DECEMBER 2020

INTERRUPT INSIDE

Our most popular articles in 2020

Software-driven cost cutting and performance optimisation of wind turbines

Controlling the power needed to de-ice drones

The 2020s: the decade of software-defined mobility

Electrification and autonomous driving
the mega trends pushing the boundaries of wire harness design

No Internet of Things without strong cyber security

5G changing the world as we know it
Three software specialists on 5G opportunities

5G
IS A GAME CHANGER FOR THE MILITARY

Meet Servet Coskun,
WHO EATS, SLEEP AND BREATHE GREEN TECHNOLOGY!

WHAT´S INSIDE .....

THE 2020s:
THE DECADE OF SOFTWARE-DEFINED MOBILITY

Electrification, autonomous driving and all-embracing vehicle connectivity is fundamentally changing the way we move goods and people around, and the digitalisation of mobility has the potential to help us handle the huge challenges the world is facing regarding urbanisation, sustainability and climate change. No doubt, the 2020s will be the decade of software-defined mobility.

BY: Arne Vollertsen for TechPeople A/S and Crister Nilson, Consultant Manager & Automotive Business Area responsible, Sylog AB

An average new car is managed by between 70 and 100 Electronic Control Units, and constantly monitoring itself and its surroundings with hundreds of sensors.

To emphasise the challenge, some call it "The Mother of All Tech Battles": In our effort to digitalise, connect and automate every aspect of mobility, we need to handle steeply increasing system complexity, cyber threats, new business models, and lawmaking issues, just to name a few of the many obstacles ahead.

As experts in embedded and IoT solutions, and a trusted and experienced technology partner to the transport and automotive industry, at Data Respons we face these challenges on a daily basis. And based on that expertise we feel we have a fairly clear view of the things to come in the 2020s, a decade that doubtlessly will bring enormous changes in the mobility sector.

A computer on wheels

The vehicle industry has come a long way since the introduction of the Cruise Control, the first vehicle feature that integrated mechanical and electrical systems. That was in the 1950s. Now, cars are computers-on-wheels running millions of lines of code. An average new car is managed by between 70 and 100 Electronic Control Units, and constantly monitoring itself and its surroundings with hundreds of sensors.

Partly, this revolution has been triggered by other technology areas, for instance telecom. There has been exponential growth in memory and processor power, while components have become cheaper, smaller and more robust. On top of that, a set of new components like radar, infrared cameras and ordinary cameras are being added to the system, further increasing complexity on all levels.

Facing this complexity, vehicle architecture is evolving as well. Currently, there are two main approaches in vehicle architecture: Either one large computer serving the whole vehicle or a distributed set of computers with a network between them. Both paradigms have their pros and cons, and it remains to be seen which approach will prevail.

Increasing amounts of data

However, as autonomous driving is slowly developing, component and system complexity is increasing, and with it the amount of data to be processed. To handle that complexity it is tempting to look for inspiration in aerospace and aviation, or similar domains operating complex, mission critical systems. That makes good sense, e.g. when it comes to data analysis, as these areas produce a lot of data to be processed, analysed and combined in the most efficient and correct ways.

But there is a difference. In aerospace and aviation you operate in controlled areas, and traffic is heavily regulated. Though obviously not without risk, it happens in a fairly controlled environment. That is not the case with a self-driving vehicle navigating in an urban area with its unpredictable mix of conventional cars, pedestrians, children, pet animals etc. So, is the object detected by the car's radar a rock, a plastic bag or a child? Or is it somebody walking across the street with a bicycle, like in Temple, Arizona, in March 2018, when a woman was killed by a self-driving Uber car?

A thing of the future

A truly autonomous vehicle is still a thing of the future, although Tesla is leading the way with self-learning algorithms. But there have been a number of accidents in the US which clearly indicate that autonomous vehicles cannot be trusted 100 per cent. They still depend on driver intervention, although some car manufacturers seem to be over-selling their partially automated vehicle, e.g. by using the term "Autopilot" to describe its Driver Assist system.

Following an investigation of a crash in 2018 in California in which the driver of a Tesla died, Robert L. Sumwalt, chairman of the US National Highway Traffic Safety Administration, summed up the situation in this way:

"It's time to stop enabling drivers in any partially automated vehicle to pretend that they have driver-less cars." (New York Times 26.2.2020)

To be on the safe side, it is sensible to restrict fully autonomous vehicles to controlled environments like industrial sites or harbours.

But all that may change quickly. Industry roadmaps show, that by 2025 almost every car manufacturer will have a fully autonomous car in its product portfolio. From that point on the number of autonomous vehicles will rise quickly. When approx. 50 per cent of all vehicles have become autonomous it would make sense to gradually allow autonomous vehicles in non-restricted areas. We could see autonomous driving in semi-controlled environments like for example on motorways. Regulators may decide, that some parts of a motorway only are to be used by autonomous vehicles, with drivers switching back to manual when leaving the motorway and heading for urban areas.

The powertrain is simple

As mentioned, with improvements in vehicle autonomy the complexity of the vehicle will increase significantly. With one exception: the car's powertrain.

Compared to an electrical engine a conventional combustion engine has more mechanical parts, and it is much more difficult to control injection times, combustion in the cylinders etc. In this regard the vehicle of the future will be simpler. However, when it comes to the powertrain manufacturers face an altogether different challenge: What will be the fuel of the future?

Although it is widely agreed that the conventional fuel combustion engine will be a parenthesis in human history, the battle about what will come next is still raging. Currently electricity seems to be gaining the upper hand, but although batteries are a much more efficient way of using energy than gasoline, they have an environmental impact, requiring rare minerals and recycling when worn out. For instance, to extract 1 ton of lithium requires 2 million litres of water. And cobalt, another rare metal required to manufacture batteries, comes primarily from thousands of small, private mines in the highly unstable Democratic Republic of Congo, often involving child labour.

For these reasons, a probable future scenario could be a combination of a battery pack on-board the vehicle, combined with electrification of roads through induction via the road surface or other energy transmission technologies.

But all that is extremely hard to predict. By the end of this decade things may have changed and other superior technologies may have emerged.

Vehicle-to-X

Regardless what powertrain technology will prevail, multi-layer connectedness will be the dominant feature of any future car. The vehicle will connect to its immediate surroundings, to local infrastructure, to other vehicles, and to the cloud, all at the same time.

The vehicle will monitor its surroundings through an array of different sensors, and it will receive data from surrounding infrastructure like traffic lights or an approaching emergency vehicle. Also, vehicles will communicate with each other. This short-rage vehicle-to-vehicle communication could come into play, when a vehicle is part of a train of vehicles. If the car in front detects an obstacle and hits the brakes it will instantly signal to the cars behind it to brake as well. Thus a vehicle can extend its on-board sensor capacity to thousands of additional sensors in its vicinity.

Note. The image is manipulated for the purpose of illustration

In addition to vehicle-to-vehicle and vehicle-to-near-infrastructure communication there will be long-range connectivity enabling other features, like user-based insurance, condition monitoring or various car-as-a-service solutions.

Securing data lakes

The data produced by the vehicle is stored in large data lakes, to be utilized for instant analysis, for development of new services and much more. Manufacturers, scientists, authorities and others can dig into these data lakes e.g. to design more efficient logistics and mobility systems. Accessing and utilizing these vast amounts of data ought to be beneficial to all involved, provided that integrity and privacy is guaranteed.

Obviously, these new possibilities create many risks as well, and in this it is crucial to stress the importance of cyber security and data integrity. Imagine if criminals could get access to data showing that a car and its owners

are out of town, leaving their house unguarded, making it an easy target for break-in. Or imagine a trucking company trying to hurt a competitor by breaking into its system, downloading faulty roadmaps to the competitor's fleet management system, deleting freight orders etc.

When it comes to cyber security and data integrity, the mobility industry can look to sectors in which these issues are mission-critical, banking and finance for instance, where transactions, access, and confidentiality are guarded by state-of-the-art technology.

Rewriting laws and regulations

Also, the digitalisation of mobility will give lawmakers some hard nuts to crack. Laws will need to be rewritten, nationally and internationally, and there will be tough debates on the freedom of the individual and the right to privacy versus what's best for society and for the environment.

As an example, everybody would probably agree that it would be in everybody's best interest to allow an approaching emergency vehicle to take over control of vehicles in front of it and force them to pull over, for it to reach an accident as quickly as possible.

But how about taking that scenario one step further: In everyday traffic, should local authorities be allowed to take control of a number of cars and reroute them to avoid congestion? Or maybe even prevent a number of vehicle owners from using their vehicle for a period of time, for the sake of the environment? Imagine walking out to your car in the morning to drive to your office, just for it to tell you "No, not today, please use public transportation instead".

Huge investments

Digitalising and automating the mobility sector will not only pose big challenges to lawmakers. Businesses are also taking huge risks and making significant investments in technology, knowing that some of it may not make it to mass production.

As it is widely known, Tesla, the technology leader in autonomous electric vehicles is burning billions of dollars. Still, in 2019 Tesla produced only 367.500 vehicles, next to nothing compared to the world's large-scale vehicle manufacturers. They churn out between 7 and 10m units a year.

With so much happening in the mobility sector, manufacturers have a lot on their plate. Simultaneously, they integrate new components into vehicle systems, they develop algorithms for autonomous driving, and they work with electrification of the powertrain.

Adding to that, the challenges of electrification of the powertrain and autonomous driving is attracting significant investment from companies outside the vehicle sector. New companies focusing on either developing algorithms for autonomy or technology for electrification are emerging. And as profitability in the vehicle industry is slowly shifting from metal and mechanics to software and services, there may very well be a new Ford or a new Toyota among them. The future may see completely new business cases in the vehicle industry, shifting from a car brand as we know it to a service provided by a nondescript shell on wheels.

Truly, these are exciting times in the mobility sector.

Want To Know More?

