geo chem, passive seismic," he said.

Zimbabwe

Zimbabwe exploration began in the 60s, when Rhodesia (as it was called at the time) wanted its own source of oil to get around sanctions. There are two basins of interest, the Nama Basin (extending from Namibia into Zimbabwe) and the Zambezi basin. Both show oil seeps to the surface.

Oil producer Invictus has focussed on the Zambezi basin. It is Permian-Triassic, he said.

The background is that in the 1990s, oil producer Mobil used magnetic and gravity surveys taken by plane looking for minerals, to look for oil. There is a great deal of surveying for minerals in Africa.

Mobil found a very deep basin. They acquired a 2D survey to better understand the depth of the basement and the sediments and other rock layers.

They concluded that the Zambezi basin was best, with an enormous anticlinal structure in the middle, and two highs within the block. But they also thought it was likely to be gas, which they did not see a route to market for, and they were not comfortable with the Mugabe government, so decided to exit.

Invictus Energy picked it up in 2018, and they have a license covering the Cabora Bassa Basin in northern Zimbabwe. (Mr Sutherland is a non-executive director of Invictus Energy). They drilled two wells, named Mukuyu 1 and 2.

Mukuyu 1, was a gas discovery, but the company was unable to take a sample due to tool failures. Under Australian Securities Exchange (ASX) rules, it cannot be announced as a discovery.

The Mukuyu 2 well is 6.8km away on the same structure, and led to the Upper Angwa discovery, 450m up dip from the point in the reservoir intersected by Mukuyu 1. It was possible to obtain samples.

An announcement was made of 35m of pay. "It doesn't sound huge, but it's within a very large structure, which is not too common in this part of the world," he said.

The drilling also found a deeper overpressure interval, which could be explored further later.

There are also plans for a 3D survey and other drilling projects.

Invictus is targeting a number of other closures which were found on the Mobil data. One of them shows a 10km long velocity 'flat spot' on the seismic, "something we thought was very much worth following up."

South Africa

In South Africa, there have been some methane and helium discoveries in the Wits Basin.

A company called Renergen has explored further, finding methane and helium from deep sources. "We knew there was an old petroleum system but didn't believe you could make something of it," he said.

Renergen has stated proven and probable (2P) reserves of 407 BCF of methane, but also 13.6 BCF of helium, which is "many times more valuable."

There was a meteor impact in South Africa 2bn years ago, with the impact structure known as the Vredefort Dome. This stopped further development of the basin.

Kinetiko Energy is exploring for methane in the Karoo basin, looking at coal bed methane and "muddy source rocks" in that zone. The reservoir is clastic rock sealed by shale, "so essentially a conventional gas development."

Kinetiko is working in a region where there is a great deal of coal power generation, close to

Sasol's Secunda plant. This has been described as the world's biggest single CO2 emitter, with 57m tonnes CO2 a year. The coal is turned to liquid fuels.

The plant operators would prefer to run on gas, and the plant becoming a gas to liquids plant. This would save them money since there is a carbon tax in South Africa. "Let's hope Kinetiko can produce it," he said.

Independent auditors have assessed 6 TCF of recoverable gas, at depths of just 150m to 700m underground.

"There are wells that have been blowing out for 40 years and have not depleted," he said.

Rhino Resources is also exploring in the region and doing environmental impact assessments (EIAs) for future drilling activities. Two other active companies are Bastion Oil and gas and an associated company Bulwark Energy. "So, a massive amount going on."

Other areas

In Angola there has been a "revitalisation", with the government agency Agência Nacional de Petróleo (ANPG) "doing a good job of licensing acreage, attracting people with improved terms and an open attitude," he said. "There's been blocks awarded and there's an ongoing round."

In Zambia, a local company GeoPetroleum is exploring the Mweru basin, it is also interested in helium.

In Tanzania, a company called Helium One is looking in the Rukwa graben.

"They recently announced they found helium and hydrogen," he said. "I find it incredible you can find hydrogen in the subsurface."

Also in Tanzania, ARA Petroleum and Aminex are working on development in the Ruvuma Basin, and there is some exploration going on.

In Mozambique, SASOL had a discovery last year in the Bonito formation.

"There's a lot going on in a fairly large area."

Energy shortage

Many areas of Southern Africa have a deficit of power generation, and a new supply of gas could help fix that. Mr Sutherland noted that in his home in Cape Town, South Africa, power was about to be shut off for two hours, and the following day there will be no power for 6 hours.

It is known as 'load shedding', taking demand away from the grid by switching people's power off. For people in the region, "it is a fact of life", since 2007.

The load shedding was worse in 2023, when it was common to have power outages of 12 hours. It impacts industry as well as homes, such as with mines unable to operate. "It's having a huge impact on South Africa's economy," he said.

Many mines are building their own solar plants – some as big as 150 MW. But batteries are normally too expensive, so there is still no power when the sun is not shining.

Mr Sutherland has a solar generation system on his own house and sells excess energy to the grid. He would prefer to store it with his own batteries to provide power during the outages but finds batteries too expensive. "Battery economics are difficult," he said.

digital energy journal

This report is based on the Finding Petroleum webinar on Feb 9 2024, "Explore onshore Southern Africa - not just deep, deep, water!"

To watch the video online, go to **www.findingpetroleum.com** then navigate to events / past events / Feb 9 2024 event

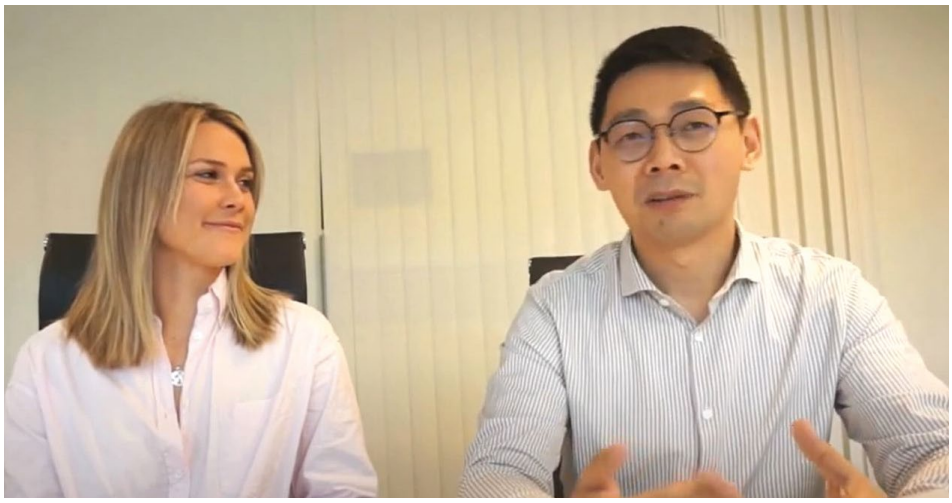
eDrilling's plans for autonomous drilling

Drilling software company eDrilling is developing an AI tool to support the drilling process and decisions in incremental steps, leading to autonomous drilling. CTO Jie Cao explained the steps it is taking

Drilling software company eDrilling of Stavanger is developing an AI tool to support drillers, which will progressively be able to do more and more to support the drilling process.

