SMART INDUSTRY

powered by AVNET SILICA

The IoT Business Magazine

7.50 EUR | 2021

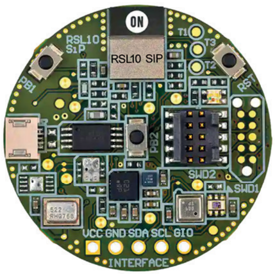
PRECISION FISHING

THE FUTURE OF MAKING
Predictive Manufacturing

THE END OF CABLES
Intelligent Power Transmission

IN FROM THE COLD
Smart Utilities

EU CYBERSECURITY ACT
MAKING THE WORLD SAFE FOR IOT


ON
RSL10 SIP
SWD2
SWD1
VCC GND SDA SCL GIO
INTERFACE

EUROPE LEADS THE WAY

Tim Cole
is the editor of *Smart Industry – the IoT Business Magazine*. His latest book, *AI Means Business*, is available from Amazon.

The world of tech in divided today into two giant blocs that determine where the ship is headed and who profits most. As in many other areas, the United States and China seem locked in an epic struggle for predominance, and IoT strongly feels the effects. So, what role does – or can – tiny Europe play, crushed between these two titans? Maybe a bigger one than many believe.

Take the EU Cybersecurity Act (CSA), which author Stian Overdahl dissects in detail in the title story of this issue. For the very first time, it establishes common standards for the safety and security of computers, networks, and software that are binding, at least within the territory of the European Union.

Trade is now so deeply interlinked that a single cargo ship stuck in the Suez Canal can cause the complete disruption of global supply chains. Europe is, in effect, causing a similar chain reaction by establishing standards that the rest of the world must follow. The fact that the European Union is the second-largest economy in the world and that trade within the Union accounts for more than one-third of the world total means that, as a bloc, Europe boxes far above its weight in terms of global power.

What Europe says goes in many areas. Think of the much-maligned General Data Protection Regulation (GDPR), which is, by far, the toughest privacy law in the world. Though it was drafted and passed by the European Union, it imposes obligations on companies and organizations everywhere that target or collect data relating to Europeans.

The same will go for the evolving body of laws and regulations on cybersecurity. The ISO Common Criteria, a standardized framework with which computer companies can specify their security targets in terms of functional security and assurance requirements, Europe accounted for 1,612 such schemes, the US only 67 – and China doesn't even show up. Ignorance is no excuse and even Chinese manufacturers will have to follow Europe's lead, especially if the currently voluntary CSA rules become mandatory. Talk in Brussels indicates that this will happen sooner rather than later.

The trend is clear – hackers and cybercriminals aren't going to let off exploiting what is an increasingly lucrative activity, especially as technologies such as artificial intelligence make it even easier for them to mount mass attacks and deploy more effective methods.

And despite moves by legislators to introduce standards that are consistent across the bloc, companies themselves need to step up and to take responsibility for their own network security. That requires more investment by private companies – both in ensuring that their technology is up to date, but also in training staff and engaging with specialist service providers such as cyber risk insurers.

The alternatives – such as in the case of Pilz Automation, who are interviewed in this edition – are not worth contemplating.

Europe also needs to build momentum in this space when it comes to innovation. There is the crucial issue of a "brain drain" of skilled workers. For years, many specialists have relocated to the US to complete research or fill lucrative roles working for Big Tech.

Complementing the regulatory overhaul in the EU is a ramp-up in spending and investments, including a network of security operation centers to monitor and anticipate network attacks, a major new European Cybersecurity Competence Center, expected to be located in Bucharest, and even deployment of a secure quantum communication infrastructure (QCI).

Nevertheless, it remains to be seen how effective such measures will be, and whether the EU will emerge a trailblazer – or if it's just playing catch-up.

CONTENTS

03 Editorial
04 Contents/Imprint
06 Avnet Centennial: 100 Years of Making History
14 Smart People

SMART BUSINESS

16 The EU Cybersecurity Act:
Making the World a Safer Place
28 How to Build Your Own Campus Network with 5G
32 The Great IoT Connectivity Lockdown
34 The Future of Making – Making the Future
40 Addressing the Identity Crisis in IoT
44 Smart Utilities: Coming In from the Cold

SMART COMMUNICATIONS

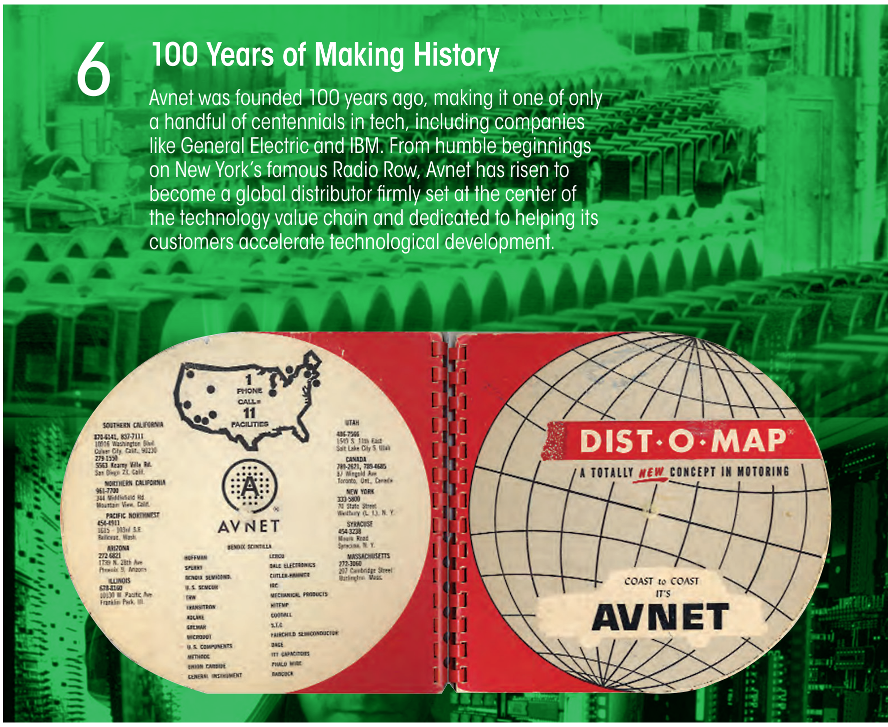
48 Disaster Prevention: Weather or Not?
52 Maritime IoT: A Sea of Data
56 Sustainable Investment: IoT for Good

SMART LIFESTYLE

62 Building Technology: Giving IoT a Lift
66 Precision Fishing: Net Benefits
70 Robotic Floor Care: Cleaning Up after Covid
72 Interview: The King of Kegs

SMART SOLUTIONS

74 Wireless Power: The End of Cables
78 ICS Vulnerabilities: No Lockdown for ICS Hackers
80 Bernd Schöne: Beware of Backdoors!
82 Avnet Column: Security from the Get-Go
84 Smart Sensors: Hot Stuff
88 Smart Companies
92 Smart Products
98 Gerd Leonhard: Science Fiction or Science Fact?



6

100 Years of Making History

Avnet was founded 100 years ago, making it one of only a handful of centennials in tech, including companies like General Electric and IBM. From humble beginnings on New York's famous Radio Row, Avnet has risen to become a global distributor firmly set at the center of the technology value chain and dedicated to helping its customers accelerate technological development.

34

The Future of Making – Making the Future

Predictive maintenance, using IoT to anticipate and prevent breakdowns by collecting and analyzing machine data, has been gaining momentum in recent years. Based on its successes, some innovators are applying the same kind of thinking to entire manufacturing operations and are even aiming to tie in visibility on the supply and demand sides.

62

Giving IoT a Lift

The global elevator market was $82.29 billion in 2020 and is expected to grow at an annual rate of 2.5 percent by 2027. However, the basic technology has hardly changed within the last 100 years. Now, a new generation of smart lifts promises to take IoT to new heights.