DR. ANDREAS LASSMANN
Managing Director
IT Sonix

NO INTERNET OF THINGS
WITHOUT STRONG CYBER SECURITY

The concept of IoT holds great potential: By connecting millions of devices to the internet we can save time and money and become more efficient, we can offer our customers more convenience, better service and much more. But no grand vision without a snake pit of problems: With the Internet of Things comes the Internet of Threats. We need to protect our new network-aware systems and devices. There will be no Internet of Things without a strong focus on cyber security.

BY: Arne Vollertsen for Data Respons & René Matthiassen, TechPeople consultant, CISSP, CISM, ISO27001 senior lead implementer and auditor

Some security experts compare the current state of IoT security with Asbestos. They predict that in a few years time we'll look back asking ourselves "What were we thinking of?". Others draw parallels to the World Wide Web of 1994-95, arguing that IoT will be a security train wreck for years, before we eventually figure it out.

Messages like these may paint a too gloomy picture of the challenges within IoT. But nevertheless, cyber security is a crucial IoT prerequisite, not least due to its close interaction with the physical world. IoT threats can go far beyond the well-known, conventional Internet threats like credit card theft. They could disable home security systems, manipulate navigation systems on connected vehicles, disrupt smart medical devices or knock out entire energy systems.

IoT is speeding up

At Data Respons we have broad experience and a long track record in IoT security, and currently we are experiencing a significant increase in customer inquiries and projects in the IoT cyber security domain.

No wonder, because IoT is coming at us with terrific speed. We are connecting more and more devices and systems to the Internet, whether they're industrial control systems, cars, cameras, door locks, fitness trackers or medical technology. By 2020, the number of installed IoT devices is forecast to grow to nearly 31 billion worldwide. And IoT threats are increasing simultaneously: Experts predict that in 2020 more than 25 per cent of enterprise attacks will involve IoT.

Increasing awareness

Luckily, awareness of the importance of IoT security is increasing. For instance, it was a wake-up call for the IoT business, when in 2016 the Mirai botnet succeeded in enslaving millions of devices, including IP cameras and routers, turning them into centrally controlled botnets for Distributed Denial of Service (DDoS) attacks. Currently there are still Miria variants, like Mukashi, out there constantly scanning the web for vulnerable IoT devices, looking for weakly protected machines with factory-default credentials or common passwords.

Moreover, in June 2020 the largest independent consumer body in the UK, Which?, revealed that 3.5 million cheap wireless cameras produced in China and distributed worldwide could potentially be hijacked by hackers.

New security agenda

So, the picture is quite clear: IoT sets a whole new agenda for cyber security. It's not enough to take security concepts and standards from the world of modern administrative IT and adapt them to this new domain. Furthermore we have to keep in mind the closeness of IoT to the physical world, together with the increased complexity and multi-layer nature of many IoT ecosystems. All this requires a multi-level approach to security.

For the sake of clarity let's divide IoT projects into two different categories, each of which requires different approaches: Firstly, developing a complete new IoT product from scratch, and secondly, adapting a legacy system to the new world of IoT.

Greenfield projects

Developing new IoT products is relatively straightforward, seen from a security perspective. Starting from scratch gives you the advantage of incorporating security into an early stage of your design. You can do security-by-default, taking all the right decisions when it comes to patches, updates, access control, user authentication etc., integrating security from the very beginning.

Also, greenfield projects allow you to adopt a holistic security approach. Thinking holistically is the best way to handle the complexity of the multi-layer IoT ecosystem. It means thinking security on every level, whether it is on the sensor/actuator and gateway level, whether it is encrypting the data sent through the system, or securing the stored data and the web and mobile applications being developed.

Risk assessment

Another important approach is risk assessment. It helps you channel your security effort into where it's most needed and where it will make the biggest difference. Risk assessment means finding vulnerabilities and threats, estimating the likelihood of the threat to become reality, finding ways to mitigate attacks etc.

It is crucial that risk assessment is done for the complete end-to-end value chain of an IoT product or service, bearing in mind that it's more complex than conventional digital services. An IoT solution will typically be blending technologies, devices, software, connectivity, data storage etc., so there is much to consider. For instance, you may have designed an IoT device with great security features. But if you fail to think security when you're designing the app associated to it, you might get in trouble. Likewise, if there are flaws in the cloud solution you have chosen to store your data.

Risk assessment is increasingly gaining momentum, driven among other things by standards and legislation requiring developers to take a holistic, risk-based approach to IoT security. Furthermore, this approach helps you prioritize your development resources and helps you spend your security budget where it makes the biggest difference.

Legacy systems

A whole new challenge comes, when we want to adapt older systems to the modern IoT world. Bringing systems developed 20 or 30 years ago into the new world of IoT requires much consideration regarding security.

Quite understandably the companies responsible for these systems want to give their customers access to the new business opportunities coming from IoT. As an example, manufacturers of ship engines and other heavy duty ship equipment are looking for ways to bring their machinery online, thus

creating new possibilities for service and maintenance. But enabling these legacy systems in terms of access and connectivity to the internet from everywhere and from a wide range of devices means exposing them to a new world of security risks. Connecting to the Internet means connecting to potential cyber threats.

Low level of security

This is particularly challenging, as these legacy systems are "born" with a very low level of security, both in terms of the way they have been developed and the way they are maintained. Now they have to be aligned to the modern cyber security world, and to meet state-of-the-art requirements for patching, updates, password protection etc. That is a major challenge.

Probably the companies responsible for these legacy systems are not in the habit of issuing security patches, simply because they have never been required to do so. Patches were released, when there was a requirement for e.g. new functionality.

Making legacy systems that were never intended to work with any kind of security, comply with modern security requirements is a complex task. But it has to be done, because all the advantages coming from connectedness will turn into threats, if we are unable to ensure the confidentiality, integrity and availability of these systems.

IoT Vulnerabilities

PATCHING
Patches are not released with the same frequency as commonly done in the IT world. That leaves vulnerabilities in the system for a long time before patches are sent out to fix the problem. Or worse: Some devices are not designed to receive patches/updates at all

WEAK PASSWORDS
Some IoT devices have only 4, 5 or 6 digit passwords, and this lack of complexity means they are easily breakable. Also, it may not be possible to change the admin user of the device, and default usernames and passwords are easy to find on the Internet.

COMMUNICATION
Is communication from the device encrypted, and if yes, is encryption strong enough? Is it encrypted both in transit and in rest?

FAULTY SOFTWARE
When you develop your IoT product it may be a good idea to reuse software developed by others. However you have to check that the software you're reusing is without security flaws, and that you're using the newest version of the code.

END-OF-LIFE
What happens if the component or device you're using reaches end-of-life and is not supported by the supplier anymore?

PRIVACY PROTECTION
Do you have any data about your user stored on the device? What about 3rd party integrations?

ONLY ONE LAYER OF SECURITY
One layer is not enough. You need defence in depth, where several layers of security are used to protect data and information

The need for security standards

The vast majority of IoT devices or devices used in ICS (Industrial Control Systems) do not follow or have not been designed to follow security standards or guideline. This means that we'll need to "pave the road while we drive it" i.e. design and implement security during the implementation, instead of during the design of the products or early in the products' lifecycle.

Some security standards exist though, like IEC 62443. Others are about to be developed on a European level e.g. from ENISA (The European Union Agency for Cybersecurity) and ISO (International Standardization Organization). These will become available in the years to come.

More pro-activity needed

Luckily, awareness regarding cyber security is rising. The media is publishing cyber crime stories on an almost daily basis, and manufacturers and service providers face considerable pressure from both customers and from governments and regulators, if they are found neglecting their security responsibilities.

But still we see more reactivity than pro-activity. All too often security experts or tech-savvy users are the ones that find and publish security flaws. Only then manufacturers will fix the problem, and by that time the damage done could be significant.

In the coming years we will be witnessing numerous incidents, in which IoT devices are used for cyber attacks or in which customer data has been compromised. The companies affected will react in retrospect, but ideally it should be the other way around: Because of high security standards and heightened awareness we will – hopefully soon – get to a point, where reacting in retrospect is rare and where heightened awareness will keep incidents to a minimum.

Well-known dilemma

However, the well-known dilemma between convenience and security will continue to challenge companies, developers as well as cyber security experts. The old saying about password complexity also applies to IoT security: the longer and more complex, the more secure, but the more tiresome as well.

On the one hand companies and customers want convenience and ease-of-use. They want devices and services available at their fingertips without the hassle of security procedures. On the other hand we have the security experts pushing for confidentiality, integrity and availability. The tricky thing is to find the balance between these two considerations.

But when you consider this dilemma more closely, you'll find that there is no getting around security. In fact, although the starting point for many companies in IoT is the cost savings and convenience IoT has to offer, they quickly realize that only with security in place they can focus back on realising the potential of IoT, optimizing processes, boosting service, reducing costs and designing outstanding customer experience.