The long term goal is that this tool will find the most efficient and safe way to drill the well to its final depth, predict incidents and hazards, optimise parameters, and automate complex and repetitive tasks. So it will be full autonomous drilling.

In doing this, it could identify ways to reduce the costs of drilling the well, something which might be particularly useful in geothermal wells when finances are more constrained.



Jie Cao, CTO of eDrilling (right) explains the company's "Wingman" AI concept with Caroline Vorpenes, chief growth officer of eDrilling (left). You can see the discussion on YouTube by searching for "The future of drilling with AI: interview to eDrilling's CTO, Jie Cao"

Levels of AI

An AI can support or make decisions at a number of different levels.

The initial stage can be termed the "passive" stage, where we do not have any AI, said Jie Cao, chief technology officer of eDrilling. Decisions can only be made by human experts, or with trial and error. Digital tools are for collecting data and making calculations.

The next stage is "reactive", where we have digital systems which react to what is going on, such as identifying problems happening and sending alerts to operators. This can be termed the "expert system".

The third stage is 'proactive', where the machine tries to predict what might be about to go wrong. Drilling operations have predictive models. The software is looking 'ahead of the bit' to see what you might be about to drill into or see potential risk before it happens. This could be termed "automated advisory".

The fourth stage is where you could have an AI "agent" actually making decisions, in a fully adaptive and self-optimising system. It can make decisions about optimising operations, reducing possible risks and reducing downtime. "You can have a very general and improvised system to help you make the best decision," Mr Cao said.

What AI should do

An AI agent could be thought of as a tool able to give advice like Chat GPT. But to provide drilling advice, it could not base its data on language models, as Chat GPT does

eDrilling started a project called 'Wingman', to develop such a tool. It first wanted to use the name "CoPilot", but it has since become widely used by Microsoft.

A good 'wingman' would know the fundamentals of drilling, and know about previous drilling activities, so be able to help you with the process. It should know where you are now and what you are going to do next, and what the consequences of this might be, Mr Cao said.

The 'wingman' should be aware of drilling limitations, such as limits of the rig and the formation, and stop you going over red lines.

The wingman could detect emerging risks and warn you about them.

A superintendent managing a number of drilling rigs could also have a wingman, giving advice about any wells needing particular attention.

The wingman would look at all of the decisions you have to make, not just support one aspect of drilling.

"We believe it is highly possible - or definitely feasible," he said. "These technologies have been verified in other industries."

eDrilling started Wingman as a live project at the end of 2023.

Steps of building

The first step of building it will be to develop an AI "agent" which can practise drilling, learning with existing drilling simulator software, which is used for training drilling engineers and testing well designs.

This simulator can run on both real, historical drilling data, and simulated data. The agent will be able to learn the fundamentals of drilling, what the sequence of steps are.

eDrilling will use its own wellSIM simulation software for this.

The second step is to train the agent on a 'drilling digital twin', a digital version of the current project (so like a simulator but which reflects current reality).

The agent can explore options and determine the best move, using real data in the same way as it uses a simulator, so it is learning from real life.

eDrilling already has a digital twin technology.

The third step is to improve the agent's ability to learn, including with deep learning and reinforcement learning. It means finding the best algorithms.

The AI drilling agent will be deployed to work together with drilling engineers, to see if it can identify hazards. "This phase might take some time," he said.

Ideally people from multiple companies and multiple stages of the drilling process would be able to work with the drilling agent.

The fourth stage is where it can be introduced to market as a tool to help drillers.

"These components are essential to an AI drilling agent," Mr Cao said.

"We believe eDrilling is in pole position to develop that."

One of the biggest challenges will be getting people to trust the agent, he said. This may be easier to achieve if people have been in-

volved in the agent development.

And the technology itself will be a major challenge, combining machine learning algorithms with physics-based modelling. Engineers will want to 'reason' with the AI's suggestions, with their own physics-based models.

"That's what we need to do, that's not easy at all," he said.

"We want to have collaboration with research institutes, academia, universities, to work out how to incorporate this hybrid methodology to test the new AI algorithms, the reinforcement learning algorithm."

Background

eDrilling is based in Stavanger, Norway, and makes software tools to support drilling operations, mainly in oil and gas. It makes tools for planning wells, simulating drilling, monitoring drilling, keeping drilling within operational limits, doing managed pressure drilling and dynamic well control. So, all about helping drilling engineers to make better decisions

eDrilling has been using model-based reasoning since 2008, where you make a model of the physical world to try to work out what is happening. This was used to diagnose any problems while drilling is going on and send out alerts.

It has also been developing supervised machine learning (which aims to find patterns in labelled data), to support drilling operations. It has tackled classification problems (where a machine aims to 'classify' what it is seeing), and 'prediction problems' (where the machine tries to predict what will happen).

"The AI Drilling Agent project is the biggest science and engineering effort we've undertaken as a company," says Toni Fadnes, eDrilling's CEO. "We have always demonstrated leadership in AI R&D and developing an everyday companion to engineers and crew members will make AI real and relevant for our industry globally."

Energy cyberattacks are getting worse

Cyberattacks on energy companies around the world are increasing, hackers are getting more competent, and consequently attacks are getting more expensive. ICIS experts present the current picture, with sobering stories from Denmark, Germany, Ukraine and the US. *By Aura Sabadus, energy and cross-commodity expert, and Rob Dalton, senior market reporter, Independent Commodity Intelligence Services (ICIS)*

Recent surveys indicate a 97 per cent rise in cyber threats across various industries, including energy, since Russia's 2022 invasion of Ukraine.

Energy companies are redirecting funds from new projects to enhance cyber defences.

Geopolitical tensions, notably Russia's invasion of Ukraine, have spurred state-sponsored actors from countries like China and Russia to engage in cyber espionage and disrupt critical infrastructure.