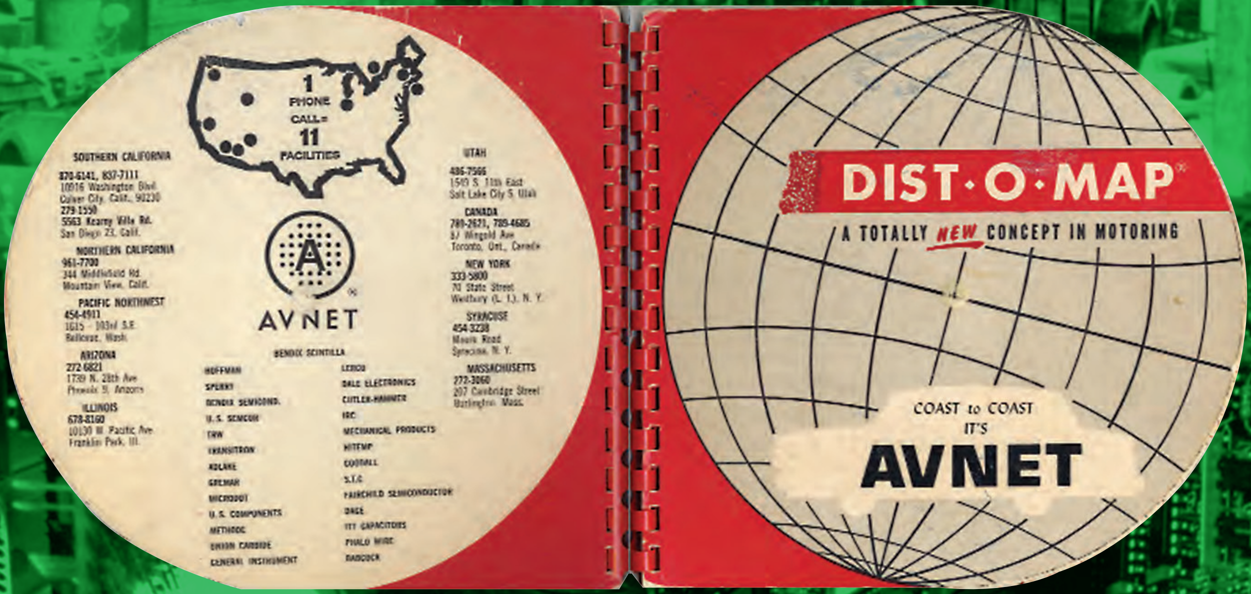
16 Making the World a Safer Place

Policy makers all over the world are scrambling to ensure that there are adequate rules and regulations to protect them – but the EU seems to have a head start. The EU Cybersecurity Act is intended to make networks, computers, and software safer, but there are also concerns it will add costs and administrative burdens for businesses – or even create confusion and ambiguity.

IMPRINT

Publisher
Avnet Silica (Avnet EMG GmbH), Gruberstrasse 60d,
85586 Poing, Germany
Production and Project Management
RSP Management GmbH, Hohenbrunner Weg 41B,
82024 Taufkirchen, rspitz@rsp-publishing.de
pmc active GmbH, Bretonischer Ring 10, 85630 Grasbrunn
Tel. +49-89-454-557-728, Fax +49-89-4545-5770
Project manager Richard Spitz
Editor-in-chief Tim Cole
Text editor Eric Doyle
Art director Sara D'Auria, www.inframedesign.de,
Harald Sayffaerth, www.01graphics.de
Contributors Martin Milter Bay, Heinz-Paul Bonn,
Marc McCoy, Alan Earls, Gordon Feller, Chen Fradkin,
Martin Grossen, Gerhard Kafka, Bee Hayes-Thakore,
Gerd Leonhard, Michael Moorfield, Stian Overdahl,
Bernd Schöne, Oliver Schonscheck, Rainer Claassen
Pictures Shutterstock, Fotolia
Production manager Stephan Quinkertz
Printing Westermann
Managing director Richard Spitz, Stephan Quinkertz,
Alan Markovic

TRUSTED SOLUTIONS FOR YOUR DESIGN CHALLENGES
Extensive library of reference designs architected to accelerate your designs and get to market faster
Analog + Power + Embedded Processing
Visit renesas.com/win for more details
BIG IDEAS FOR EVERY SPACE
RENESAS



1 PHONE CALL= 11 FACILITIES

SOUTHERN CALIFORNIA
870-6141, 837-7111
10916 Washington Blvd.
Culver City, Calif., 90230
279-1550
5563 Kearny Villa Rd.
San Diego 23, Calif.

NORTHERN CALIFORNIA
961-7700
344 Middlefield Rd.
Mountain View, Calif.

PACIFIC NORTHWEST
454-4911
1615 - 103rd S.E.
Bellevue, Wash.

ARIZONA
272-6821
1739 N. 28th Ave
Phoenix 9, Arizona

ILLINOIS
678-8160
10130 W. Pacific Ave
Franklin Park, Ill.

AVNET

BENDIX SCINTILLA

HOFFMAN
SPERRY
BENDIX SEMICOND.
U.S. SEMCOR
TRW
TRANSITRON
ADLAKE
GREMAR
MICRODOT
U.S. COMPONENTS
METHODE
UNION CARBIDE
GENERAL INSTRUMENT

LEDCO
DALE ELECTRONICS
CUTLER-HAMMER
IRC
MECHANICAL PRODUCTS
HITEMP
CODITALL
S.T.C
FAIRCHILD SEMICONDUCTOR
DAGE
ITT CAPACITORS
PHALO WIRE
BABCOCK

UTAH
486-7566
1510 S. 11th East
Salt Lake City 5 Utah

CANADA
789-2621, 789-4685
87 Wingold Ave
Toronto, Ont., Canada

NEW YORK
333-5800
70 State Street
Westbury (L. I.), N. Y.

SYRACUSE
454-3238
Moore Road
Syracuse, N. Y.

MASSACHUSETTS
272-3060
207 Cambridge Street
Burlington Mass.

DIST·O·MAP®

A TOTALLY NEW CONCEPT IN MOTORING

COAST to COAST IT'S AVNET

Avnet Centennial

100 YEARS OF MAKING HISTORY

Avnet, a Fortune 200 company, was founded 100 years ago, making it one of only a handful of centennials in tech, including companies like General Electric and IBM. **From humble beginnings on New York's famous Radio Row, Avnet has risen to become a global distributor** firmly set at the center of the technology value chain and dedicated to helping its customers accelerate technological development. Join us here on a trip down memory lane.

By Tim Cole

Family Reunion

The Avnet family gathers for a wedding reception. Clockwise from top left: Robert Avnet and his wife, Maxine; Joan Avnet and her husband, Lester; Norman and Roz; Helen Avnet and her husband, Charles.

It was the early 1920s. With World War I a memory, New York City's docks were awash in surplus military and ship-to-shore radio parts.

Amateur (ham) radio enthusiasts, intrigued by what they read in popular magazines like *Modern Electronics*, were putting together crystal set devices, "cat whiskers," of their own from kits. The market for radio components was heating up.

Into this nascent industry came Charles Avnet, a 33-year-old Russian immigrant. He began buying and selling surplus radio parts in 1921, just as the first component stores opened for business on New York City's Radio Row. Rapid advances in technology soon made radios a common sight in American homes. The Consumer Electronics Association reports that in 1922, 100,000 radios were sold at an average cost of $50. By 1924, the annual factory dollar volume had multiplied tenfold to $50 million, and there were more than 500 commercial radio stations broadcasting nationwide.

The Golden Age of Radio was in full swing, and Charles found himself at the heart of it. As radio manufacturing grew, so did the role of parts distributors. From a small store in Manhattan, Charles sold about $85,000 in components his first year in business. When the Great Depression hit in October 1929, Charles, like many others, suddenly found himself in debt. In what would prove an astute decision, he shifted his focus from retailing to wholesaling. Radio remained an inexpensive escape for many. The newest novelty, television sets, were making inroads into people's homes. Charles dealt in parts applicable to both. Not only did he pay off all his debts, he realized a modest profit. By making good on his loans, he was build- ➔

Do it Yourself

Before World War II, Lester Avnet became convinced that electric connectors were the future, so he set up his own manufacturing plant on North Moore Street in New York's butter and egg district.

Avnet and the Golden Age of Radio

A NEW MEDIUM IS BORN

In 1901, Guglielmo Marconi's Wireless Telegraph and Signal Co. received the Morse code letter "S" transmitted to Canada from England. The first wireless signal to cross the Atlantic Ocean, it relied in part on a diode vacuum tube created by John Fleming. In 1906, Reginald Fessenden broadcast a Christmas Eve selection of music and stories to ships with receivers off the Atlantic coast. An amplifying vacuum tube, the audion tube, was invented in 1912 by Lee DeForest and was the essential component in what would come to be known as "radio," a word with its etymological roots in "radiated signals." Peter Jensen came up with an idea for hi-fidelity, or amplifying, speakers in 1915, calling his company Magnavox, Latin for "great voice." By this time, people all over the country were tinkering with radio kits. By the end of the 1930s, 20 percent of all cars had factory-installed radios. Governments had established untold numbers of official stations and networks on almost every continent, their citizens even more. From this time KDKA until World War II began — the Golden Age of Radio — more than 100 million radio receivers had been sold.

ing a reputation of business acumen and honesty that would serve his eponymous company well.