ELECTRIFICATION & AUTONOMOUS DRIVING

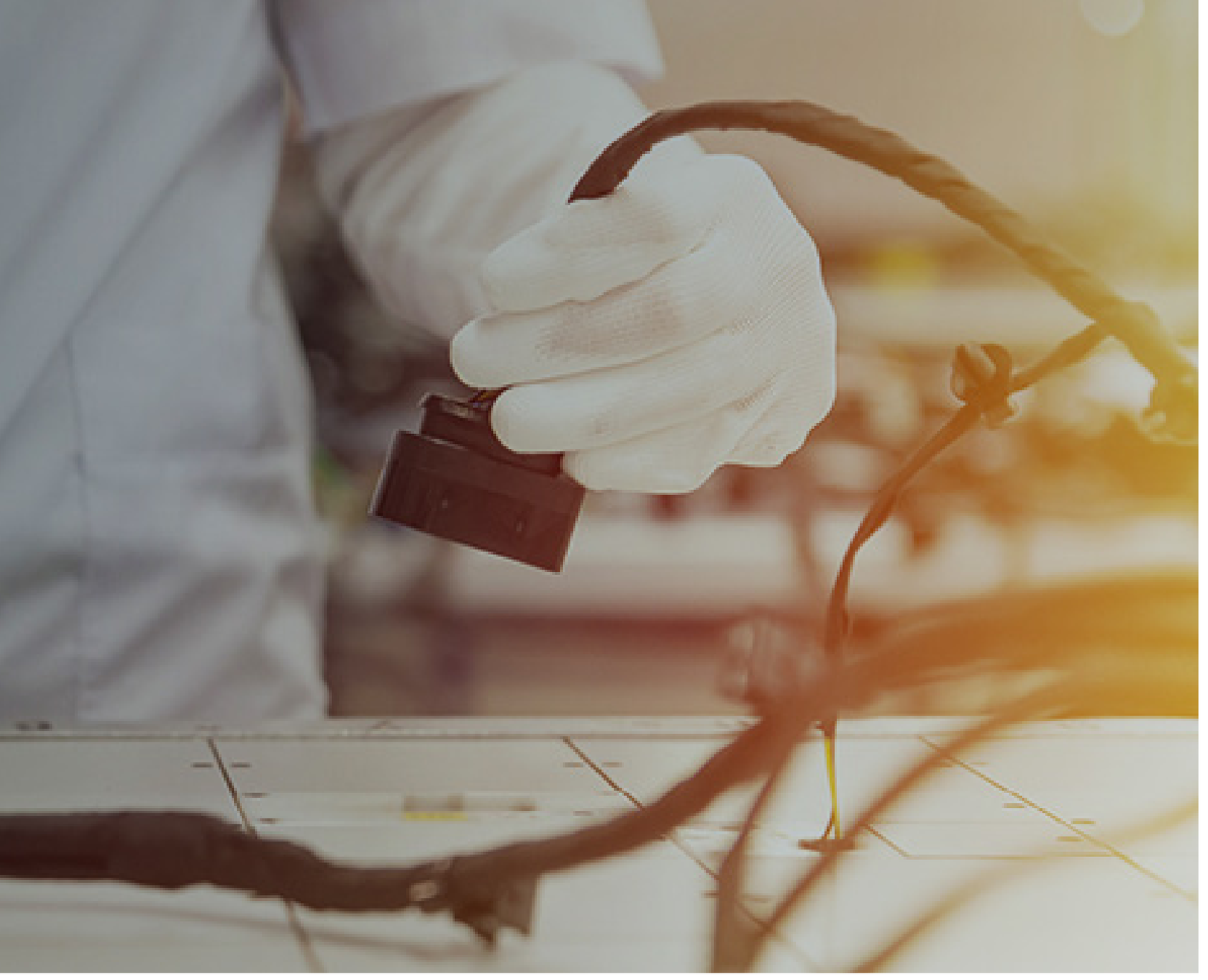
THE MEGA TRENDS PUSHING THE BOUNDARIES OF WIRE HARNESS DESIGN

Everybody is talking about autonomous driving and electric cars. However, not many are aware of the invisible helper making it all happen. It is the car's nervous system – the cables and connections that make signals and data flow inside the vehicle, enabling the super sophisticated features of a modern, sensing vehicle. Say hello to the wire harness.

BY: Arne Vollertsen for Data Respons & Martin Lampinen, Managing Director, inContext AB

Wires are just wires, you may think. How complicated could that possibly be?

Well, extremely complicated in fact, at least since our cars started morphing into computers on wheels. The 50s and 60s are long gone. Back then power steering, electric windows, and the occasional aircon were the height of luxury motoring. Nowadays the metal skin of a premium car hides a multitude of sensors, actuators, control units, high-performance computers, infotainment system etc., and more features and components are being added at breathtaking speed: Five years ago, vehicles had 25 per cent less circuits than today's cars. Five years from now, that number will increase by another 30 per cent.



Indispensable connectivity

The wire harness is the spider's web in the middle of it all, and it is indispensable to nearly all aspects of a modern vehicle. That is why designing the wire harness of a state-of-the-art car, bus or truck requires both a general understanding of car components like sensors, actuators, batteries, motors etc., as well as knowledge of the nuts and bolts of electrical systems design.

You need to know everything about wires and connectors, and you need to understand the vehicle as a whole to be able to design a wire harness, that is clever and cost-efficient, while being easy to assemble and service as well.

Welcome to the world of wire harness design, right now struggling with a nasty cross-pressure: How do we connect an ever-increasing number of components with less and less space at our disposal?

Wiring experts

inContext is one of a handful of specialist companies focusing on wire harness design, and its 80+ developers are involved in a broad range of projects in the Swedish vehicle industry. Their expert skills in Complete Electrical Systems Design go into the development of new cars, buses and trucks that incorporate cutting edge technologies. For instance, inContext is working on a new electro powered bus, electrification of a plug-in hybrid truck, and providing wire harness design for the special requirements of military vehicles. Also, inContext contributes to future autonomous vehicle concepts with interconnect, electrification and software development.

The next generation harness

In short, the inContext people know what they are talking about, when you ask them what the next generation wire harness will look like: It will enable more powerful electrical systems to operate vehicles, as the latest electrical connectivity allows ever more signals from on-board sensors, other vehicles, road-based infrastructure and satellites to be streamed into a high-performance computer. That computer, in turn, will transmit signals through the wire harness to braking, steering and other control systems.

All this is gradually maturing into a technical infrastructure for electrification and autonomous driving – an exciting vision, indeed, but a vision not without challenges.

More stuff, less space

To begin with, as mentioned above, there is the cross-pressure issue: A growing number of sensors and other devices are being added to the vehicle, and thus needing more wires to integrate them into the car's system. But at the same time vehicles want to become smaller, thinner and lighter. So, where to put the new wire spaghetti when you've got less space at your disposal? It's hard to discard anything, as you still need all the traditional vehicle components for it to work properly.

Wire harness designers are competing fiercely with all the other teams in charge of developing a new vehicle. They all need their piece of the shrinking space to be allocated for their specific use, so everybody needs to compromise to make it work.

Going modular

Modularity is one of the keywords in that specific dilemma, looking into the future of wire harness design. Designing with modularity in mind can help cope with the cramped space and rising amount of wires in a modern vehicle, particularly because many vehicles are produced in a number of different variants.

In theory, you could design a wire harness that could handle all the vehicle options and features on offer. But that would be too costly, it would add to the vehicle's weight, and it would take up too much space. Instead you need to think LEGO. With a modular design you can expand the basic harness with sub-harnesses where needed.

That approach also facilitates assembling and servicing, especially in the heavy vehicle industry, where many inContex customers operate. When assembling a vehicle, instead of rolling out the complete wire harness and installing it at once, you can do it in sequence. This plug-and-play approach to assembling makes good sense, when a vehicle comes in many different variants, as is the case in the heavy vehicle industry. And what makes sense in assembling makes sense in maintenance as well. It is a lot easier to replace a wire harness designed in a modular fashion. You avoid having to replace the whole thing because of one cable breaking down.

Handling high voltage

Another significant challenge for wire harness design is electrification. The magnetic field created by high-voltage cables tends to disturb low-voltage systems, so when designing a harness you need to factor in this EMC noise (Electro Magnetic Compatibility). To protect the signals running in the low-voltage communication cables you have to be careful not to put them near to their high voltage siblings. And that is quite a challenge, especially with limited space at your disposal.

High voltage cables can pose a threat to humans as well. If a passenger riding an electric bus carries a pacemaker the EMC noise coming from the bus motor could interfere with it. That is yet another risk has to be addressed by wire harness designers in collaboration with component owners. And apart from EMC noise there is the sheer size of high voltage cables, not to mention their cost. For both reasons they need to be as short as possible.

Autonomy coming

Everybody is talking about self-driving vehicles. inContext is contributing to this megatrend, as well as to electrification, by designing reliable, cost-effective wire harnesses that are easy to assemble and service.

Moreover, next generation wire harnesses may enable extremely powerful electrical systems to operate vehicles without human intervention. For that we need more sensors, more bandwidth, bigger computers – and all this is leading to a re-engineering of automotive wire harnesses. The industry is thinking about architecture in new ways, for instance finding inspiration in high-security domains like aerospace. Think multi-layer redundancy, fault tolerance, advanced connectivity, and cyber security. Those are the requirements of the future, and you have to think really hard trying to meet these goals while keeping down weight, power consumption, and overall cost

New types of cables

One way of addressing these trends is rethinking the wires themselves. We are going towards using a larger variety of wires, compared to the regular wires used in a standard vehicle CAN system.

CAN is not enough to transfer the huge amounts of data in the system, and CAN cables need to be complemented by coax- and ethernet-type cables. However, many of them are not really adapted to the automotive industry, so manufacturers are working to develop new types of cables to meet the changing requirements in the industry.

The harness of the future

No doubt, wire harnesses are evolving rapidly, to meet the challenges posed by electrification and autonomous driving. But what are the long-term perspectives? Looking into the future, what will a state-of-the-art vehicle wire harness look like in 10 years?

According to the inContext experts, wire harness design will probably be totally different from now. Today we use wires because they are flexible and easy to route, but the future of wires may not even be wires. Most of the signals could be communicated via wireless, provided we find satisfactory solutions to all the cyber security issues that inevitably will follow.

Wireless technologies have a number of advantages, for instance when it comes to saving weight and avoiding EMC noise. However, power cables are difficult to replace entirely. To simplify that part we might begin using modular busbars going through the whole vehicle, functioning as the main power source for vehicle electronics.

inContext

Interconnect, autonomous systems and embedded software

Read more about inContext here

SOFTWARE-DRIVEN
COST CUTTING AND PERFORMANCE OPTIMISATION OF WIND TURBINES

Wind turbines are fascinating, not only due to their size, but also because of their hi-tech combination of large-scale mechanics, power engineering, sensors, and sophisticated software. Yet the wind turbine business is no different from any other industry, with fierce competition and a strong focus on optimisation and cost cutting. Software plays an important part in this game.