In North America, 20% of cyber-attacks target the energy sector, according to IBM. Recently, the US CISA (Cybersecurity and Infrastructure Security Agency) warned of Chinese plans to target American energy infrastructure amid heightened tensions.

According to IBM, energy companies in the UK face significant threats as large oil and gas supermajors are headquartered there.

Meanwhile, Ukraine has been the victim of relentless attacks in cyberspace. In an interview with ICIS, one company based in the country said it had witnessed at least 27 million attacks in 2023, including denial of service (DOS) designed to jam the system's normal functioning.

Despite the increasing threat level, many companies hesitate to disclose incidents, fearing reputational damage.

Last November, Leonhard Birnbaum, CEO of E.ON, one of Europe's largest utilities, said 'crooks were becoming better by the day' amid fears Europe's energy infrastructure was being flooded with thousands of cyber-attacks.

Danish attack

SektorCERT, a non-profit organisation owned and funded by Danish critical infrastructure companies, revealed how 22 energy companies based in the country were the victims of a targeted, coordinated attack in May 2023.

As a result of the attacks, the perpetrators gained access to some of the companies' industrial control systems and several companies had to go into 'island mode' operation.

Although Denmark appears to be one of the EU countries that has been under constant attack in recent years, one unusual aspect of last year's incident was that attackers knew in advance who they were going to target and got it right every time, according to SektorCERT.

During the attacks, hackers exploited multiple vulnerabilities in firewalls for initial access, gaining complete control over the impacted systems.

The cybersecurity organisation said that, at least in one of the attacks, it observed activity associated with Sandworm, a Russian state-sponsored actor linked to the Russian military intelligence services.

Germany

A few months later, in November 2023, the German Energy Agency, dena, said its servers had been targeted by cybercriminals who "greatly compromised" its technological capacity to work, making the organisation unreachable by phone or e-mail.

Subsequent reports indicated the agency had been the victim of the ransomware group BlackCat, which threatened to publish the stolen data on the dark web if ransom demands were not met.

An international group of investigators neutralised BlackCat's websites. Shortly afterwards. LockBit, another cybercriminal group, threatened to publish the stolen information.

The stolen data was indeed published on the dark web, prompting dena to call various service providers to analyse the incident and set up protective mechanisms.

Subsequently, the UK's National Crime Agency and international partners reported that they infiltrated LockBit's network and compromised its criminal enterprise.

US and pre-positioning

The US government made an announcement in February 2024 regarding Chinese state-sponsored actors. They are, the announcement said, seeking to "pre-position themselves" on IT networks for disruptive and destructive cyberattacks against critical infrastructure in the event of a crisis or conflict between the US and China.

The Cybersecurity and Infrastructure Agency (CISA), the National Security Agency (NSA) and the Federal Bureau of Investigation (FBI) said critical infrastructure organisations, including in the energy sector, may have been compromised by the Chinese state-sponsored cyber group known as Volt Typhoon.

The agencies pointed out that related infrastructure in Canada or non-continental US territories may also have been affected.

In its February 2024 advisory note, CISA said Volt Typhoon's choice of targets and behaviour was not consistent with traditional cyber espionage or gathering intelligence operations but was pushing a step further. Actors were pre-positioning themselves on IT systems to create disruptions at later dates.

"The US authoring agencies are concerned about the potential for these actors to use their network access for disruptive effects in the event of potential geopolitical tensions and/or military conflicts," CISA said.

The agency added that the use of 'living off the land techniques', such as those used by the Volt Typhoon group, had maintained a foothold in victim IT systems for at least five years, conducting pre-exploitation reconnaissance to learn about the target organisation and its environment.

The larger utilities and operators of the US federal backbone infrastructure have invested significant sums of money to protect themselves.

But a source at the US CISA told ICS there are still many vulnerabilities in the system. These can be linked to smaller companies which cannot afford to recruit or pay highly skilled IT staff. Also linked to the complexity of the energy infrastructure itself, as new devices such as electric vehicles, solar panels, or wind turbines plug into the grid, providing multiple entry points for cybercriminals.

Ukraine

Although all companies involved in strategic sectors or operating critical infrastructure are vulnerable to cyber threats, Ukrainian-based outfits may have had the biggest share of attacks over the last ten years when Russia first invaded the country.

In 2015, more than 200,000 consumers were plunged into darkness for several hours after the power grid in two western regions was hacked.

Within months of Russia's full-scale invasion on 24 February 2022, the grid was targeted once again by 'living off the land techniques.' These tripped substation circuit breakers, causing unplanned outages, that coincided with mass missile strikes on critical infrastructure across the entire country.

One company said the attacks on its own systems nearly tripled from 10 million before February 2022 to 27 million in 2023.

Preparations put in place prior to the start of the full-scale invasion helped companies be more resilient even as cyberthreats intensified, according to a source at a company that provides IT assistance and 24-hour monitoring to several outfits in the Ukrainian energy sector.

"If you want peace, prepare for war," the Ukrainian IT source said, stressing the importance of knowing the risks and implementing safeguards.

"The lessons Western companies can learn from Ukrainian counterparts should be straightforward. Migrate critical corporate services to cloud services. Distribute services across different data centres and establish your own 24-hour monitoring cyber security centre."

"Your cyber defences are your frontline defences. You never know how and when the attack will come to your company or country."

State sponsorship

Sources interviewed by ICIS in the government or private sector agreed that the majority of threats witnessed in the energy sector come from state-sponsored actors, and these may be based in Russia, China, Iran, North Korea or Pakistan.

"In Russia's case, you have 17 individual rogue cyber groups all faced West," said Stuart Poole-Robb, Group CEO of The KCS Group Europe Ltd, a London headquartered strategic intelligence and risk management consultancy.

"There are 26 units, which have a range of services from state-initiated cyber-attacks, propaganda or chemical warfare," he said. The groups emerged from a special unit established in the late 1980s and reportedly responsible for psychological operations.

These state-sponsored groups are often connected to Russian mafia groups, sometimes operating from countries such as Poland, Ukraine, Romania, the UK, or the US. They are not necessarily concerned about the type of companies they were targeting but more about their numbers, Mr Poole-Robb said.

"The units have grown from the 1980s to what we see today," he said. "They target a variety of sectors, such as the legal sector, pharma, hi-tech, energy, and finance. They are looking for inside information that they can use and abuse."