Electronic components became priority defense items as the United States geared up for World War II. Home radio set manufacturing was banned. Component distributors like Charles Avnet turned their full attention to satisfying military and government requests. He opened his first major manufacturing facility on North Moore Street in New York's butter and egg district in 1944 to assemble military antennas. His son Lester soon persuaded him the future belonged to electrical connectors, which almost every electronic device required.

When the war ended in 1945, high-quality military surplus was available for less than one-tenth its original cost. The Avnets stocked up. Once they established a team of trained sales engineers, they began manufacturing connectors of their own as well.

The onset of the Korean Conflict in 1950 boosted the fortunes of those with the right inventory of components for military and government use in missile systems, airplanes, and other applications. Bell Labs' invention of the transistor in 1947 was already fueling an electronics revolution, and the US/Soviet Union space race and international arms race would send the industry into high gear.

California Dreaming

Ten years after World War II ended, Charles, Lester, and his brother, Robert, had a thriving business assembling connectors to customers' specifications. They incorporated in 1955 as Avnet Electronic Supply Co. with Robert as chairman of the board and Lester as president. Charles took on the roles of vice president and treasurer. In 1956, increasing business necessitated the opening of a facility in Los Angeles to provide more convenient and faster service to the aviation and missile industries, and Robert relocated there. To fund expansion and corner the market on connectors, Avnet celebrated the close of the decade by going public. The company was listed on the American Stock Exchange with the issuance of 175,000 shares of common stock under the symbol AVT.

The invention of the microprocessor and the relationship Avnet forged with its inventor, Intel, and semiconductor suppliers AMD, Fairchild Semiconductor, Motorola, National Semiconductor, RCA, and Signetics contributed greatly to the company's vigor. Avnet was the first technology distributor to place an order with Intel in 1969. When Intel released the microprocessor it returned the favor, giving Avnet access to related software development and demonstration tools to sell to engineers for their microcomputers – a very profitable venture.

The company commenced the decade not only with an expanded portfolio of semiconductors and other components, but with the first of many unconventional acquisitions, audio equipment maestro British Industries Corp. (BIC). BIC was just the first in a string of acquisitions that would turn Avnet from a components distributor and manufacturer into a company with expertise in an array of goods, from microprocessors and die casting machines to guitars, perfume bottles, jumper cables, and television antennas. The company described in 1960 as one of the leading national marketers of electronic products would find Electronic Marketing merely one of five groups by the mid-1970s.

An Eye for Art

The Joan and Lester Avnet Collection at New York City's Museum of Modern Art is a world-class compilation of drawings from some of the most important artists of the 19th and 20th centuries.

Although he made a name for himself in the business world, Lester Avnet was a Renaissance man at heart with a long-standing interest in the arts. As a boy, he would stand outside his father's store singing opera to entice customers in the door. As his family's company grew, he purchased drawings to foster the creation of a collection devoted specifically to the medium that captured his imagination – drawing. The Avnets donated 180 works to the museum overall, the largest gift of drawings it ever received. The collection features works by Matisse, Chagall, Mondrian, Modigliani, Kandinsky, Braque, Pollock, and Rothko. In 1971, just one year after his death, the museum opened its Department of Drawings devoted to works on paper, most of them donations by the Avnet family.

Up and Up!

Avnet added semiconductor programming and inventory management solutions to its offerings. Going from zero to 5 billion dollars in only 27 years, Avnet Technology Solutions began an upward spiral that continues to this day.

Pruning Back

Convinced Avnet's future would be in the field from whence it arose – technology distribution – Tony Hamilton, named CEO in 1980, began a divestiture process, pruning sluggish divisions and product lines and replacing them with technology-related acquisitions and products with high growth potential. The Electronic Marketing Group was already the leading US distributor for semiconductors, connectors, computer products, and passive components, and in many cases it was the single-largest customer of each of its suppliers.

By 1988, computer product sales were so successful that, when ➔

Where It All Began

WELCOME TO RADIO ROW!

The end of World War I ushered in the joyful noise of the Roaring Twenties and the Jazz Age, a raucous decade of flapper-fueled Charlestons, crooners' sentimental ballads, the sizzling bands of Harlem, and the first notes from swing and big band music pioneers like Benny Goodman and Count Basie.

Into this heady atmosphere the first affordable, mass-produced consumer radios were introduced, expanding the technology beyond the realm of hobbyists. In and around America's East Coast harbors a brisk trade in radio components blossomed. Just a few strides from the docks of New York City's Lower Manhattan was Cortlandt Street, soon christened "Radio Row."

By the 1960s, Radio Row encompassed six blocks, its milieu an exuberant, cacophonous din of music and street sounds as vibrant as the city itself. More than 300 stores lined its streets – for four decades, the largest collection of radio and electronics stores in the world.

It was, as *The New York Times* called it, "a paradise for electronic tinkerers." In 1966, a two-year battle royal for the soul of Cortlandt Street came to an end when the New York Supreme Court ruled that the Port of New York Authority could condemn and bulldoze the area to make way for the twin towers of the World Trade Center. The Ajax Wrecking Company demolished the first of 26 vacant buildings in the area soon thereafter. Radio Row was silenced forever.

revenue exceeded $385 million, the company separated the business and formed the Hamilton/Avnet Computer division. Roy Vallee, who would become CEO in the late 1990s, was named division president in 1989 and the following year led the merger of Hamilton/Avnet Computer (which marketed primarily to manufacturers) and Avnet Computer Technologies (which focused on end users) into a single division, Avnet Computer.

The group hit $1 billion in sales in 1997 and established a headquarters of its own in Arizona in 2000. The acquisition of Savoir Technology in 2000 made Avnet the world's largest distributor of IBM mid-range computer products. Now called Avnet Technology Solutions, it has evolved into a purveyor of services and solutions for resellers, manufacturers, integrators, and end users. Strong leadership, consistency, focus, and a successful business model have built what started as a side business into one of the best computer businesses in the distribution industry.

In the late '80s and early '90s, Avnet under its new chairman and CEO Leon Machiz began a spate of acquisitions that would turn it into a global technology distribution leader.

The purchase of the Access Group, a UK semiconductor distributor, in 1991, and two other semiconductor specialists, France's FHTec Composants and Scandinavia's Nortec, secured a place in three of Europe's five largest markets. Avnet went on to acquire companies in Italy, Ireland, Germany, and the Netherlands, along with a number of pan-European distributors. The crown jewel was the 2000 acquisition of RKE Systems and Europe's leading semiconductor distributor, the EBV Group (EBV Elektronik and WBC). Part of Germany's VEBA Electronics Distribution Group of companies, the deal was unprecedented in that Avnet and its number one rival, Arrow Electronics, cooperated on the purchase – Arrow took a North

A Little Help from Our Friends

Avnet's acquisition of Guild Musical Instruments in 1965 was one of many in the consumer products market. An Avnet/Guild vice president presents a Guild Starfire 12 to The Beatles' John Lennon and George Harrison.

American subsidiary – to further consolidate the industry.

Avnet Design Services (ADS), established in 1997, grew out of a simple customer request in New Zealand for an Avnet engineer to help design a new product. Now its customers are a Who's Who of cutting-edge companies, including General Dynamics, Emulex, and Garmin. ADS provides engineers with technical advice on component, hardware, and software solutions, design and prototype services, and test and production assistance. The goal: get customers' new products to market faster.

The company had been circling around the idea of value-based management since the late 1990s. Quite simply, people need a significant amount of value added to many products before they can buy and use them. In Avnet's case, that means helping companies with everything from engineering expertise as new ideas come to life to tech support long after products have been manufactured and purchased, not to mention financing, programming, marketing, integrating, and yes, even distributing technology products.

When it comes to designing products, Avnet's total-systems approach helps manufacturers integrate technology from component suppliers like Intel, Marvell, Maxim Integrated, Microchip, Micron, NXP, ON Semiconductor, Renesas, STMicroelectronics, and Xilinx. Avnet has nine design centers in five countries: China, India, Israel, Singapore, and the United States. Manufacturers rely on Avnet engineers to help them analyze and choose the best component solutions from among the vast array available. Avnet's engineers also integrate components from multiple suppliers into reference and evaluation kits that solve real-world problems.

> ” In a global economy, business migrates to the most efficient provider. We intend to be that provider.
>
> **Roy Vallee**
>
> Chairman and CEO of Avnet (1998–2011)

Avnet's innovative culture and entrepreneurial spirit, coupled with its commitment to customer service excellence and its strong business relationships, have assured partners they have chosen well. The company's global scope and economies of scale, talented people, and focus on value-based management ensure that it will continue to be a leader in the technology industry. Welcome to Avnet's value creation era!