BY: Morten Fogtmann and Anthony Roberts, TechPeople

There are many ways to use software for optimizing wind turbines. Detecting bats is one of them. Bats and wind turbines don't go well together, and in many countries bats are protected animals. To prevent them collide with the rotor blades, a bat detecting system stops the wind turbine when bats are detected in the vicinity.

With all the buzz surrounding sustainable energy you would think being in the wind turbine business could be compared to winning the lottery. Far from it: The global wind turbine industry is under considerable pressure, with only a handful of manufacturers making a profit.

Why? Because governments are gradually reducing their subsidies expecting renewable energy to become competitive on its own. Subsequently, competition is fierce and development engineers are working tirelessly to find new ways to cut production costs while increasing the output and the durability of each new generation of wind turbines.

Levelised Cost of Energy

So, although software developers come at a comparatively high price for wind turbine manufacturers, their work is crucial for cost savings in the long run. They continuously find ways to reduce what the energy sector refers to as LCoE, Levelised Cost of Energy, being the summary measure of the overall competitiveness of different energy generating technologies.

Software is a key component in this effort. Software is an important tool for optimising cost in the wind industry, on many levels and touching on all parts of a wind turbine: tower, nacelle, hub, rotor, and power electronics.

TechPeople is a long-standing partner of the Danish wind industry and TechPeople software engineers are contributing to numerous projects using software to optimize the design and the output of wind turbines. However, due to the competitive situation in the sector, many of these projects are subject to Non Disclosure Agreements. That is why this article will be focusing not so much on specific projects as on presenting a high-level view of the challenges and achievements in using software as a cost-optimising tool in the wind industry.

Turning hardware into software

Eliminating a piece of hardware and replacing it with software is a well-known cost-saving measure in many industries. It is done in the wind industry as well. As an example, a hardware counter module monitoring the toothed ring to measure speed and angle of the hub can be replaced by transferring the hardware functionality into FPGA code.

Optimising the structure of the tower

In building wind turbine towers, the amount of steel needed is an important cost factor. The tower must be able to cope with the pressure on the rotor blades, dependent on wind speeds in the specific area where the wind turbine is deployed.

The blades can be pitched to manage the pressure against the tower, adjusting to different wind speeds, and changing the angle of the rotors towards the wind. This reduces wind pressure and subsequently reduces the need for steel used in the tower. Further-

more, the pitch system allows the turbine to operate in conditions where a turbine with fixed wings would be forced to shut down to protect itself. The pitch system of a state-of-the-art wind turbine is controlled by a distributed real-time system enabling the wings to pitch very quickly.

You can even pitch each rotor blade separately and make it pitch automatically when it passes the tower, to reduce stress on the tower resulting from the change in wind characteristics when the blade passes the tower. This increases the lifespan of the wind turbine.

What is a distributed real-time system?

A distributed real-time system consists of a number of (computer) nodes that are interconnected by a real-time communication network. Most distributed real-time systems are embedded in larger systems, like a mobile phone, a car or a wind turbine, interacting closely with their physical environment. The performance of such a system depends not only on the logical results of the computation but also on the exact time these results are produced. Many applications are safety or mission critical, so fault tolerance and reliability are crucial features.

A distributed real-time system can contribute to optimization and cost saving by enabling a device to react immediately to outside input and thus achieve a higher degree of efficiency and performance.

Sensor fusion

A modern wind turbine is equipped with a vast number of sensors measuring e.g. speed, temperature, vibration, light etc. Without sensors, wind turbines would be less safe, more costly to operate, and have lifetimes less than the 25 years they are expected to run. Furthermore, wind turbine operators rely on accurate data about every turbine and its components, to secure operational safety and efficient maintenance. As an example, dedicated sensors can detect sparks produced by faulty machinery, to prevent fire.

Also, increased processing capabilities lead to new ways of using sensors, including using them for other tasks than they were designed for. For instance, data from a wind speed sensor can detect ice on the rotor blades. With multi-sensor data fusion you can design sophisticated fault detection systems with a higher diagnostic accuracy than individual sensors, with an array of vibrational, acoustic, temperature etc. sensors monitoring gearboxes, blades, and other mission critical parts of the wind turbine.

What is multi-sensor data fusion?

Multi-sensor data fusion refers to combining observations from a number of different sensor types to monitor complex machinery e.g. self-driving vehicles, based on the assumption that evaluating data from disparate sources leads to a more precise result than if the sources were used individually. In a sense, multi-sensor data fusion tries to replicate the work performed by the human brain, weaving diverse input together to form a complex picture, taking advantage of different "points-of-view". Multi-sensor data fusion is widely used in robotics and can utilize techniques like pattern recognition, artificial intelligence and statistical estimation.

Wind turbines need electricity to run

It may come as a surprise to many, but wind turbines need electricity to run. Not only do they produce energy, they consume energy as well, so they need back-up power supply, for instance for starting up again after shutdown due to strong winds. Restarting a modern wind turbine is a complex task. You have to re-calibrate the wind turbine and synchronize it to the grid, before releasing the brake.

Offshore turbines in particular have to be designed to use as little power as possible produced by their diesel generators, to make fuel supply last as long as possible and keep expensive re-filling at a minimum. Software is used to optimise the energy consumption of the turbines.

"Also, increased processing capabilities lead to new ways of using sensors,including using them for other tasks than they were designed for.

Adjusting wind turbines to national requirements

Manufacturing wind turbines is a global business, so manufacturers use much manpower to adjust their products to local legal and environmental requirements. This also goes for the lights on top of the turbines. They have to be adapted to local requirements, both when it comes to light intensity, colour and frequency. In some places the lights have to blink 24/7, elsewhere only at night or only when airplanes are approaching.

Detecting airplanes requires a radar system, and similar measures are taken for "bat detection".

Bats and wind turbines don't go well together, and in many countries bats are protected animals. To prevent them collide with the rotor blades, a bat detecting system stops the wind turbine when bats are detected in the vicinity. The reason for choosing these seemingly extreme measures is that a bat detection system makes it possible to deploy wind turbines in areas where it would be otherwise prohibited.

How does a bat detection system work?

Wind turbines can be a lethal threat to bats. Not only do they risk direct collision, but also the high air pressure differences in the area surrounding the turning blades can cause internal injuries.

One form of bat protection strategy is to limit the operating period of the turbine based on time of day and year, as research shows, that bats are most active within two hours of sunset and in temperatures between 19 and 21 degrees. The disadvantage is a reduction in operating time and thus power production. Another approach would be to place hyper-sensitive microphones around the turbines to detect the ultrasound signals bats use to orient and forage. The ultrasound signals are then analysed, and according to the specific bat species identified and its behavioural pattern the operation of the wind turbine shifts to bat-mode, e.g. changing rotor speed, changing the pitch angle of the rotor blades etc. In this way the turbine can still produce energy while reducing the risk of bat encounters.

Also, bat deterrent systems are being developed that use ultrasonic speakers to discourage bats from approaching operating wind turbines. The speakers produce ultrasonic sound in a range of frequencies that negate the bat's own signals. Bats send out ultrasound signals and use the reflections of these signals to navigate and find insects etc. The deterrent system sends out a signal that masks the bat's return signal, so that it cannot locate any prey in the airspace surrounding the turbine rotors.

Competition continues

Nothing indicates, that the competition in the wind sector will diminish in coming years. So, probably the world will run out of fossil fuel before software engineers in the wind energy business will run out of challenges. Software will continue to play a crucial role in cost cutting and optimisation, including utilizing Machine Learning and Artificial Intelligence, together with an ever-increasing number of sensors for control and monitoring. Also, with wind turbines getting larger and larger, and offshore wind farms moving further away from land, much remains to be done.

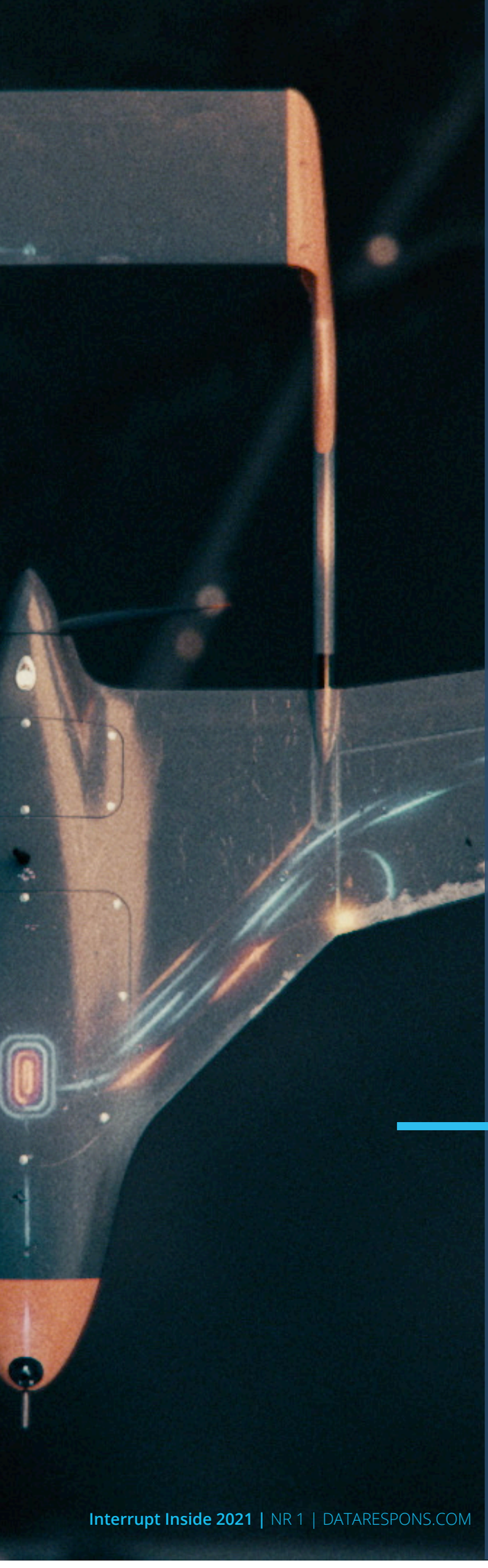
TechPeople is a consultancy house within the Data Respons group. The company is based in Copenhagen, and specialises in embedded solutions and IT business systems. TechPeople have specialists within hardware, software, mechanic development, project management and product testing. TechPeople's innovative customers range from large international companies to creative start ups.