Distributed grids

Many power companies are building more distributed grids, which would ensure that attacks remain localised rather than spread out to the entire ecosystem.

"There are pros and cons for distributed energy," the CISA specialist said. "The risks are more spread around, and if something goes down, there are other units for backup."

"However, how much do you rely on renewables for a cold start of the grid? There are open questions there."

He said CISA recommends greater segmentation of energy systems to ensure attacks remain localised. But challenges will persist as long as systems continue to rely on older operational technology, which is more expensive and difficult to upgrade.

Cybersecurity needs more than compliance - AspenTech

With cybersecurity, energy companies should do continuous risk assessment, systems monitoring, and have 'proactive defence', as well as complying with regulations, says AspenTech. *By Benjamin Beberness, Vice President, Industry Business Units, AspenTech*

Compliance should be seen as the beginning of cybersecurity efforts, not the endpoint.

While regulatory compliance is a crucial step in safeguarding against cyber threats, it is not sufficient on its own.

The energy sectors must embrace a comprehensive cybersecurity strategy that includes ongoing risk assessment, embracing technological advancements, and fostering a culture of transparency and proactive defence.

This proactive and comprehensive approach to cybersecurity will not only protect critical infrastructure but also ensure the reliability and resilience of our energy systems in the face of ever-evolving cyber threats.

It is imperative for the industry to not only defend against the cyber threats of today but also prepare for the complexities of tomorrow.

The fundamental limitation of compliance as a cybersecurity strategy is its static nature. Regulations are designed to provide baseline security standards. But hackers are continuously advancing their methods.

As a result, a compliance-only approach can lead to a false sense of security among enterprises, where ticking off regulatory checkboxes might be prioritised over implementing robust, dynamic defence mechanisms.

A strategic approach to cybersecurity involves not just defence but also preparation for potential breaches.

By incorporating these practices, energy companies can make cybersecurity a seamless part of their operational framework, enhancing both their efficiency and security posture.

Solutions

Energy firms can benefit from adopting solutions that tightly integrate cybersecurity features with operational technology systems. This might involve using software that provides both operational insights and security data, giving a holistic view of both performance and threat status.

Advanced solutions, such as artificial intelligence and machine learning, can predict and mitigate cyber risks by continuously adapting to new threats.

Real-time monitoring systems that use predictive analytics to identify potential threats before they manifest are especially beneficial. This can involve the integration of machine learning models that predict and detect anomalies in system behaviour, which could indicate a cybersecurity threat.

Benjamin Beberness, Vice President, Industry Business Units, AspenTech

Digital twin technology could be used for cybersecurity by simulating cyber-attacks in a controlled virtual environment. This allows for the testing of potential vulnerabilities and the assessment of the impact of various cyber threats on virtual models of physical systems without risking actual operations.

Using cloud technology for non-operational systems adds an extra layer of security. For example, implementing redundant systems in the cloud enables utilities to reduce downtime during and after a cyberattack.

Methods

The energy sector should adopt a proactive approach that integrates cybersecurity into the fabric of its operations from the outset. This is likely to involve a continuous process of risk assessment, updating and testing defences, and training personnel to respond effectively to incidents.

Organisations should develop and implement a framework for regular assessments of cybersecurity risks as part of the operational process. This framework would also include guidelines for updating and maintaining security measures in response to these assessments.

Working with third parties to test cyber-defences can provide insights that can be critical not only for improving the security posture but also for demonstrating the commitment to cybersecurity to stakeholders.

Energy companies often engage ethical hackers or white hat hackers to simulate controlled attacks. These simulations frequently uncover critical vulnerabilities that may not be addressed by existing regulatory frameworks.

For staff, most energy companies require regular, mandatory training programmes that focus on cybersecurity awareness and procedures. This training could be integrated with the implementation of their systems, ensuring that employees are knowledgeable about both operational and security features.

Establishing a secure programme for the industry to exchange information on cybersecurity practices and cyber incidents would be highly beneficial. Companies can use this to strengthen their own cybersecurity initiatives.

digital energy journal

Data principles suggested for UK offshore industry

A UK task force has proposed six data principles UK offshore industry should follow, to share data, increase data value, develop targeted solutions, share data models, develop data repositories and collaborate

The Data Principles Group, a task force set up by the Offshore Energy Digital Strategy Group, has proposed six data principles the UK offshore energy could follow, based around data sharing.

Briefly put, the principles are that companies will share data, increase data value, develop targeted solutions, share data models, develop data repositories and collaborate with data.

The aim is that by following the principles, UK oil and gas companies and others involved in offshore industry will be able to improve efficiency and reduce emissions, with decision makers having access to better data.

They will be able to develop more accurate and robust predictive models.

It will ultimately lead to a "digital integrated offshore energy system."

There will be quicker resolution of problems, and more high quality data will be available for AI.

UK offshore companies will be asked to commit to the principles.

The members of the Data Principles Group are David Lecore of North Sea Transition Authority (NSTA); Kurt Prendergast of Kellas; George Rorie, Shell; Dave Simpson, DNV; John Mitchell, The Crown Estate; Steve Johnson, Petrofac; Liam Bennett, OFGEM; Dimitrios Pezaros, University of Glasgow; Ian Lawrence, Storegga; Ed Evans, ODI; Robert Swiergon, NSTA

"By adopting these principles and actively participating in collaborative data initiatives, organisations can contribute to industry-wide advancements, and position themselves as socially responsible and innovative participants in the energy transition," said Ed Evans, Data Principles Group Chair and Senior Consultant at the Open Data Institute (ODI).

"This will enable the UK to take the lead in achieving Net Zero, a significant aim for the ODI and many of our partners, funders and wider network."

The principles

The first principle is that the company commits to "actively sharing data," collaborating with other companies on initiatives which lead to more efficient operations, reduced emissions and sustainable practises.

The second principle is that the company will increase the 'value' of its internal and external data. For example, by applying AI, data science and robotics on the data sets.

The third principle is that companies will collaborate in developing "targeted solutions" seeking to solve specific problems. By working together they can avoid duplication of effort.

The fourth principle is that companies will share data and data models. These can be used to provide visibility of infrastructure, logistical options, the subsurface, and other aspects of the natural environment.

The fifth principle is that companies will facilitate accessible, secure data repositories for all stakeholders who are using it. The data sets will be "stewarded, trusted, secure, standardised and accessible."

The sixth principle is that companies will seek to improve their operational efficiency and reduce their risks through data collaboration. They will integrate this shared data into their decision making processes.