The Men Who Built Avnet

Charles Avnet, Founder; President 1921–1955

Charles Avnet, a 33-year-old Russian immigrant, opened a small store on New York City's Radio Row. From his store in Manhattan, Charles sold about $85,000 in components his first year in business. In 1929, Galvin Manufacturing Co. introduced the first practical car radio, the Motorola, short for "motor Victrola." Charles capitalized on this development, adding automobile antenna assembly and kits to his repertoire and effectively moving from a standard distributor to a value-added distributor putting parts together for sale to consumers.

Lester Avnet, President, 1955–1967; Chairman 1964–1969

Despite the many interests and talents that could have steered him away from the family business, the electronics industry was his destiny, and he poured his considerable enthusiasm into it. He was an expert on electrical connectors, extremely knowledgeable about foundry practice and metallurgy, and was known for bringing children to annual meetings to share his passion about business.

Robert Avnet, Chairman 1955–1964

With the support of his brother Lester, Robert Avnet presided over one of the most dynamic periods in the company's history. Not only did Avnet more than double the number of assembly plants and sales engineering/service locations by 1964, but it underwent a metamorphosis from a business devoted to electrical connectors to a holding company with interests ranging from electronic components to record albums. Robert inspected radio receivers as a captain in the US Army Signal Corps during World War II. He was also a founder of the Albert Einstein College of Medicine.

Interview Phil Gallagher, CEO of Avnet

source ©: Avnet, Inc.

A Great Start

Avnet has come a long way in the past century from a small shop selling radio parts to a global distributor and a Fortune 200 company. How did it get here and where is it heading?

Avnet was formed in 1921 when the US government lifted its ban on private radio, prompting Charles Avnet, a 33-year-old immigrant fresh from Russia, to begin buying and selling surplus radio parts on Manhattan's Radio Row. Then came antennas, connectors, and something epochal: calculating machines. Equipped with vacuum tubes adapted from radio, these computers, Charles proclaimed at the time, would alter human history forever – and he was right.

I've been with Avnet for 39 of the company's 100 years, and its people exemplify what's enabled the company to withstand all of that change: adaptability, resilience, and perseverance. We're still here because we've embarked on a continuous transformation alongside the ever-evolving technology market.

And while one hundred years is an enviable run, we prefer to think of it as a great start. Today, Avnet sits squarely in the middle of the technology value chain, with expertise in components distribution and deep knowledge of the global supply chain.

> ”
> Avnet and Intel have partnered for five decades to help connect the world and enhance the way people interact with it.

Avnet was the first distributor to place a product order at Intel, which had just started producing its first microprocessor, the 4004. How has the relationship worked out?

In November 2019 we celebrated an amazing milestone with Intel leaders: 50 years of partnership! Back in 1969, Avnet (or Hamilton/Avnet) placed its first PO with Intel for $170,000. Over the past five decades, Avnet and Intel have partnered to help connect the world, and enhance the way people interact with it. Our alliance is still going strong and I am confident that a new generation of Avnet and Intel leaders will gather again to recognize future milestones.

In the mid-eighties, Avnet was the number-one US distributor in semiconductors, computers, connectors, and passive components, but you were still just a national distributor. When did globalization hit?

In 1991, Avnet began its modern era of globalization with the acquisition of the Access Group, a UK semiconductor distributor. And in 1995, Avnet entered the technology distribution market with the acquisition of Hong Kong's WKK Semiconductor. Our strategy was simple: grow organically faster than the markets we serve, and augment that growth with value-creating mergers and acquisitions. We have made small acquisitions as well as some of the largest in industry history. Each has enhanced our product or geographic portfolio while adding critical talented employees.

Today we operate in over 140 countries, with over 125 locations supporting over two million customers with 15,000+ employees. Avnet is always evaluating the needs of our customers and expanding into new areas as the market demands.

How is Avnet helping customers and suppliers build solutions to meet some of the fastest-growing demands in the marketplace, like connected IoT devices and automotive solutions?

As connectivity is built in to more and more of the technology we rely on, we are once again at a point of transformation for our industry, our suppliers, our customers, and of course for Avnet. Everyone's focused on understanding how to build connected capabilities into their existing and new products, and Avnet is enabling both our suppliers and customers to succeed in this effort. We offer comprehensive solutions both above and below the cloud, thanks to the talented teams we've onboarded through several acquisitions in recent years. We now help companies around the world with engineering expertise, financing, product enhancements, marketing, and system integration, in addition to the physical distribution of technology products.

More specifically, in the automotive industry, there are more electronic devices than ever before for applications such as instrumentation and infotainment to cameras, radar, and lidar. The speed at which electrification is accelerating is amazing. To support our customers, whether it be a reference design, total ADAS (advanced driver-assistance system) solution, or complex global supply chain need, Avnet has put in place global design and supply chain teams with expertise in the automotive industry to help get designs to market quickly and efficiently.

Fundamentally, across many verticals, we act as an extension of our customers' teams. They can leverage our deep technical and supply chain expertise throughout the product life cycle to maximize their return on investment. Companies turn to Avnet for two simple reasons: we save them money and help them grow faster, thereby accelerating their success.

The Avnet Silica division is one European semiconductor specialist of Avnet, Inc., and acts as the smart connection between customers and suppliers. Selling components is only part of your business, right?

Avnet Silica is the European semiconductor specialist division of Avnet, one of the leading global technology distributors, and acts as the smart connection between customers and suppliers. The distributor simplifies complexity by providing creative solutions, technology, and logistics support. Avnet Silica is a partner of leading semiconductor manufacturers and innovative solution providers over many years. With a team of more than 200 application engineers and technical specialists, Avnet Silica supports projects all the way from the idea to the concept to production.

Currently we're redefining our strategy and structure to be an even more efficient organization. Our goal is to deliver for all stakeholders as technology and supply chains rapidly change. Our customers rely on us to help them stay nimble in the face of future volatility or even shocks like the pandemic. We are streamlining the business and getting emerging businesses like IoT and Avnet Integrated to drive demand for our supplier partners to accelerate higher-margin growth.

Avnet is deeply involved with Microsoft and their IoT offering especially around Azure. What about your own offering, IoT Connect, which leverages Microsoft's Azure hybrid cloud computing service?

Avnet's IoTConnect platform is a cloud-based platform, powered by Microsoft Azure, and it's highly scalable to address common industry needs and challenges. The platform provides pre-built market-specific applications for quick solution development and data services to deliver customer insights and impactful ROI. In addition, it offers the security of IoTConnect-certified plug and play devices to simplify solution design. Plus, Avnet's IoTConnect Partner Program enables system integrators and OEMs to accelerate and scale their IoT solution development by developing new device solutions and service models on the platform. With a standardized way to harness IoT and access to Avnet's extensive suite of experts, developers can quickly build smart apps and solutions.

> ”
> IoT can bring tremendous benefits, but with them come risks and responsibility to keep them reliable and secure.

Security is critical – but are IoT solution providers addressing this problem adequately?

While IoT was a driving force in the wave of technological change a decade ago, security has been its greatest adversary. Avnet is working to ensure its customers' IoT deployment will be stronger, more successful, and most importantly more secure. When thinking about IoT today and in the future, there are a lot of "nice to haves." Security is not one of them. It needs to be built into IoT solutions from the ground up, across both hardware and software. We've seen how IoT can bring tremendous innovation and benefits to individuals, organizations, and societies. But with those benefits come both the risks and the responsibility to keep those systems reliable and secure. To do that we're going to need to think, act, and invest differently.

Has the pandemic accelerated the IoT?

With the majority of people working remotely because of the pandemic, we want to be more connected than ever. The Internet of Things is becoming more intelligent, immediate, and interoperable. We are creating a world where everything that should be connected to the Internet is connected. Like the smartphone app economy, the Internet of Things is simply becoming part of life and business as we know it.

Behind the Scenes

SMART PEOPLE

All over the world, brilliant individuals are hard at work creating the technologies and solutions that will one day **make the Internet of Things come alive.** We visited a few of them and listened to their fascinating stories.

Mohamed Dhaouafi of Cure Bionics

Reaching Out to Amputees

At a student competition four years ago, Mohamed Dhaouafi, a Tunisian engineering student, learned that a teammate's cousin had been born without arms but couldn't afford a prosthesis. The memory wouldn't leave him alone. When he was looking for a project with social relevance, he discovered that many people were in the same situation. Dhaouafi formed a team to develop a functional but cost-effective prosthetic arm.

The World Health Organization (WHO) estimates there are about 30 million amputees worldwide and in poor countries most of them cannot afford prostheses. It's even worse for children and young people, who usually need replacements every year because they are still growing. Even an inexpensive prosthetic arm costs about $10,000.