Want To Know More?

KIM FAHRENHOLTZ
Managing Director
TechPeople

CONTROLLING THE POWER NEEDED TO DE-ICE DRONES

Animation of the current going from the drone's battery to de-icing panels in the wings



In its effort to bring the first drone de-icing system to market, Trondheim-based startup UBIQ Aerospace reached out to Data Respons R&D Services for hardware expertise to control the energy needed for setting drone wings on "defrost": A challenging assignment with a tight deadline.

BY: Arne Vollertsen for Data Respons

Just like passenger jets and other manned aircraft, drones run into trouble when ice builds up on wings and propellers. Manned or unmanned, they need to be aware of what frozen water can do: Ice accumulated during flight increases an aircraft's weight, reduces lift and maneuverability, and can ultimately cause it to stall and crash.

When it comes to fixed-wing drones, power will do the trick. Similar to the basic concept of an oven, you can send an electric current through a resistive material – in this case ultra-thin sheets – to heat up the wings and fix the problem, according to Kasper Borup and Kim Sørensen, founders of the Trondheim based startup UBIQ Aerospace.

From research to business

Building on their PhD studies and research at the Center for Autonomous Marine Operations at the Norwegian University of Science and Technology, the UBIQ team is now turning their research into a commercial product. Named D•ICE it is the world's first autonomous drone de-icing system. It is designed for medium sized fixed-wing drones with a wingspan of 3 to 5 metres but will also be applicable to large unmanned aircraft, the most valuable of which can cost up to 500 million Dollars.

D•ICE is a completely autonomous system, requiring no outside operator to manage. To detect icing hazards, a sensor package monitors atmospheric conditions. The data is analysed by a set of algorithms, which also monitor the behaviour of the drone, to detect any changes due to icing. A control unit then channels the appropriate amount of power from the aircraft's battery to the thermoelectric panels mounted on the wings and tail of the drone.

Harsh environment

As Kim Sørensen and Kasper Borup point out, when developing such a complex product there is a long way from prototype to finished product ready for volume production. Not least when the technologies involved come straight out of the research laboratory, and the system is required to function in a harsh environment with strict requirements regarding stability and safety.

– We've worked on this for 7 years, starting out in research and then beginning to commercialize the technology in 2017. Primarily our competences lie in software and development of autonomous systems. We are a small team, and we can't do everything ourselves, so when we needed to improve some of the hardware we decided to look for a partner. We did a thorough survey to find the right company to collaborate with, and Data Respons just stood out. They were extremely responsive and dedicated, and after meeting with them we just felt relieved. We had found the right people for the job, and we're going to work a lot more with them in the future.

Hardware expertise

UBIQ wanted to tap into Data Respons' broad experience in preparing prototypes for large-scale production as well as designing hardware for harsh environments, such as aviation, subsea and military applications. On top of that, they had a tight deadline, with only a few months to get a new version of the de-icing system ready for a number of important – and expensive – wind tunnel and flight tests.

– We asked them to design a new version of the control unit that processes the sensor data and controls the flow of energy from the drone's battery to the thermoelectric panels. They managed to significantly improve the controller. Now it is much smaller than the previous one, less error prone, more sleek and functional, and designed to meet the industry standard in this domain.

– Just to mention one thing, now we've got much better control of the powerful current that goes to the panels. That may not sound super sexy, but when you're sending high current through a small aircraft that can cost millions you need to be able to control it precisely, to avoid the risk of melting panels or a burning battery.

The control unit for the UBIQ de-icing system has been designed by Lyder (left side) and Ole (right side), drawing on Data Respons' vast experience in developing hardware solutions for challenging environments such as subsea and defence. Furthermore, on top of being a highly experienced hardware engineer Ole is also a drone enthusiast. He designs his own drones and is very well informed in regards to hardware and software controlling drones, battery usage, motors etc. Among other things he uses on-board cameras and VR goggles to view the world from the drone's perspective.

Tight deadline

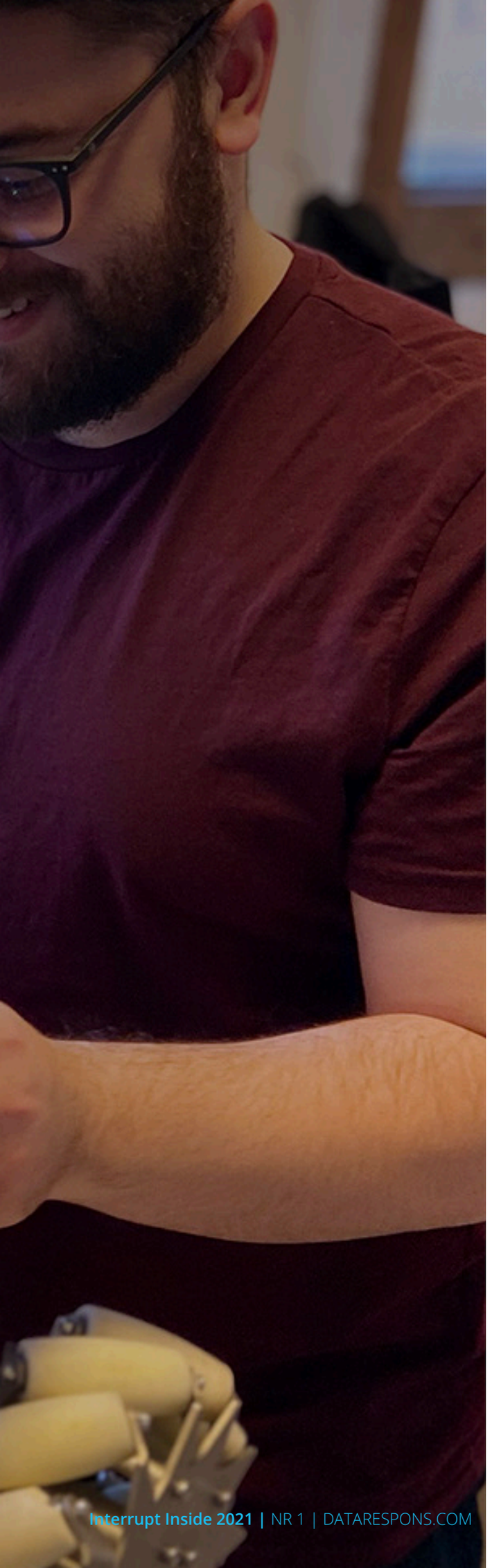
Furthermore, the Data Respons team was able to meet the tight deadline of the project. Starting in the beginning of June it had to be completed early September. The team was able to speed up the project by collaborating with a Data Respons sub-supplier in Shanghai that has worked with the company for more than 10 years.

– We are impressed by what the team has done. For us it is really comforting to have people with that level of expertise contribute to the project. Now there is one thing less for us to worry about, and that allows us to concentrate on what we are good at: developing autonomous systems.

– And we haven't finished partnering with Data Respons. We are very satisfied with the collaboration and with the support we got. They have experience in developing robust hardware solutions that meet the tough requirements in our domain, and they know how to bring prototypes up to industry standard and preparing them for batch production. We'll definitely make use of that expertise moving forward.

MEET SERVET COSKUN, WHO EATS, SLEEP AND BREATHE GREEN TECHNOLOGY!

Servet is a specialist electronics engineer working for Data Respons subsidiary TechPeople. He has his heart set on technology and sustainability, and in his spare time he started his own start-up company with the mission to make Vertical Farming competitive compared to conventional farms and greenhouses. To achieve this goal, Servet designed a self-driving robot gardener called Watney.



BY: Arne Vollertsen for TechPeople A/S

Watney is being developed by electronics engineer and TechPeople consultant Servet Coskun. He is designing the autonomous self-driving robot with a scissor lift to move the 250 x 80 cm plant trays stacked three stories high at the experimental facility in Kastrup, operated by seasony until recently.

Vertical Farming

Vertical Farming is high tech growing of crops in large windowless industrial buildings close to the world's mega cities. Plants are stacked on shelves, with their roots in water instead of soil. Sunlight is replaced by LED light, while water enriched with nutrient circulates in a large, closed system. Thus Vertical Farming can achieve total independence from outside weather conditions. Crops can be harvested several times a year, and food can be produced close to where it is consumed.

Since Dickson D. Despommier, professor of microbiology at Columbia University, launched the concept of Vertical Farming in 1999, it has been quite popular among futurists, tech-trendsetters and others promoting new technology handling climate change. But so far it has been rather difficult to turn the Vertical Farming vision into reality.

Vertical farming has the potential to contribute to handling some of the great challenges the world is facing:

In 2050 Earth's population will have increased from 7,5 to approx. 10 billion people, with two thirds of them living in urban areas. As a result, global food production has to increase by 70 per cent. This is where vertical farming could come in, not least because food could be produced directly within the mega cities of the future, thus eliminating the environmental impact of transport.

A step towards profitability

Until now Vertical Farming has been unable to evolve into large-scale production. The few attempts made soon brought one crucial weakness to light: profitability. Naturally, it dampens the enthusiasm, when a head of lettuce coming from Vertical Farming ends up being 10 to 20 times more expensive than a conventional one.

The main reason for this lack of profitability is the amount of manual handling needed. Vertical Farming is labour intensive and needs rigorous automation before it would make commercial sense to go from small experimental demonstrators to large-scale production facilities. This is where Watney the robot gardener comes in. Watney is being developed by electronics engineer Servet Coskun. He is designing the autonomous self-driving robot with a scissor lift to move the 250 x 80 cm plant trays stacked three stories high at the experimental facility.

Analysing operating procedures

For a year Servet and his company has run their own small-scale Vertical Farming facility together with a local company, operating a chain of restaurants and canteens, to find the most labour intensive operating procedures and find ways to automate them.