About Data Principles Group

The Data Principles Group is a "task group" set up by the UK Offshore Energy Digital Strategy Group. It held its first meeting in July 2023.

Organisations in this group include Crown Estate Scotland, The Marine Management Organisation (a public body), the Marine Scotland Directorate of the Scottish Government, North Sea Transition Authority (NSTA), Ofgem, The Crown Estate, the Net Zero Technology Centre (NZTC), Offshore Energies UK (OEUK), the Technology Leadership Board (TLB), and Renewable UK (RUK).

The Digital Strategy Group was set up to implement recommendations of the Digitalising Offshore Energy Systems report, published by Energy Systems Catapult in 2022.

There are two other task groups. The "Delivering a Common Data Toolkit Task Group" will consider establishing a common data toolkit to facilitate controlled and automated data sharing across the sector. The "Driving Cross-Sector Digitalisation Task Group" will look at co-ordinating digitalisation efforts to enable efficient investment and capture cross-sector requirements.

Time for some data principles for offshore energy?

Emerson's "boundless automation" vision

Automation company Emerson presented a vision for a "boundless" automation system, with devices, edge computing and cloud systems connected with a holistic data "fabric"

Automation company Emerson has developed a "Boundless Automation" vision for a future industrial automation digital architecture connected together by software. It was presented first at its Emerson Exchange EMEA 2024 user event in Düsseldorf, Germany, in February 2024.

It involves a holistic 'cohesive' software ecosystem, connecting the field devices, the edge (on-site) computing, and integrating data on the cloud, making all data instantly accessible and ready for analytics.

All of the devices in an industrial site would be integrated into the system. So, there would no longer be a situation where different devices are put in place by different departments, such as for reliability, safety and sustainability, and their data is all kept separate,

Many digital transformation projects have encountered data which is difficult to integrate and lacking in context, and held in silos, Emerson says. It means that it is very difficult to deploy AI and machine learning tools. Siloed plant data goes on to become siloed cloud data if it is not transformed.

"Boundless automation" means that the cloud, edge and field are all connected together by software. All the data pipelines are integrated together. Software can be deployed anywhere in the field from a remote location.

It means that the automation system is far more software driven. It replaces the current set-up which is geared more around hardware expenditure, and where the work is mainly administering devices.

It will become much easier to make data available to whichever people or systems need it.

With a more software driven system, it is easier to develop better cybersecurity systems. For example, all access can be 'zero trust', where access is provided based on identity, context and data required, and it can be made very granular. There can be much less uncertainty in a decision of whether access should be granted or not.

For field devices, there can be new sensor types, wireless communications making deployment easier, multiple communications options available, analytics within the devices, and standardised data models. It is possible to manage a group of devices together as a 'fleet'.

"After decades of implementing evolving automation strategies, manufacturers recognize the need to extract greater value from data that is locked in a rigid and now outdated automation architecture," said Emerson President and CEO Lal Karsanbhai.

DeltaV Edge Environment

In an associated development, Emerson announced in February that it was launching the "DeltaV Edge Environment".

DeltaV is Emerson's distributed control system, or 'automation platform'.

The "Edge Environment" is a digital 'workplace' where people can develop tools for data manipulation and analysis, even AI, running close to the data source, connecting directly to the automation system data.

This can have benefits compared to the usual method of sending all of the control system data to the cloud and then doing analytics over cloud software. Users know that the data they are working with is always complete, up to date, and fully reflective of the actual operating condition.