Without an assistive device, amputees remain restricted in their freedom of movement and often suffer from social stigma that prevents them from attending school. Many of them, therefore, remain unemployed for life. In addition, many prostheses are too heavy or the wrist can't be rotated, or they have only three fingers. Dhaouafi's team developed a solar-rechargeable model arm, with a manually rotatable wrist and five fingers, that costs only $2,000. He founded his own company, Cure Bionics, to produce and market the prostheses, which are 3D-printed in lightweight plastic.

> Going out on a limb to help the disabled in Africa, the Middle East, and beyond.
>
> **Mohamed Dhaouafi**
> Founder of Cure Bionics

source ©: The Tony Elumelu Foundation

Two sensors in the arm's socket detect electrical activity of the muscles just under the skin. Users learn to tense the muscles in a specific way and an AI algorithm translates the signals into three grips: enclosing an object, gripping with an extended index finger (for example, to operate a smartphone or computer keyboard), and a three-finger hold. Actuators move the fingers via fine wires.

Initially, Cure offers three different sizes that grow with the user via adjustable cuffs. To train users, the team has developed a virtual reality (VR) application where a user can learn to control a virtual arm in an entertaining simulation viewed through VR glasses.

Dhaouafi hopes to be able to help people throughout Africa, the Middle East, and beyond. Next, he plans to develop artificial legs and he hopes to develop an exoskeleton that can help in rehabilitation after an accident.

Ivan Ndip at Fraunhofer Institute

Fraunhofer Urges Early Start for 6G

The starting gun for the next generation of mobile communications has already been fired. "With 6G, we have the ambitious goal of achieving a terabit per second and a latency of about 100 microseconds – that is, 50 times the data rate and one tenth the latency of 5G," says Ivan Ndip, an expert in antennas and radio frequency systems at the Fraunhofer Institute for Reliability and Micro-integration (IZM) in Berlin. 5G currently yields data rates of up to 20 gigabits per second at a latency of around one millisecond.

Ndip and other experts are convinced that many areas of Industry 4.0, such as medicine, autonomous driving, smart cities, and entertainment, will benefit greatly from new 6G applications – but they also warn of new challenges.

Ndip explains the difference using the example of autonomous driving, where one of the goals is to greatly reduce the number of accidents. "Autonomous driving is primarily a collective aspect," Ndip says. "What 5G will achieve is a maximum data rate of about 20 gigabits per second. When a car is driving autonomously, it needs to communicate its position to other road users in real time, it needs to be able to measure distances and look around 360 degrees at the same time. It must also know the road very well and be able to look into the distance but, of course, also very close and very precisely.

"This requires sensors, which we are also developing at Fraunhofer IZM: a combination of radar and camera," he adds. "These sensors collect an enormous amount of data which must be shared simultaneously. But uploads and downloads also have to take place in real time. For example, city maps are downloaded in very high resolution – 20 gigabits per second is nowhere near enough for all these processes. In addition, the cars must react reliably to unexpected circumstances, with extremely little delay, autonomously. Therefore, in addition to very high data rates, very low latency is required at the same time."

source ©: Fraunhofer-Institut für Zuverlässigkeit und Mikrointegration IZM

Unfortunately, 5G does not allow infrastructures and networks to be built that simultaneously guarantee hundreds of gigabits per second and extremely low latency. Ndip does not believe that true autonomous driving will be possible with 5G. "We don't even know if the specifications we have today for 5G will be met. The necessary collective or networked intelligence doesn't yet exist. 5G doesn't allow the data rates and latency needed for this. That's why we need 6G."

Ndip believes it is important that telcos and governments are already looking at 6G today, even though it is not expected to be introduced until 2030. He says there are still many unanswered questions – such as hardware development for mobile communications above 100 GHz, as it is expected that the D-band (0.11 THz to 0.17 THz) will likely be used.

D-band frequencies have never been opened before for mobile communications, so the research and development community would have to start much earlier to address hardware and software issues for applications. Ten years before launch would be desirable, he says, to allow specifications to be established about five years before launch, giving time for trials to follow. There is still a lot of work for researchers like Ndip to do before the public can enjoy the benefits of the next generation of wireless communications.

> 50 times the data rate of 5G and one-tenth of its latency.
>
> **Ivan Ndip**
> Expert at Fraunhofer IZM

Cecilia Flores of Webee

Change Is Brewing

Camellia sinensis – the tea plant – is extremely sensitive to rainfall and soil acidity, two of a whole number of factors that affect flavor and crop value. Now, after nearly two millennia of human cultivation, experiments are underway to harness IoT to enhance growing and perhaps even harvesting of the tender leaves that billions of people consume as part of their daily routine.

For instance, Seeed Studio, a Chinese technology company, has been testing its SenseCAP, a wireless IoT sensor network. The gateways and sensors gather the environmental data at the local tea plantation, which helps growers manage the farm more efficiently. In a deployment in the high-altitude Mengding Mountain of Sichuan province in 2018, the project was predictably nicknamed IoTea...

Cecilia Flores, cofounder and head of marketing at Webee, an IoT technology supplier, says the most pressing tea cultivation challenges are fungus diseases, insect attacks, and soil acidity. One solution is a leaf wetness sensor that mimics a real leaf to understand its behavior and monitor its activity and humidity levels at all times. "This can help avoid infections by predicting the growth of fungus, improving crop spraying, and predicting unexpected events," she says. But time will tell just what these new tea leaves auger for an industry steeped in so much tradition.

> We can avoid fungus by predicting its growth with the help of IoT.
>
> **Cecilia Flores**
> cofounder of Webee

source ©: Vital Voices Global Partnership

The EU Cybersecurity Act

A PRICE WORTH PAYING

With businesses and consumers in Europe facing ever-more sophisticated cyber threats, policy makers are scrambling to ensure there are adequate regulations to help protect them. **A host of new rules should improve cybersecurity,** but some industry groups warn these will add to costs and administrative burdens and may even spawn confusion and ambiguity.

By Stian Overdahl

The scale of Europe's cybersecurity vulnerability is startling. In 2019 alone, there were almost 450 cybersecurity incidents involving European critical infrastructure, such as finance and energy companies, while healthcare organizations and professionals have been especially hard hit during the Covid-19 pandemic. Ransomware attacks are growing sharply globally with more than €10 billion paid out in 2019, a big leap from the previous year. Mariya Gabriel is European Commissioner for Innovation, Research, Culture, Education, Youth, and Sport. She has been ranked among the 50 most influential women in Europe in the field of cybersecurity. She believes that "Cyber threats have become a matter of national security. They underpin the resilience of critical infrastructure, from power plants to the banking system and online marketplaces for small businesses." According to her studies, cybercrime will cost the world €5.5 trillion by the end of 2020, up from €2.7 trillion in 2015. "This rise is due, in part, to cybercrime activity during the Covid-19 pandemic," she says. This could be the largest transfer of economic wealth in history and, if it happens, it will be more profitable than the global trade in all major illegal drugs combined.

Especially worrying, on the business front, is that European companies are considered less prepared to thwart a cyberattack than their counterparts in Asia and America. Over two-thirds of EU businesses, in particular SMEs, are considered novices when it comes to cybersecurity, according to a high-level summary by the European Commission (*The EU's Cybersecurity Strategy for the Digital Decade*).

Experts also point to a brain drain of cybersecurity professionals from Europe, especially to the United States. It was estimated that 291,000 job postings for cybersecurity positions within the EU remained unfilled in 2020. That matches the experience of Martin Giess, the CTO and co-founder of EMnify, a Germany company that offers cellular connectivity solutions to businesses ranging from logistics to industrial IoT. "[Companies in] Europe are quite a bit behind when it comes to cybersecurity," says Giess. "In North America there is more willingness to adopt new functionality and implement it."

Geiss says that typical weaknesses include companies buying off-the-shelf components and not updating default settings, or companies working in a "first or second-generation technology environment that is ten or 15 years old." Companies that have experienced some kind of attack are far more willing to invest in IT security, he adds, while those that have not tend to be more complacent.

➔

Security Is the First Cut

On the consumer front, people who worry about cybersecurity point to the massive profusion of connected devices in a market where price is often the main consideration, while many consumers lack even rudimentary knowledge about device security. That implies the onus should be on manufacturers to apply principles such as security-by-design to their products. However, tests by consumer watchdogs have revealed major vulnerabilities in children's dolls, smart watches, smart doorbells, and other intelligent home products, says Frederico Oliveira da Silva, senior legal officer at the European Consumer Organization (BEUC), an umbrella group representing the interests of national consumer groups. Risks include hackers being able to talk remotely to children, capture video, and, in the case of intercom doorbells, gain access to a property, as well as more general threats like exploiting IoT devices as part of a botnet attack.

An additional problem is a lack of EU-wide legislation has meant that consumer protection agencies have by and large been unable or reluctant to remove insecure products from the market. In the case of a doll, My Friend Cayla, widely publicized security and privacy failings did not result in an EU ban, though in Germany authorities withdrew the device in 2017 over privacy concerns.