– We soon found out that handling of the trays should be at the top of the list, and to automate that procedure we designed Watney. It has scissor lift and forklift functionality and can drive autonomously to a plant tray. It then moves up to a desired height, takes out the tray and moves it to a new position.

– You can find similar self-driving robots in other domains, small-scale ones in pharmacies and big ones in the manufacturing industry and in logistics centers. We have designed Watney to fit the specific requirements of Vertical Farming, and I expect Watney to be ready for series production by the end of this year or early next year.

– In the long run we will to provide Watney with additional functionalities, like a camera monitoring the growth of the plants and checking for pests. Watney will also be able to cut the plants. Our long-term goal is to enable Watney to do everything a gardening worker does – and more.

Off-the-shelf components

Servet Coskun is primarily using off-the-shelf components to build Watney, an approach he picked up while studying and working for a company developing autonomous vehicles for industry and logistics. These engineers preferred to use standard components when possible, developing their own electronics only if they could come up with a more customized and cheaper solution.

– Watney will help us reach our goal, which is reducing manual handling in Vertical Farming with 50 per cent, says Servet Coskun. – That goal is very ambitious, but it is necessary to get there to make Vertical Farming compatible and scalable.

Watney needs help

However, Watney will not be able to achieve a 50 per cent reduction on its own. It needs help, and analysis of the work processes has highlighted other areas that could benefit from being automated. – While the handling of plant trays is at the top of our list, cleaning and preparing the system after a harvest comes in second. In Vertical Farming plants grow in a hydroponic system, in water circulating in a closed environment. They grow in large trays and after a harvest each tray has to be cleaned, and roots and other residue removed. That is done by connecting a secondary system, which cleans the trays using water with hydrogen peroxide added. After cleaning the tray is reconnected to the primary system. That process we want to automate as well.

Cumbersome calibration of sensors

– Another work intensive process is calibrating the sensors monitoring the closed system supplying the plants with water. In hydroponics the water has to have specific characteristics, e.g. a pH value of around 6.5, which is a little lower than ordinary drinking water. When growing, the plants emit basic substances causing the pH-level to rise. For the pH level to remain at 6.5 we have to continually measure it and reduce it if necessary.

– A pH sensor is very sensitive and requires calibration once a month, which is messy work. You remove it from its usual place in the main tank of the watering system. Then you clean it and put it in three different calibration resolutions. Each time you have to wait until it delivers a stable measurement, which you then register in your computer. Then you return it to the main water tank.

– On top of that, the sensor measuring the salinity of the water needs to be calibrated in two calibration resolutions, while the oxygen sensor needs one calibration resolution. A large Vertical Farming plant is equipped with a large number of sensors, so it makes good sense to find ways to automate the handling of them. The solution Servet is using today is range of sensors run on low power boards from Particle and communicate via WiFi.

By the way, Servet Coskun's robot gardener is named after the main character in the 2015 Ridley Scott movie The Martian. In 2035, astronaut and botanist Mark Watney, played by Matt Damon, is left behind on Mars, but manages to survive by growing vegetables in an improvised hi-tech nursery.'

5G

IS A GAME CHANGER FOR THE MILITARY

Secure wireless data communication is hugely important for the military, both at home and abroad. Besides the apparent administrative use, this goes not least the military tactical communication management system.

BY: Mikkel Helweg, Business Development Manager
Terje Jensvik, Technical Manager Solution in Data Respons Solutions Norway

Critical assignment communication is key

Within operative applications, critical mission communication – including critical machine-type communication (cMTC) – is crucial. This involves ensuring the necessary functionality, a high degree of robustness, security, shielding of data, and ensuring high uptimes across existing wireless carriers such as the IP-based LTE and 4G.

However, in line with increasing digitization, automation and autonomation, it is crucial that the military can also exploit new technologies such as fifth-generation mobile communication. That is to say, 5G is not a technology in itself but is a set of requirements, see 3GPP's 5G-NR (New Radio) standard (release 15 and later).

High speeds and low latency on the 5G network

5G's speed of 10 gigabits per second (see eMBB or Enhanced Mobile Broadband) is estimated to be 100 times faster than 4G. And the technology's theoretical delay of just a few thousandths of a second (1 ms) is 400 times faster than the blink of an eye...

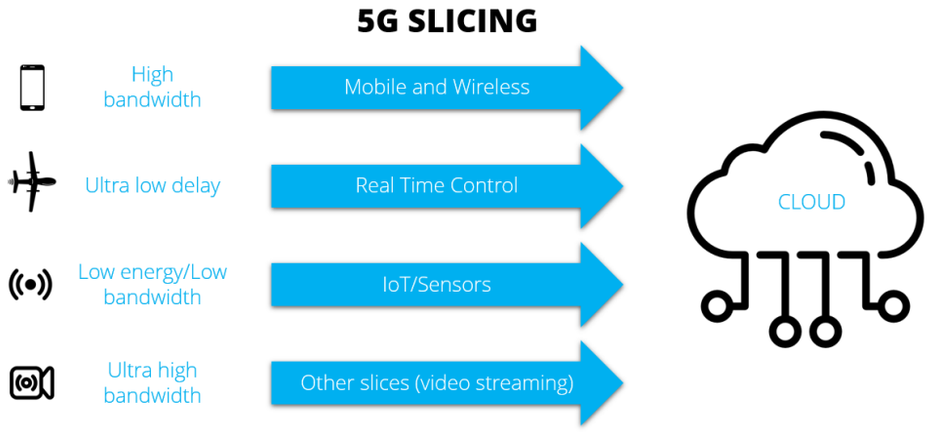
5G terminology likes to talk about URLLC (or Ultra-Reliable Low-Latency Communications) with regards to the above. The low delay is achieved among other things with the help of so-called Edge computing where data processing and data generation (systematic indicators, trends and performance data) is executed as close as possible to the endpoints, including sensors and effectors, where these can exchange data with one another locally with practically zero waiting time.

Separate "defence area" on the 5G network

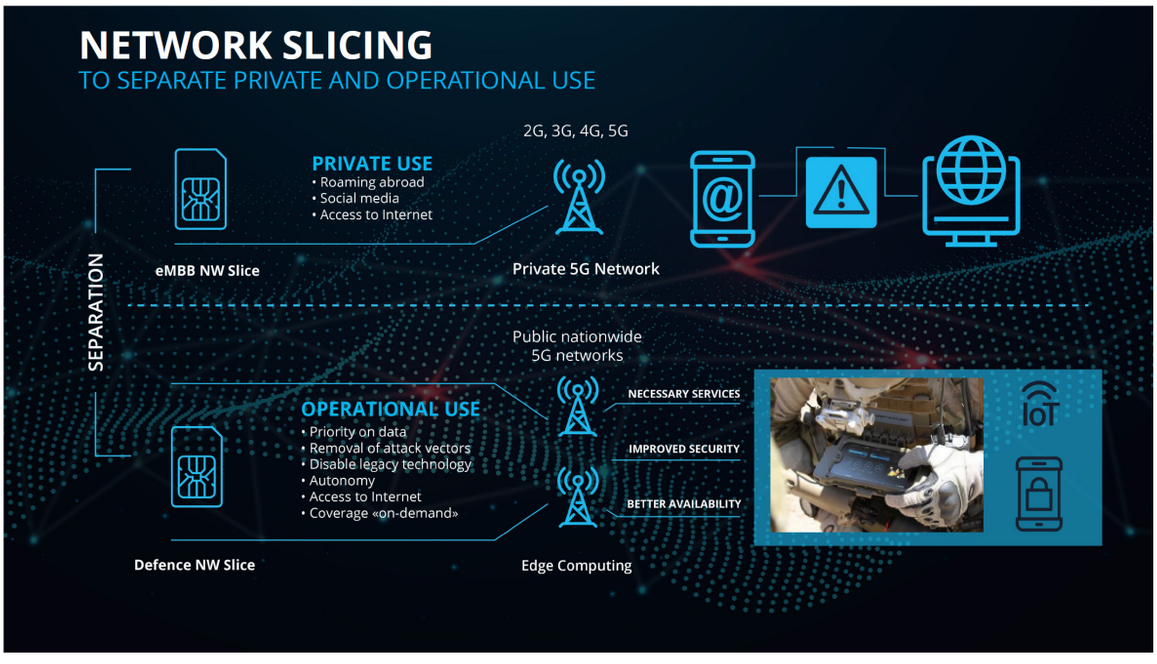
With the help of Software-Defined Networking (SDN) and Network Function Virtualization (NFV), it is possible to assign private, specially adapted user areas – so-called "network slices" – to different sectors, industries and enterprises on the 5G core network. These areas are built on top of the underlying mobile network. They are central to 5G technology since it is not possible to combine all the capacities previously mentioned without extreme investments. For example, it is impossible to combine very low delay with massive area coverage (up to 1 million units per square kilometre, ref. massive machine-type communication; mMTC). The private slices are therefore adapted based on critical parameters for each sector or enterprise, or different defence applications.

For example, a private 5G "Defence Slice" with high, prioritized speed and low latency will simplify heavy end-to-end encryption using keys that can only be read by the recipients. This is what is being tested in the 5G Vertical Innovation Infrastructure (VINNI) project which the Armed Forces are participating in.

These sorts of private areas are also of interest for other key agencies in the public sector, regardless of whether these agencies are part of a national defence structure or not. It is, for example, an expectation that a dedicated 5G network slice will replace the current emergency network in Norway from 2027 (after the Norwegian government decided back in 2017 that the next generation emergency network – NGN – should be based on a commercial mobile network). This network then recognizes that the coupled unit belongs to the "emergency services slice" and prioritizes it over other network traffic and communication.