It may mean that it is possible to do much

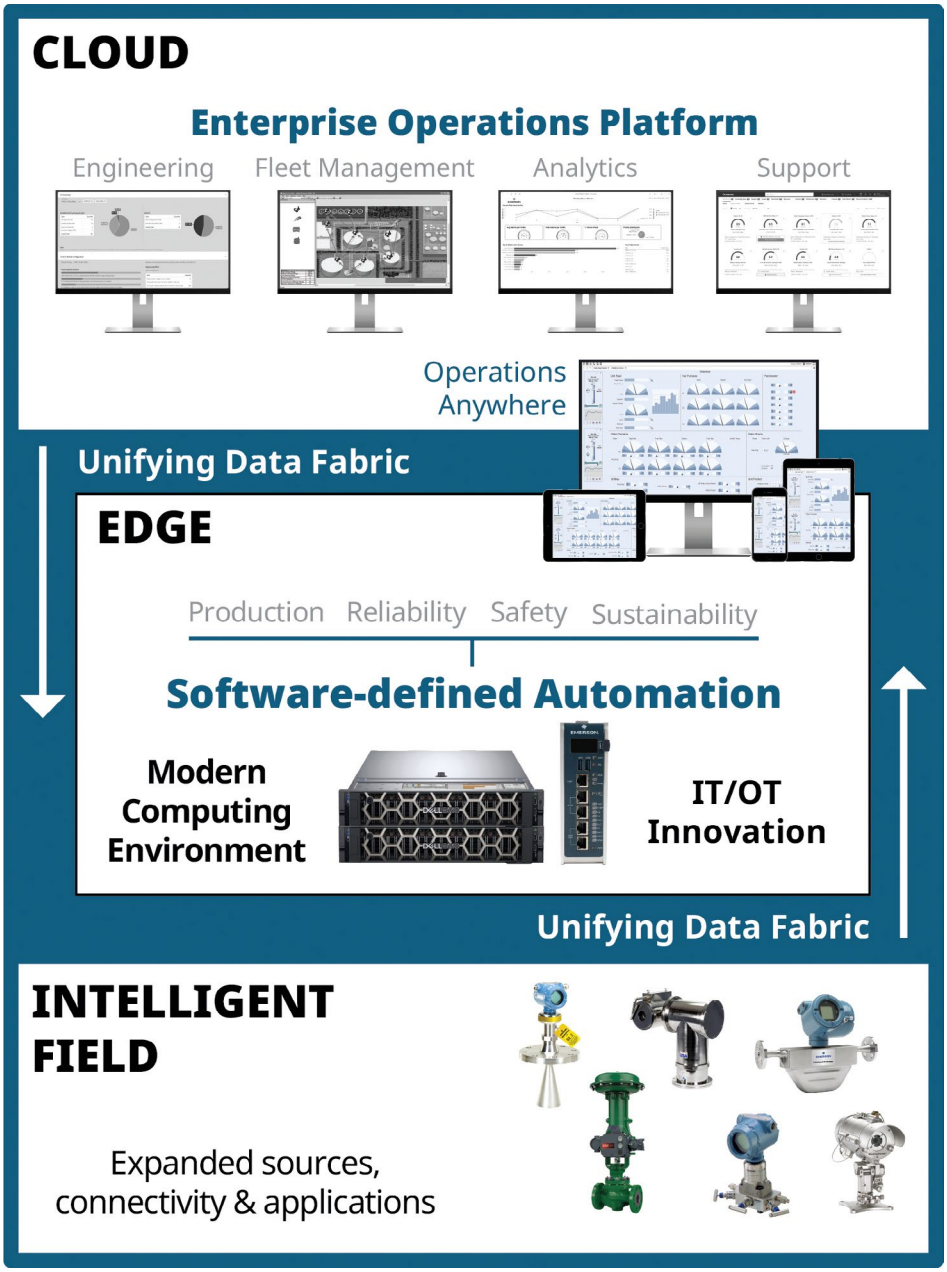


Illustration of what Boundless Automation" looks like

more with the distributed control system, using the data directly to find ways to improve production or efficiency.

The new Edge Environment includes a testing environment or "sandbox", where people can experiment with dashboards and applications, or train AI tools.

The data from the control system to the testing environment is only able to flow in one direction and is encrypted. This means users can have constant access to real time data without having a risk of messing up the operations.

Users can run visualisations, analytics, alarms, digital twin simulations and other systems with data from the DeltaV Edge Environment.

It uses standard data communication protocols such as OPC UA and can integrate with other software tools using REST API interfaces. It can be programmed using scripting tools like Python.

Emerson sees the DeltaV Edge Environment as "the first step in defining the control system of the future"

Digital valve controller with edge computing

In October 2023, Emerson launched the "Fisher FIELDVUE DVC7K" digital valve controller.

This is an example of edge computing, with a digital system connected directly to a field device (the valves).

The edge computing system can analyse the health of the valve and advise on the right corrective action.

Personnel can be alerted about developing problems, so the maintenance can be proactive rather than reactive.

For example, a control valve may be reacting slowly to commands requiring it to move, which is often an early sign of impending issues. The DVC7K will recognize this type of condition, alert personnel, and provide recommendations for fixing the problem.

The device can communicate with Bluetooth protocol over a distance of 30 feet, so maintenance staff can receive data onto their handheld device. The data can also be sent longer distances via wired connections.

Previously data from a digital valve controller would first need to be sent to a host system to be processed, and data could only be viewed from within the control room.

Digital transparency – a pathway to better digital technology?

Could more digital transparency, defined as digital systems which are much easier to understand, be a door opener for faster implementation of digital systems in the oil and gas industry? And how can we get there? *A Digital Energy Journal perspective*

Oil and gas / carbon capture digital technology could benefit from more digital transparency, particularly in operational decision making.

This is Digital Energy Journal's hypothesis – one we would like to explore with the industry – and we welcome you to join us.

By digital transparency we mean the ability for people to understand our digital systems, and the ability for digital systems to understand (perhaps better expressed as 'align with') the way we work.

We do not mean sharing data. A decision by an oil and gas operator to share data is a commercial decision, and commercial decision makers tend to prefer not to share any data they consider valuable unless they are forced to. Encouraging digital transparency is something completely different.

This is not a revolutionary idea - you will see that just about all of the articles in Digital Energy Journal relate to digital transparency in

some way. How can we get there faster?

What digital transparency means

Digital transparency can be expressed as three basic things.

First, it is easy for people to understand how digital systems work, whether they are system developers or users.

Second, it is easy for our digital systems to 'understand' how we work. This means that we have clear, granular understanding of our goals and processes, and how we expect digital technology to support them.

That needs to be done with as much granularity as possible. A very low granularity statement of a goal could be "we aim to be more efficient". But in real life you have multiple people attacking this goal in different ways, and also considering other goals while they do so, and the company develops processes, including human decisions, to pursue these goals.

Third, it is easy for people who understand the domain to understand how our digital systems are constructed, because it is built around these goals and processes.

Much of our digital systems is software, but our digital systems are far more than this.

"Digital systems" includes the portfolio of software products we use. Also, our processes for managing data, including understanding of the data inventory, data quality management and governance, knowing what is fit for purpose, data security and access management, data accessibility and how all of this aligns with our industry goals and working processes.

Digital transparency is not usually something any product vendor will see as a high priority in how they present their products. Most vendors are primarily seeking to sell, not to help clients understand how their products work. It is something technology clients need to ask for and develop themselves.

Human decisions vs automated processes

Automated processes, which do not involve any human decision making in them, are popular in the industrial digital technology world. A traditional factory makes money from automated processes. A technology trend of recent decades has been to extend automated processes beyond the factory gate. We see companies which appear to be completely operated by automated processes, such as Amazon and Uber.

But the complexities and variety of the real world means that the pursuit of automated processes can only go so far. Beyond that point, company decisions need to be made using traditional human judgement. And our digital technologies need to support human judgement. Most of the oil and gas industry operates, and succeeds commercially, in its operations beyond the point that automated processes can handle.

In a world of automated processes, the digital and automation system is king and most workers are subservient to it. The only people who need to understand the digital systems are the programmers.

But a world reliant on human judgement is a completely different paradigm. People need digital systems which explain the world in a way which makes sense to them in pursuit of their goals. The digital systems need to be orientated around their goals. This is something completely different. This is the concept we present here.

Toughest problems

While digital transparency is useful everywhere, it will provide the biggest benefits in trying to solve the industry's most difficult problems, or helping people to pursue complex goals which are otherwise not being achieved.

Much of the time, the industry's normal approach to digital technology works well enough, in that it serves us in our work to find, drill and produce hydrocarbons, and characterise CO2 storage.

But today the industry has new challenges, which it is not yet on top of, and where more digital transparency could prove useful.

In exploration and production, we need to get better at working with and synthesising multiple data sets, and past human experience, in order to manage equipment, find efficiencies, work better with suppliers, track emissions, maintain safety, and reduce fuel consumption.