In 2018, the General Data Protection Regulation (GDPR) was introduced, which can be used to apply heavy penalties for data breaches, but these laws are typically not intended to be used to prevent the sale of cyber-insecure products, notes Da Silva.

A Step in the Right Direction

Europe leads the way in privacy protection with its GDPR directive introduced in 2018, which applies heavy penalties, but the landmark regulation do not prevent the sale of insecure products.

> The onus should be on the manufacturers to apply security-by-design to their products.
>
> **Frederico Oliveira da Silva**
> European Consumer Organization (BEUC)

source ©: BEUC

Given the scale of the problem, it's no surprise that cybersecurity is a key focus for legislators in Brussels, with the emphasis on a number of new and updated rules designed to bolster security in business environments and for consumer IoT. These include an update for the Network and Information Systems (NIS) Directive, the EU Cybersecurity Act (enacted in 2019, though elements came into force in 2021), and a delegated act of the Radio Equipment Directive (RED), which is expected to be introduced in 2021. Certain key technology areas – cloud, 5G, and artificial intelligence – are also receiving special attention.

The result will be that those companies that have the least-developed cybersecurity profiles will have to work the hardest to meet baselines, while those with the right measures already in place are better positioned to comply. The downside is that increased security may result in higher costs across the supply chain. Giess at EMnify, which uses multi-network IoT SIM cards to connect client assets to the cloud, believes the regulatory push is driving increased focus on cybersecurity within businesses. "It definitely creates pressure on companies, and we are seeing an increased interest in our products," he says. "You can really perceive that cybersecurity is becoming a more important buying criterion for customers. It's not only about the price and the quality of the service – it's really that your products can fulfil certain security requirements."

Navigating the Rules Maze

When it comes to cybersecurity, there is no single law in the EU but a mosaic of rules and regulations. The most prominent horizonal rule for cybersecurity is the NIS Directive, covering entities within sectors considered vital for the economy and society, such as energy, transport, water, banking, financial market infrastructures, health care, and digital services.

The NIS Directive is currently being overhauled. In part, this is nec- ➔

Cybersecurity Labeling in Finland

A SURE SIGN OF SAFETY

One approach to cybersecurity for connected consumer devices is to introduce a labeling scheme to help buyers make educated choices and increase market pressure on manufacturers to meet higher standards. Finland is the first country in the EU to introduce such a scheme and it's based on the ETSI EN 303 645 standard. The program has several features; participation is voluntary but obtaining a label relies on the product being tested by a third party.

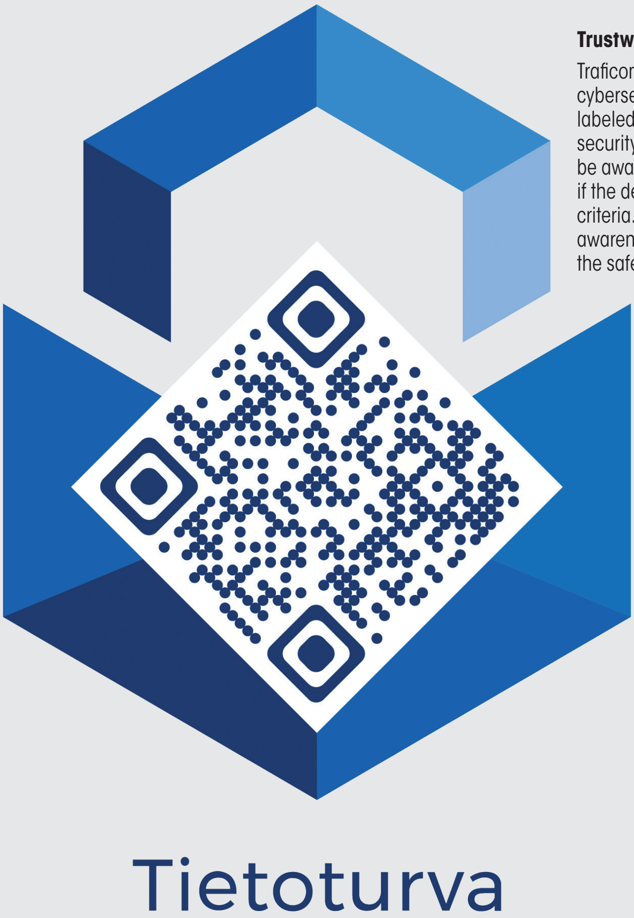
The approach has been to set the baseline requirements, using a threat model relevant to consumers, says Saana Seppänen, senior specialist at the Finnish Transport and Communications Agency (Traficom), which administers the scheme. "We want to tackle the mass attacks that come from the networks and that make it possible, for example, to create botnets or very easily endanger privacy. At the same, if you have a lightweight product which doesn't pose a great threat to the user, it doesn't make sense for it to be certified in a very heavy way, so we want to tackle the most common threats without causing unnecessary cost to companies," she says.

Over half of the people are willing to pay more for secure devices and services.

Saana Seppänen

Finnish Transport
and Communications
Agency (Traficom)

source ©: Suomidigi



source ©: Ruuvi Innovations Ltd (Oy)

Trustworthy Source

Traficom in Finland has launched a cybersecurity label that guarantees labeled devices have basic information security features built in. The label can be awarded to networking smart devices if the devices meet certain certification criteria. Traficom aims to raise consumer awareness of information security and the safe use of connected devices.

Traficom originally considered allowing companies to self-certify, as specified by the CSA, but "companies didn't find it credible and our surveys found that consumers see authorities as a trustworthy source of certification, they can trust that it means something," she explains.

When it comes to impact, Seppänen says surveys have shown that consumers in Finland are very concerned about security: "Over half of the people that we interviewed said they were willing to pay more for the devices and services that were found to be secure."

Nonetheless, if an EU-wide approach to device cybersecurity is rolled out, the Finnish scheme may have to wind down to comply, admits Seppänen.

Not all consumer advocates are in favor of a labeling scheme, noting that a better approach could be to ensure that all products sold to consumers are sufficiently secure, meaning there is no need for labels in the first place.

EU Radio Equipment Directive (RED)

HOW INSECURE IS CONSUMER IOT?

A principal factor that will shape the views of the Radio Equipment Directive (RED) delegated act relates to how significant groups or individuals view the scale of the cybersecurity problem in consumer devices.

While it has been clearly demonstrated that some devices lack basic security features, some industry participants see the problem as overblown, for example by pointing out that an open Bluetooth link can only be exploited by a person in close proximity. Others note that the risk profile of consumer products differs sharply from business products used in an organization, such as a bank, and believe that, based on the risk profile, any cybersecurity requirements for consumer IoT should remain voluntary and be driven by market forces (as in the EU Cybersecurity Act).

Built-In Risks

Due to a lack of regulation, low-quality, non-cyber-secure products remain legal in Europe. B2C IoT products tend to be cheaper and lower quality and thus create more risk. Businesses typically demand encrypted products and often have better knowledge of how to secure their devices.

These differing views were acknowledged in *Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment* (April 2020), a consultancy report commissioned by the European Commission which considered various options for legislation of connected consumer devices (it ultimately recommended the RED delegated act approach). "Whilst some industry manufacturing associations expressed the view that the nature of the risks has been exaggerated outside of smart toys, ICT and cybersecurity associations and cybersecurity testing houses mentioned that, despite improved awareness among industry about the vulnerabilities, there are still too many products coming to the market that do not even have the most basic cyber-security features integrated into smart products, making them vulnerable to hacking, attack and, therefore, also the data on a device or that the device is able to access (from other sources or devices)," the report states.

The problem has "grown much worse in the past five years" due to a lack of regulation, allowing "low-quality, non-cyber-secure products" to remain legally sold on the European single market, according to some stakeholders surveyed by the report's authors. In addition, B2C IoT products are seen as presenting a greater risk than those in the B2B market, given that B2C products tend to be cheaper and lower quality. Businesses typically demand encrypted products and often have better knowledge of how to secure their devices.

A view on the same topic was expressed by several scientists at Microsoft in a paper titled "The Seven Properties of Highly Secure Devices": "Industry largely underestimates the critical need for the highest levels of security in every network-connected device. Even the most mundane device can become dangerous when compromised over the Internet: a toy can spy or deceive; an appliance can launch a denial of service [attack] or self-destruct; a piece of equipment can maim or destroy. With risks to life, limb, brand and property so high, single-line-of-defense and second-best solutions are not enough."

essary because analysis showed it was not being applied across the EU in a uniform way, creating discrepancies between the member states and affecting the internal market, says Cristina Cretu, a senior privacy and technology consultant at Romanian law firm MPR Partners. The Covid-19 pandemic has further reinforced the view that digital services are important pillars crucial to avoiding disruption by cyber incidents that can affect the proper functioning of the European Union, necessitating an expansion of activities that will fall under the directive, says Cretu.