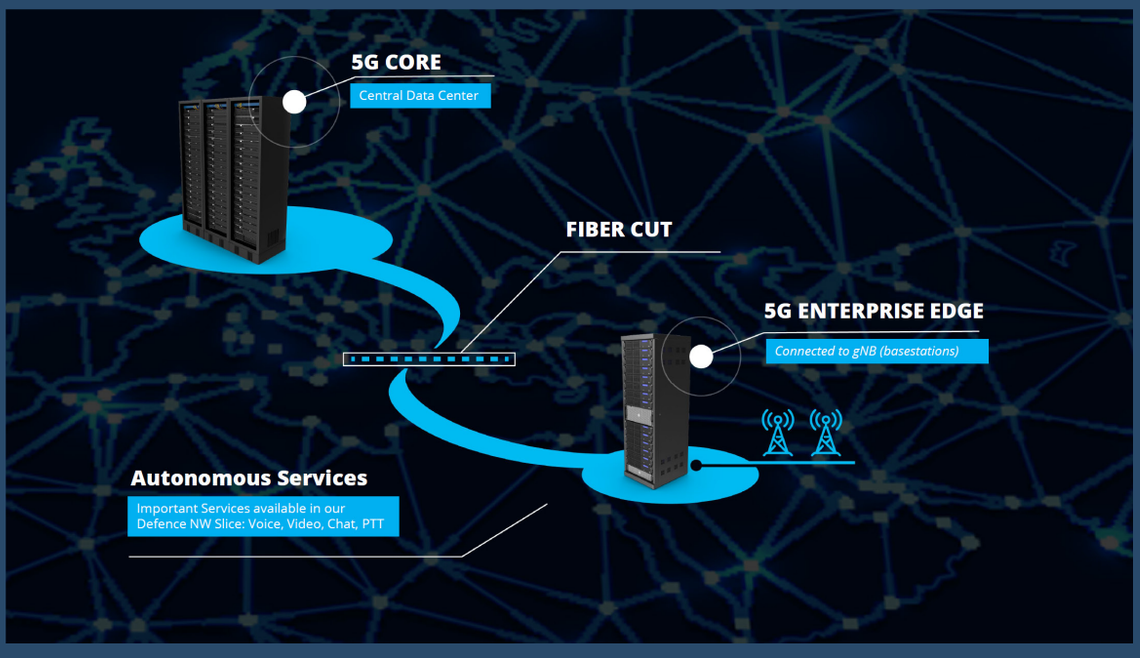


Slicing up the 5G network (own presentation after Intel illustration)



Slicing up the 5G network

5G Autonomous Service



5G Autonomous Service

Edge Computing nodes in airports, hospitals, in a municipality to provide essential services when the central 5G Core is not available.

IoT in the military domain; IoMT

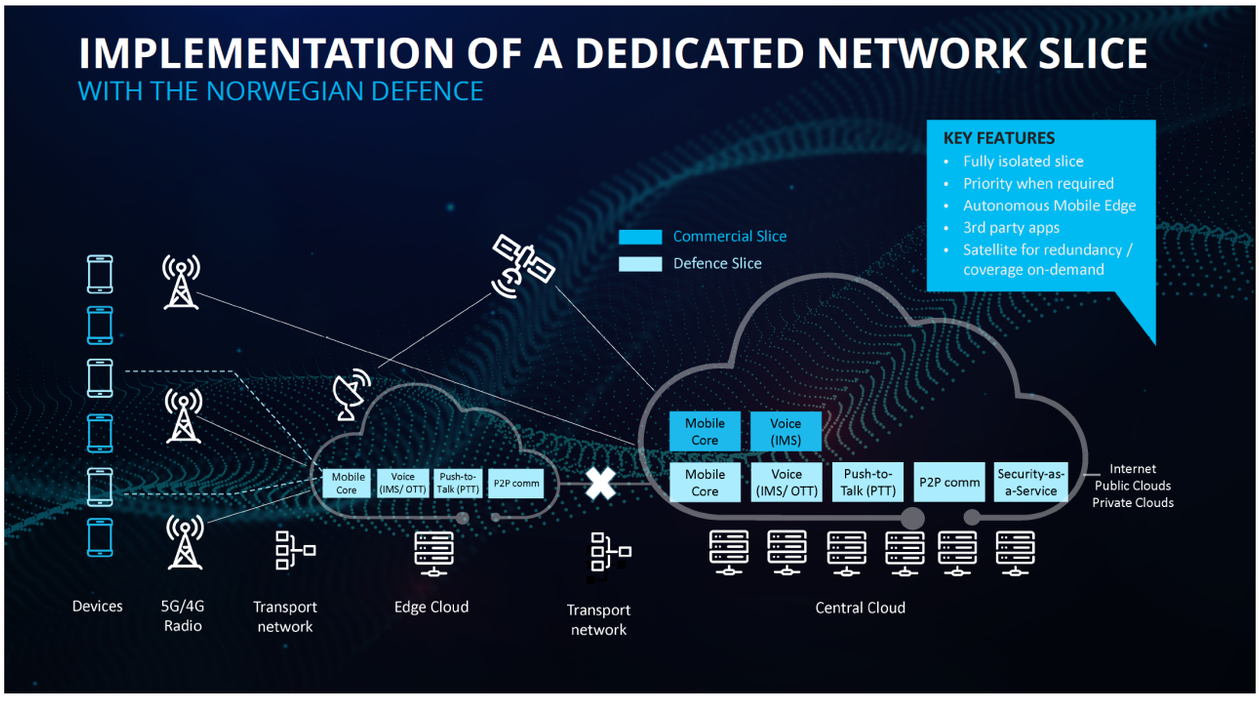
We are already very familiar with the expression the Internet of Things", the so-called IoT or IIoT (Industrial Internet of Things), whilst the international military jargon talks of the Internet of Military Things (IoMT) or Internet of Battlefield Things (IoBT).

Whatever term you use, the essence is the same: smart devices that talk to each other and their surroundings in their own cyber domains via the internet. This way, you can collect, process and interpret data, and control devices and sensors remotely. For the military, it is about sensor fusion; merging and analyzing data from devices and sensors such as surveillance cameras, detection sensors, base stations and gateways, smartphones, radios and communication nodes, and not least of all manned and autonomous vehicles and drones.

Based on this information, models and usable real-time data are generated for logistics and area control, intelligence and situational awareness, command and control, and finally active protection of combatant units and bases.

With the properties and capacities offered by 5G technology, we can take a giant leap forward and (as previously mentioned) the military can gather their IoMT together into one dedicated slice – a "defence NW slice" – with robust security algorithms and procedures, and where the properties and real-time speed of 5G technology (with performance in line with fibre optics) mean the guaranteed quality of service (QoS).

This all means that the military can get the most out of artificial intelligence (AI), virtual reality (VR) and advanced reality (AR). They can also react to emergency situations and control drones and vessels – individually or in swarms- in real-time via the mobile network.



Defence NW slice

Infrastructure, vulnerability and frequency range

There has also been a great deal of debate surrounding 5G and its vulnerability, not least in relation to radio equipment and key components for the 5G core network from the Chinese company Huawei. Several countries have chosen to ban Chinese technology from their critical infrastructure, the digital foundations of the nation. The largest telecommunications companies in Norway have also decided against Huawei ever since the new Norwegian Security Act came into force in 2019.

It is also about what frequency range the military will use. In Europe, there are three so-called 5G pioneer bands, two of which fall under Frequency Range 1 (<6GHz), specifically the low band (700MHz-2.3GHz) and the medium band (3.5GHz). The third falls under Frequency Range 2 and is often called the millimetre wave or high-frequency band (26GHz+).

There are opportunities and limitations, advantages and disadvantages to the different frequency bands, including with respect to the military's future use. The low band, known in Norway as the national network, is characterized by a high degree of robustness and increased area coverage. Still, it is not particularly fast compared to the other two bands. The medium band handles bigger volumes of data and is typically built up in suburban areas. The high-frequency band is characterized as being super-fast but only over short distances, meaning it requires a high cell density and extensive use of repeaters (millimetre waves suffer significant attenuation or are completely blocked by building walls and physical obstacles, and are absorbed in the atmosphere).

The military have applications in all frequency bands

No military cannot rely solely on borrowing frequencies from commercial operators, and instead must be able to establish and manage their own coverage where necessary. Military organizations also realize that frequencies within all three of the ranges are useful but for different applications. Frequencies in the low band are useful for deployable broadband solutions and tactical radio lines (outside of built-up areas where the risk of WiFi interruptions is lower).

In the medium band, the military already have existing licences for radar installations and depend on these frequencies being taken into consideration going forwards. There are also parts of this range that are of interest to the military in connection with the group and direction-defined antenna technology (MIMO/beamforming) and 5G drone detection (multi-static radar). The medium band is also widely used in the USA for radars, missile defence, electronic warfare and monitoring airspace.

However, the American Department of Defence (DoD) recently approved 3.4 and 3.5GHz frequencies for helping national technology companies to compete with China. Finally, the high-frequency band is interesting for the Armed Forces in terms of ultra-broadband card communication at bases and headquarters, for distributed sensors which require a lot of data communication, and for 5G satellite technology.

Regardless of the range, having their own dedicated and harmonized frequencies will allow the military to develop new, robust and secure technology solutions for administrative and operational applications.

Without 5G, we can't exploit the potential of new technologies to the full

There is also a debate raging internally within NATO regarding the vulnerability, infrastructure and range, but what is certain is that without 5G communication it would be close to impossible to fully exploit the possibilities offered by big data, artificial intelligence and cloud processing in both the military and other sectors. The same goes for getting the full-capacity effect out of hi-tech platforms such as the multi-role F35 aircraft in so-called multi-domain operations where situational information from Land, Sea, Air and Space is processed in a fifth domain – the cyber domain- allowing us to react by combining effectors from these domains.

The current government has stated in various forums that "the military must be the best at utilizing technology" and that this should be achieved through a high degree of independent technological competence, and cooperation between the military and governmental agencies.