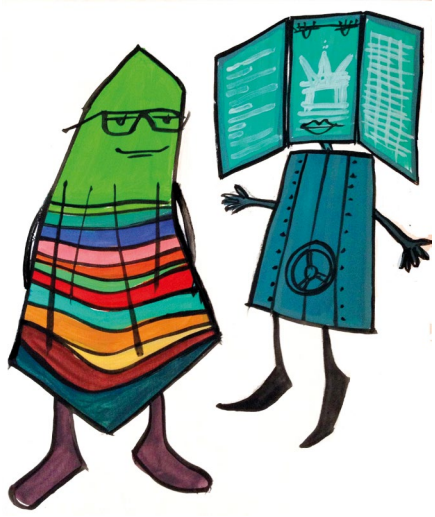
In carbon capture and storage, we need to get better at understanding CO2 storage sites, and understanding how CO2 is behaving in reservoirs as it is being injected, using multiple data sources combined with human geotechnical knowledge. We need to continue improving the efficiency and cost of CO2 capture and transport systems.

Technology benefits

Digital transparency is not just about choices of software and how we manage data and security. It is also about how our software is coded, and how easy the code is to understand.

We achieve digital transparency, to people who understand the real world domain, when the logic of the code and the attributes are aligned with the goals and processes of that domain, rather than structured around a database.

This should mean that different software products built for the same business goal can be integrated more easily, since they are built around the same processes and attributes, which are those the real world domain uses.



The logic of the software should be easy to understand by people who already understand the domain's logic.

We should find it easier to extend and adapt the software products we have. This should mean that we can use the same software products forever, rather than having to completely replace them every few years, like we do with our smart phones. This is something the Silicon Valley business model, and its investors, seem to expect of all technology products.

If we plan to use the same software for decades with gradual upgrades, it makes more commercial sense to put in the effort of incorporating specialist company knowhow and processes into the software, or client companies developing and owning their own software.

Cybersecurity should also be easier. The risks in the digital technology should align with risks in the real world. These are normally more transparent and easier to understand than digital risks. So we know which parts of our digital systems need the strongest defences.

With more transparent digital systems it is easier to spot if it is being compromised. We can also understand our cybersecurity systems better.

Digitally transparent systems should not be easier to hack, since we can use encryption to control who the systems are transparent to.

AI

Digital transparency is useful for AI. We want the AI tools themselves to be transparent rather than black boxes. But we will also get the most benefit from AI tools when they find their place within a transparent system.

Unless we ever see artificial general intelligence, AI tools will only be able to do specific

tasks that they have been programmed to do. This may be very helpful, but only if we can see what data we are feeding into them and see how we can use their outputs as part of our work.

Large language models can do many different tasks but only within the realm of knowledge covered by written text available for the model to index. In the energy industry they can be useful in finding answers from geological papers on the internet for example. But not useful in telling us how to fix a compressor.

Improving emphasis on data management

An emphasis on digital transparency can also drive a better focus on data management.

Oil and gas data management professionals often despair at how low priority data management is given in oil and gas companies, with senior management only caring about it when they need something and can't find it.

But with digital transparency, the whole digital system, including data management, can be easily seen by everybody.

It becomes much easier to see the function data management plays in supporting the business to achieve its goals. And also much easier to see where good data management processes are not being followed, and what problems that is leading to.

And digital transparency can also show how well managed data is important in making it easy for people to access the data they need to make their decisions.

Improving safety through Learning from Normal Work

We can identify ways to improve operational safety by studying day to day working practises in better ways. Dr Marcin Nazaruk explained how it can be done

In the past, much safety learning was drawn from understanding how accidents happened. But today we have fewer accidents, and the lagging indicators are no longer sufficient to tell us how well we manage risk.

Conversely, we often believe if we do not have any accidents, it means we all rules were followed, and all controls were applied , says Safety Transformation expert, Dr Marcin Nazaruk.

So we may have reached the limit of how much we can improve safety by learning from accidents. The safety focus needs to move to 'learning from normal work', he says.

This includes finding better ways to learn from employees about their work, identifying 'error traps' in the way that work is done, identifying risks which can be caused by a multiple factors happening at the same time, and identifying where operational factors mean that work cannot be easily done in the 'safe' way it was planned to be done.

Learning from normal work requires the development of a new mindset, and specific practical skills, it is not just about following a process, he said.

Dr Marcin Nazaruk, safety transformation expert

Background

Dr Nazaruk originally studied psychology then took a PhD in applied safety science in partnership between academia and an industrial partner.

He subsequently worked in a number of high-hazard industries, including over 10 years in the oil and gas sector, leading global human performance programs and human factors investigation efforts, before starting his own company, Psychology Applied, in 2022.

He has since contributed to publications on proactive learning for IOGP, SPE and the Energy Institute. He has also chaired a number of human factors industry groups.

"Throughout my career, I've seen repeat and surprise accidents, the investigation findings completely missing the point, the inability of corrective actions to make any meaningful improvement, and a huge misunderstanding of how human and organizational behaviour works," he writes on his website.

"Enhancing what we currently have may be easier and more effective than adding in something completely new," he said.

Learning from accidents?

It is easy to believe that incidents happen because something or someone failed or malfunctioned, Dr Nazaruk says. If there are no incidents, we assume that all procedures were followed, and we do not look too closely at what make the completion of work difficult or challenging. Conversely, if there was an incident we assume something was done wrong, such as a procedure not followed.

But actually, when we look into how the work was completed without accident, we find the same factors present in incident investigation reports. Steps in procedures may be skipped, there may be insufficient time, or the correct tools might be unavailable. These challenges evolve over time, limiting available choices and prompting people to adapt and find ways to overcome them. These adaptations enable jobs to be completed smoothly and rarely cause events. In other words, things go wrong for the same reasons they go right.

"I'm happy to bet my money, I could take your recent investigation report, see the findings, visit your operations elsewhere, and I would find these things being present but there is no accident," he said.

Leadership approach

In order to learn the right lessons from normal work, you need leadership who have trust in employees and their positive intentions, or as Dr Nazaruk puts it, have a "constructive interpretation of the reality of work."

"If leaders believe that accidents happen because of lazy and complacent individuals, they will not invest in additional efforts, not allow for certain corrective actions. They will push back, criticise, use punitive methods which will kill trust," he said.

As leaders, the information we have is taken from the questions we ask, but also the questions we ask stem from what we believe about reality. It leads to a phenomenon described in a research paper by prof. Eric Hollnagel, "What you look for is what you find." The way we interpret reality is drawn from what we already believe about how the world works.

For example, if you believe that problems are usually caused by people being lazy, if anything goes wrong you will start by trying to

work out who the lazy person is, and you will find someone to blame.

But if you believe that the way things happen at work is usually due to multiple factors, then you will seek to find what interactions between these factors contributed to something going wrong, and what else may have been involved.