Key changes likely to result from an NIS Directive reform (NIS 2) include expanded scope of sectors and services considered as either essential or important entities, including postal and courier services, food, digital services (such as social networking platforms), data center services, and manufacturing of certain critical products that include pharmaceuticals, medical devices, and chemicals.

There will also be more stringent supervision of companies, including administrative sanctions and fines for failures in cybersecurity risk management and reporting obligations. The establishment of a European cyber-liaison organization will coordinate management of large-scale cybersecurity incidents and crises through increased cooperation between EU countries.

Improved data-sharing is recognized as a key component of a coherent cybersecurity policy and will improve how authorities and businesses identify threats, says Alexander Szanto, cybersecurity research fellow at Brandenburg Institute for Society and Security (BIGS). "For example, if a systems supervisory control and data acquisition (Scada) infrastructure is attacked in Germany, the same system is likely implemented in thousands of factories across the world. This means that if one company has this vulnerability, everyone has it. That's why information needs to be shared, so that everyone can implement [counter measures] at the same time," he explains.

source ©: Facebook

> NIS is not being applied in a uniform way all across the EU.
>
> **Cristina Cretu**
>
> Senior privacy and technology consultant at MPR Partners

An Act of Commission

The EU Cybersecurity Act (CSA) straddles both business and consumer markets. At its heart, it aims to unify cybersecurity standards across Europe, allowing a company to obtain certification for an ICT product, service, or practice that will be recognized in any country in the bloc.

A key element is the certification framework, which relies on the development of assessments covering various areas. The first three elements to have been developed are for common criteria schemes, cloud, and 5G, with additional modules currently in development. It's expected that consumer IoT will be dealt with soon, with the existing ETSI EN 303 645 standard potentially being a key specification for the Rolling Working Group to build upon.

This approach of developing schemes by reusing and updating existing standards as much as possible is official practice, says Philippe Blot, lead certification expert at the European Union Agency for Cybersecurity (ENISA), the agency tasked with responsibility for the CSA. The first set of schemes created will be more horizontal before the work moves on to vertical sectors like automotive or railways, he says.

Certification can be obtained at three levels: basic, where a company can self-certify; substantial, where a certification is received from a private standards company (known as conformity assessment bodies, or CABs); and high, where certification must be obtained ➔

Mariya Gabriel

The European Commissioner for Innovation and Research is considered one of the most influential women in the field of cybersecurity. "Cyber threats have become a matter of national security," she says. "They underpin the resilience of critical infrastructure, from power plants to the banking system and online marketplaces for small businesses."

Gaia-X and the Lawful Overseas Use of Data

HIGH NOON IN THE CLOUD

By Heinz-Paul Bonn

Like a gunslinger from the old Wild West, the US Cloud Act stands on main street and shouts, “Come out if you dare – unarmed and one at a time,” while Europeans stand at the windows and wave white flags. In certain circumstances under the Cloud (Clarifying Lawful Overseas Use of Data) Act, the US courts can demand the surrender of any personal data from American cloud providers, even if the data is stored on European servers and subject to European data protection regulations. In a pitiful display of appeasement, the EU attempted to use Privacy Shield, a data transfer mechanism agreed with the US, to try to protect citizens’ data from exploitation and intelligence agency snooping – which turned out to be absurd because many US companies, and possibly government departments, simply paid lip service to the agreement.

> ” Privacy is the most unenforced right in Europe.
>
> **Max Schrems**
> Austrian cyber-activist

When the Trump administration took over, it placed America first and tightened the provisions of the Patriot Act, which was forged to fight terrorism after 9/11. Since then, American cloud providers in Europe have had to violate one or the other of these acts, and Privacy Shield has been a distraction too many for some.

In the end, it took Austrian data activist Max Schrems to get the European Court of Justice to take down the Privacy Shield. Since then, the situation has not changed much: the gunslinger is still standing on the main street while Europeans sit around the regulars’ table hatching new rules for handling data, data structures, and data analysis.

Gaia-X, launched as an alternative European cloud, is now only – or after all, depending on your point of view – a set of rules for handling data in the cloud, the first version of which was presented for discussion last year.

This should lead to manufacturers having to provide users with details about which European standards have been met. Gaia-X will be analogous with food labeling, where suppliers provide information on shelf life, ingredients, and nutritional values. Gaia-X could at least become more meaningful by listing standards-compliance “contents” – but this will not drive the Cloud gunslinger off the main street. The content of the Cloud Act is unlikely to help Europe to recover its privacy independence.

Gaia-X could counteract a mostly unproven but constantly voiced reservation: the general suspicion that cloud providers are diverting and misusing their customers’ data for their own profit. However, there is a fundamental difference between professional cloud services, such as Deutsche Telekom’s T-Systems or Microsoft Azure, and data platforms, such as Google or Facebook, which see their customers as information suppliers and offer them cloud platform access at no charge in return for the disclosure of personal data.

Amazon is a special case here, because it straddles both worlds with Amazon Web Services (AWS) offering private professional cloud services on the one hand, while the Amazon retail platform allows the greatest possible sharing of consumer data on the other. This almost certainly contributes to the fact that the reservation of data misappropriation is constantly being revived.

Europe is now putting the brakes on the online platforms, under the leadership of the EU Commissioner for the Interior, Thierry Breton. The Digital Services Act is intended to create a basic service law for online platforms. It is formulated to update the provisions of the 20-year-old e-Commerce Directive, which was created under the conditions that prevailed prior to the dot.com bubble when the market-dominating platforms and business models didn't exist.

Providers are already warning that the new etiquette rules could possibly lead to companies like Google, for example, not being able to display restaurant recommendations on its interactive area maps. This is because the Maps' recommendations are based on an opaque algorithm that selects businesses according to criteria that are anything but objective – which will not meet the conditions of the Digital Services Act. It's still early days and this may not be the case as the Act is more likely to be directed against hate speech, fake news, and election influencing.

In the field of artificial intelligence, too, Europeans are trying to map the world anew with ethically motivated sets of rules. The EU is effectively repositioning itself between the western data capitalism of the USA and the eastern data communism of China. It is an attempt to regain a sovereignty lost in the post-war order. This is also how the 14-page strategy paper of the German Social Democrats is being seen in view of other issues such as the ongoing debate about the European role in the North Atlantic Treaty and the proposal of a "28th European Army" alongside the 27 national armed forces.

Europe must first recover from its European nature. The attempts to create frameworks, first in Europe and then worldwide, are examples of this still-young, burgeoning, longing for sovereignty. After all, the General Data Protection Regulation (GDPR) has already turned out to be an export hit and its content has been adapted and adopted in Japan and some Latin American countries.

It's unlikely the gunslinger will be driven off the main street by all this. Perhaps it's more likely that the Mandarin will be the one to stand up to him…

from a national cybersecurity certification authority in each member country.

Overall, the CSA will introduce a number of efficiencies. Having EU-wide certification will reduce fragmentation of certification, like the different schemes currently operating in member states such as France, Germany, and the Netherlands (which currently carry out the highest number of certifications within the EU).

This will simplify things for businesses that offer cross-border ICT products and help companies make more informed decisions about the security of their suppliers and supply chains more generally, feeding into cybersecurity universally. For example, in the case of entities covered by the NIS Directive, sourcing products certified under the CSA will help give greater assurance as to the security of their overall network.

The introduction of CABs to handle "substantial"-level certifications will reduce the time spent by national organizations in covering such activities, leaving them more time to concentrate on the "high"-level certifications, says Blot.

Despite CSA certification being voluntary (this will be reviewed in 2023), previous experience suggests that certification will become more common as organizations begin to use it to screen their suppliers, meaning that vendors will see a competitive advantage in being certified, believes Blot. "The maturity of cybersecurity requirements is still growing. For the first companies that get a cybersecurity certificate, even if it is not mandatory, it will be a differentiator in terms of their offering and more companies will follow. It's a trend seen in other areas [of the cybersecurity industry]."

At the basic assurance level – which will cover consumer IoT – companies can self-certify, which is bound to limit its overall impact in terms of connected devices sold to consumers.

"The Cybersecurity Act is part of the solution but it's well recognized that it's only one piece of the jigsaw and, indeed, not the main solution," says Rod Freeman, an international products lawyer at US law firm Cooley. "The Cybersecurity Act is important in providing a framework for standards and for certification but, on its own, that doesn't really address the nub of the problem."