In Norway the military is therefore also working on several 5G technology experiments, including experimental and pilot projects such as the 5G-VINNI project where new and secure speech and data architecture is also being integrated and tested in the "defence slice". Many of these projects are being conducted in collaboration with commercial stakeholders and businesses, which is important since Norway is home to a highly competitive environment both within and outside of the military in the area of wireless, operational and tactical communication.

Some abbreviations we have used:

SDN: Software Defined Network. NFV: Network Functions Virtualisation. LTE: Long Term Evolution. cMTC: Critical Machine type communication. mMTC: Massive Machine type communication. QoS: Quality of Service. MIMO: Multiple Input Multiple Output.

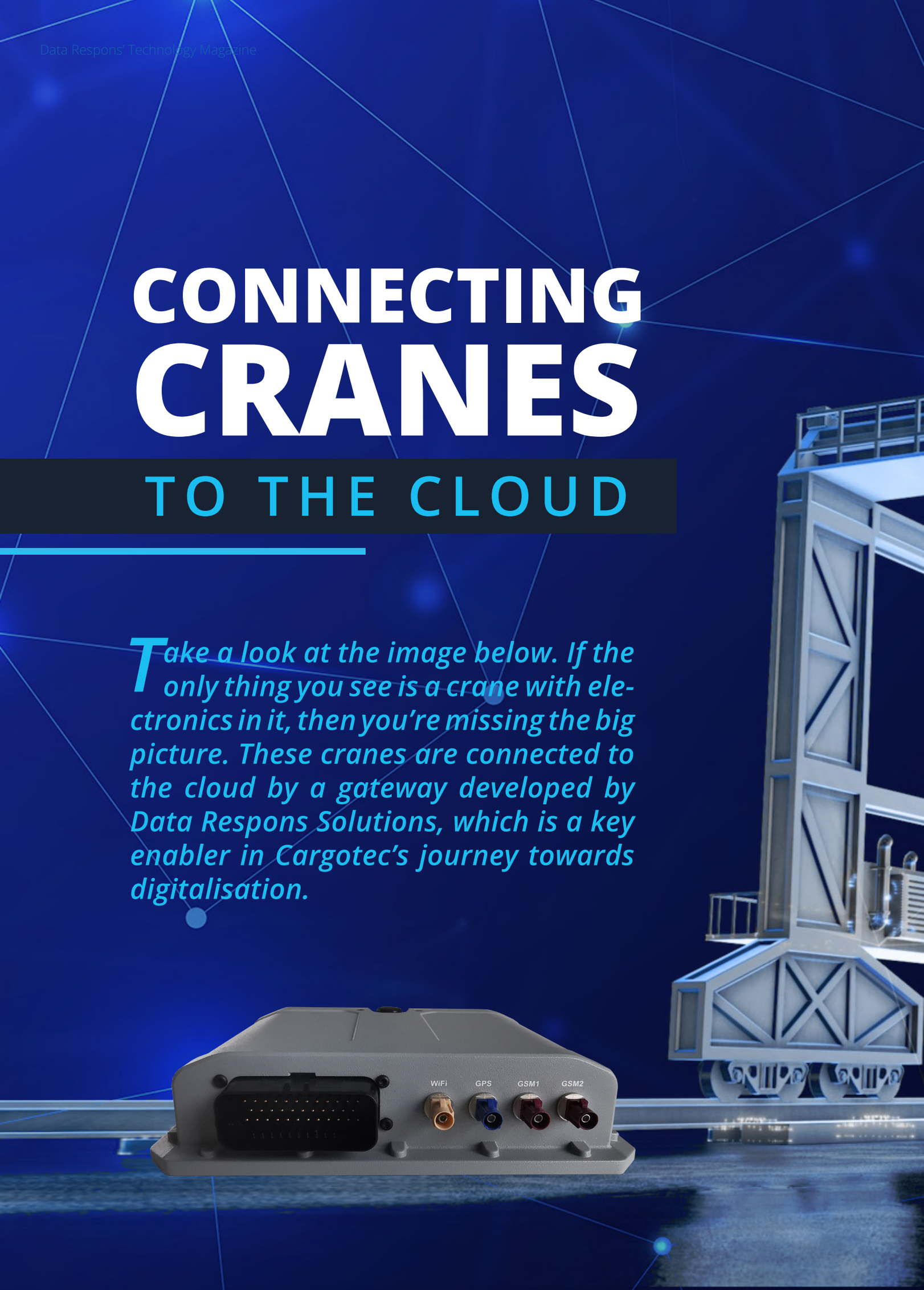
Sources:

The only external sources used in thus information was publicly available information, including reports and consultations from the Norwegian Defence Research Establishment (FFI), Norwegian Defence Logistics Organisation (NDLO) and National Communication Authority (NKOM), as well as information available on the web from NATO, Telenor, Defence systems and Wikipedia.

CONNECTING CRANES

TO THE CLOUD

Take a look at the image below. If the only thing you see is a crane with electronics in it, then you're missing the big picture. These cranes are connected to the cloud by a gateway developed by Data Respons Solutions, which is a key enabler in Cargotec's journey towards digitalisation.



BY: Arne Vollertsen for Data Respons

Cargotec is one of the world's leading providers of cargo and load handling solutions. Cargotec and its business areas Kalmar, Hiab and MacGregor are well known in the cargo and load handling industry with their products, services and solutions that support their customers in ports, at sea and on roads.

While Cargotec enables smarter cargo flow with its leading cargo handling solutions and services, it also embraces industry trends like automation, robotics, electrification, and other business activities that are closely connected to digitalisation.

Connectivity is king

In all of this, connectivity is a fundamental prerequisite. Being able to connect and communicate all equipment in ports, on ships and on trucks is essential – regardless of where they might be located. Only then can the next step be taken to design new services and open new revenue streams from remote monitoring, smart services, predictive maintenance etc.
Across all brands

This is where the box comes in. Cargotec turned to Data Respons for expert knowledge and engineering expertise in how to connect its equipment – and almost all of it across the entire range of Cargotec brands.

Anders Jansson, Sales Director Data Respons Solutions Sweden elaborates:

– Initially Cargotec asked us to design a standard gateway to connect the truck cranes manufactured under their Hiab brand. While we were preparing that project, Cargotec continued further in focusing more strongly on digitalisation. That decision allowed us to broaden the scope and build a gateway to fit nearly all products across all Cargotec brands. We've designed all the hardware and a large part of the software of the Cargotec Gateway.

Robust and versatile

Its model name is CE-IMX6-01 and with it Data Respons has taken gateway versatility and robustness to the extreme – as required by the customer.

The sturdiness of the device is remarkable. It is built to take a severe beating, withstand a pressure washer, and resist salt spray. Furthermore, it has an operating temperature range from -40 to +80 degrees Celsius, all of this to enable it to function under extreme conditions.

On top of that, the Cargotec Gateway is multi-lingual in various ways. It speaks a number of tech languages: it can communicate via Bluetooth, wifi, ethernet, and has a 4G modem for connecting to cellular networks. Also, it can connect from nearly any location around the world.

The gateway has been certified for more than 45 regions and connects to a telecom network via an e-SIM card, a dedicated chip with the same functionality as a conventional physical SIM card.

IoT ecosystem

But ruggedness and global connectivity are by far not the only features that make the gateway a major achievement in the Cargotec journey towards industrial digitalisation. Without being able to fit into the Cargotec IoT ecosystem, it wouldn't be worth much, and in this respect Data Respons has taken the role of Cargotec's development partner with also other responsibilities than the design of the gateway.

Image: Cargotec

Hans Christian Lønstad, CTO of Data Respons Solutions explains:

– We've worked closely together with Cargotec engineers and data specialists to find the optimal technical solutions, all the way from crane to cloud. We've worked with Cargotec on a number of issues well beyond technical issues related to the gateway. Together we've developed an understanding of how to combine hardware and software on different levels to make the IoT ecosystem work as a whole. We've been involved – and still are – as advisors on how the entire system should behave technically to be able to live up to the long-term plans and visions of Cargotec in regards to IoT.

Holistic approach

According to Hans Christian Lønstad, this holistic approach has been key to the successful development of the CE-IMX6-01 Gateway, demonstrated by its large production volume.

The overall goal is to handle the increasing cargo volumes crisscrossing our globe with as little environmental impact as possible. And since Cargotec is serving industries that cover the majority of the world's gross domestic product, this can make a huge difference.

The Cargotec digitalisation vision

Image: Cargotec

Tuomas Martinkallio, Director, Digitalisation, Kalmar Mobile Solutions:

– Digitalisation is one of Cargotec strategic must-win battles. Our target has been to achieve full connectivity for the equipment we manufacture, across all Cargotec brands. And that's what we've achieved. Digitalisation is one of the key initiatives at Cargotec, and currently connectivity is available for 99 percent of our equipment.

– Digitalisation enables new business models and service offerings, and our goal is that 40 percent of our net sales should come from software and service. Connectivity is a key tool in introducing new kinds of digital products to our customers, so that we can enhance their operations and safety. What we aim to do is to offer new kinds of services to the market. We want to develop real business on top of connectivity and data. Connectivity is nice, but it is not a value in itself. The magic happens when we can add value based on the data.

– For instance, Hiab has developed HiConnect, which offers equipment owners real-time data about their equipment's operation and condition. Kalmar has Kalmar Insight, a performance management tool for cargo handling operations.

– The Cargotec Gateway is the crucial element here. We needed a flexible gateway that could fit nearly all our products, as well as cope with harsh environments, and connect globally. Also, it had to be cost-effective. And as we are market leaders, it had to meet the same high quality standards as our basic products.

– The businesses under the Cargotec umbrella are quite diverse. That means we sometimes have needs that are totally opposite from each other. First of all we needed a partner that could understand our need for flexibility and that could provide us with the right technical solution for it. That is why we chose Data Respons.

– With the technical infrastructure in place we are now working with the data we are collecting. We utilize the data to do analytics and to add more value to it. We really feel the data is valuable, and we are getting a good understanding of what is happening with our equipment. In that part we're really strong, in my opinion. When we combine our R&D understanding with the actual operational data we can really create good value for our customers.