Avoiding blame

You will get better answers to questions if they are framed in a way which does not blame anybody. Instead of asking "what is the problem and why did it occur," you might ask, "what is getting in the way of completing this task safely and efficiently," "what makes this job difficult," "what do you need to complete this work safely and efficiently."

So, a shift to a focus on the needs of the worker. The question "what do you need," leads to a discussion about what is missing.

If you see something being done which appears to be incorrect to you , you can ask a worker, "what is the advantage of doing it this way?".

One company had a rule that workers should not hold their fingers close to "pinch points" in equipment, where two objects come together, causing an injury risk.

A worker was seen with hands close to the pinch points. Instead of challenging the worker, the question was posed as "what is the advantage of this behaviour which appears to be breaking a rule."

The answer was that when the worker's hands were close to the pinch points, it was easier to manipulate equipment and enabled work to be done with more precision. The further away the worker's hands were, the less precision, and more likely there were to be quality defects.

Another useful line of questioning could be "tell me about situations when you need to deviate from procedures to complete the job". It may show that problems of a certain type are sometimes encountered during nightshifts, when some resources, required under the procedures, are not available.

Useful lines of questioning might be "help me understand your task", "what makes this job difficult", "how would you improve this procedure," "tell me about a time you had to perform a specific task without being provided with the necessary training," "tell me about equipment that is not compatible with the process."

The general point here is to focus on aspects external to a person such as their task, their job, or their process. If you focus on the person, you imply that you think there is something wrong with the person, and it causes the person to be defensive.

Not following procedures?

In normal work anywhere, people are constantly adapting to changing conditions and challenges. For example, if they are using a crane to lift a load, they may find there is less time than planned, additional people in the area, correct tools such as a lifting sling not available, or someone being off work.

Workers will deal with these challenges in a way that makes sense to them given their circumstances, resources, experience etc., and workers will adapt to deal with these constraints.

The combination of constraints and adaptations will affect the risk. Some adaptations may reduce the risk, others may increase it.

The reason workers do work the way they do is not always obvious to senior management, who may not fully understand the constraints they are under, because constraints are difficult to observe directly.

For example, a company might require that people follow the "lock out tag out" process to ensure dangerous equipment is properly shut off before working on it.

This procedure involves placing a physical lock on the equipment preventing anyone else from switching it on, with a tag attached to the lock stating the name of the worker with the key.

This process can take 60 minutes. A worker under time pressure caused by the maintenance backlog, who knows there is no chance anyone else may try to activate the equipment because they are in a remote location, may feel it is equally safe to just remove the power plug from the equipment, and save an hour of time.

Another example is a procedure that requires wearing of personal protective equipment. A worker finds that the gloves are a little too tight, exerting constant pressure on fingers, leading to discomfort and pain, so it is much harder to do the task..

There may be a procedure stating that a worker cannot be distracted when doing a certain task. But there may be another process happening at the time, which needs their input in order to continue therefore creating an operational dilemma.

Error traps

When looking for situations of high risk in normal work, you should be looking for what Dr Nazaruk calls an "error trap," a condition that increases the likelihood of a mistake or non-compliance. Then look for ways this specific risk can be avoided.

One example of an error trap is a marking on a container of lubricating oil which is part of a machine. There is no indication if the mark shows the minimum or maximum level of lubricating oil. So, an employee could easily fill above the line thinking it is the minimum, when it is really the maximum.

There can be error traps in the way work is set up. In one example, a crane operator used a handheld cabled device to control the crane. The short length of the cable meant the operator could only operate the crane standing in a certain spot. From this spot, they could not properly see the load.

So, a second worker was assigned to stand on the opposite side of the room, who could see what the crane is doing, and relay instructions to the operator such as "left" and "right." But because the two workers are facing each other, "left" to one worker means "right" to the other. The buttons on the control are also marked "left" and right." So, there is an error trap, the crane could easily be sent in the wrong direction.

The problem was fixed by providing a remote control system, which allowed the crane operator to move freely, changing the text next to the control buttons to say North, South, East and West, and having a clear compass on the ceiling so everybody knew which direction North was.

Risks beyond 'hazards'

It is common practise to do "risk assessment," seeking to identify hazards involved in a certain task, then to determine if there are measures in place to mitigate them.

Risk assessors typically focus on identifying hazards which can directly cause harm, such as from lifting heavy objects, getting exposure to electricity, chemicals, or hot surfaces.

But accidents are often caused from a combination of factors which are not individually considered high risk.

For example, people think that a forklift placing a pallet on a shelf is a safe task. But if the lighting is poor, there is a risk that the driver cannot see clearly where the pallet should be placed on the shelf. So it is not placed safely on the shelf, and falls off and injures someone.

Other risks could come from doing a routine task but where there is insufficient time, the correct tool is not available, or there is an 'error trap.'

When defining risks, it is useful to define them with as much granularity as possible, Dr Nazaruk says. So, the risk of the falling pallet can be described as above, not by simply saying "there is a risk of a falling pallet".

Further information about 'learning from normal work', and Dr Marcin Nazaruk, is online at **www.learningfromnormalwork.com**

Finding Petroleum

UPCOMING WEBINARS

Register and watch videos at www.findingpetroleum.com

Petroleum systems in West Africa and its Conjugate Margin
....revitalising Exploration! - 12 Jul 2024

New Insights West of the Shetlands
West of Shetland may be the only UKCS basin that can deliver a significant number of large prospects - 05 Jul 2024

Lessons from past disruptive discoveries
The importance of questioning subsurface assumptions - 28 Jun 2024

If you are able to give a talk at a webinar on a theme related to digital competency and clarity please contact Karl jeffery on **jeffery@d-e-j.com**

PAST WEBINAR VIDEOS AVAILABLE ONLINE

Onshore Senegal - *a different bet to more and more deeper, deeper, water!* *21 June 2024*

Investment opportunities in new Direct Air Capture technology *20 June 2024*

Developments with new EU CO2 storage projects *19 Apr 2024*

New capture and storage projects in the US *Feb 22, 2024*

Explore onshore Sub-Saharan Africa - not just deep, deep, water! *Feb 9, 2024*

Better ways to model and improve emissions performance of a facility *Dec 8, 2023*

W(h)ither Global Exploration? *Dec 1, 2023*

Better ways to sense oil and gas methane emissions - *satelilte and airborne* *Nov 17, 2023*

See **www.findingpetroleum.com** click on **'Videos'**

Event plans at www.findingpetroleum.com and www.d-e-j.com