> If one company is vulnerable, everybody is.
>
> **Alexander Szanto**
> Cybersecurity research fellow at BIGS

source ©:BIGS

Adoption and Adaptation

Freeman believes that the ultimate goal is likely to be a new piece of horizontal legislation developed under the new legislative framework (NLF), a package of measures that aims to improve market surveillance and boost the quality of conformity assessments. This has been announced by the European Commission, though its eventual implementation is likely to be more than five years away.

Apart from the introduction of a new law, the NLF framework itself will need to be adapted to address the entire life cycle of a device, including security updates, vulnerability handling, and disclosure, because it currently only governs products at the time of sale.

Given the extended timeline for a new law, there has been considerable pressure on policy makers to act sooner on consumer IoT. This has been driven by the member states, including the adoption of a resolution in late 2020 by ➔

the European Council. Inaction by Brussels could push individual countries to bring into force national-level legislation, fragmenting the common market.

That calculation has resulted in a move to use a delegated act from RED to activate provisions that require manufacturers of wireless devices to fulfil cybersecurity requirements by protecting consumers from fraud and ensuring their privacy. Such a move is acknowledged to have numerous shortcomings. For a start, it will cover only Internet-connected radio equipment and wearable radio equipment (estimated at around 75 percent of the connected-device market) and will not cover connected products that only use wires. In addition to excluding non-radio components (including processors), it won't cover the life cycle of the product (patches) or require disclosure of vulnerabilities.

Despite its shortcomings, the RED delegated act is seen as the fastest way to introduce a cybersecurity law in the short term, rather than having to wait for the development of a new horizonal law. Industry groups have identified these ambiguities in what is to be covered but they also worry that the regulations will introduce a mandatory set of standards and requirements, only for these to be superseded by a new law.

> We really think this could be an added-value globally – but we need to do it right.
>
> **Christoph Luykx**
> Policy director at Orgalim

source ©: Euralarm

A New Approach

To improve the internal market for goods and strengthen the conditions for placing a wide range of products on the EU market, the new legislative framework was adopted in 2008. It is a package of measures that aim to improve market surveillance and boost the quality of conformity assessments. It also clarifies the use of CE marking and creates a toolbox of measures for use in product legislation.

"We are completely supportive of mandatory baseline requirements under horizontal legislation, or of a certification scheme [like the CSA] which is voluntary and is more of a market-driven mechanism," said Alberto Di Felice, director for infrastructure, privacy and security at Digital Europe. "What we're seeing on the other end of the spectrum is the RED delegated act. We are far more skeptical about activating that instrument to target cybersecurity. The potential for overlaps and inconsistencies is huge."

An important question is whether the delegated act will have coherence with the new horizontal law, which the European Commission has indicated is its intention. Da Silva believes that the rules put in place by the RED delegated act will match up new rules at the horizontal level that are coming, though overall the new horizontal law will be much broader in scope.

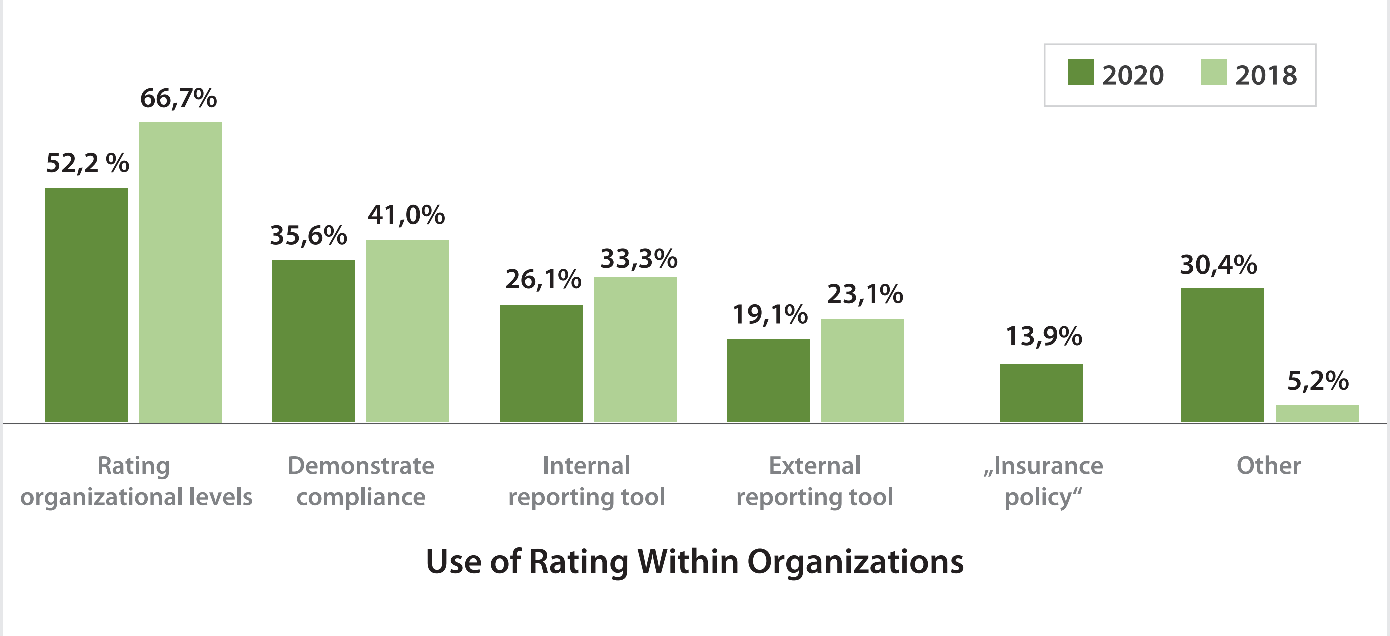
Overall, there is recognition among industry groups of the need for comprehensive regulation governing cybersecurity – and even its inevitability, given that the alternative would be a high degree of fragmentation – but the hope is to avoid contradictory or unworkable rules and develop these within the NLF, where there is input from industry.

Orgalim, a federation of European technology industry bodies, has called for horizontal legislation under the NLF. Christoph Luykx, its policy director, says that seeing such a request coming from industry may be surprising to a lot of people. "But it is precisely because we see a risk of fragmentation, the increased cost to produce and manufacture products, the confusion for the manufacturers and consumers, that is why we put forward a proposal for horizontal legislation," he explains.

Coherent cybersecurity rules for the European marketplace can ultimately help companies gain an advantage by allowing them to prove their credentials, both at home and abroad, believes Luykx. "If we get this right, and we are coordinated, and the cost and the bureaucracy of this is manageable, [manufacturers] can take cybersecurity into account from the development of a product to its rollout and during its lifetime. So, we really think this could be an added-value globally – but we need to do it right and there is still a lot of work to do."

How Much Cybersecurity Is Enough?

STANDARDIZATION VERSUS RISK MANAGEMENT



Use of Rating Within Organizations

source ©: LEET Security, S.L.

There's no doubt that cybersecurity is a complex topic to legislate. Given how fast-moving security's components are, legislation is often too slow and cumbersome. Antonio Ramos, CEO of Leet Security, a cybersecurity ratings agency based in Madrid and member of the Stakeholder Cybersecurity Certification Group (SCCG), says that recent trends in legislation around cybersecurity are, in general, positive. "Now cybersecurity is a 'hot' topic and politicians are aware of it," he adds. Nevertheless, he is critical of the overall focus on certification and minimum requirements and would like to see more emphasis on risk management approaches. "We keep thinking about cybersecurity as something that can be standardized, which, by definition, is impossible. Cybersecurity is a risk management issue which depends on risk appetite, risk exposure, and many other things that make it impossible to define which is the right level of cybersecurity for every single case. Certification is perfect for establishing a minimum level of requirements to start doing business in a field, but then we should open the hand to offer other kinds of mechanisms that have proven useful in other markets, such as rating, labeling, self-assessment, or auditing," he says. Rather than defining a list of security controls for every situation, an alternative approach is to define how to measure cybersecurity and then establish how much is needed in each case, suggests Ramos. "This approach is much more efficient and improves the efficiency of certification. In fact, this approach is the one that the Spanish Center for Protection of Critical Infrastructures (CNPIC) is using for the definition of the cybersecurity certification framework for critical operators. A scheme with different levels against which operators can set certifications and then the Center decides which level is right depending on the criticality of the infrastructure," he explains.

source ©: 20 Minutos Editora, S.L.

Trusted Tool

Rating is an important tool for managing cybersecurity in the value chain. Third-party certification is the most frequently used mechanism for 63.4 percent of respondents.

Define how to measure cybersecurity and then establish how much you need.

Antonio Ramos
CEO of Leet Security

Interview

source ©: Pilz GmbH & Co. KG

Fight Like Rocky!

Pilz Automation, an industrial automation specialist founded in 1948, suffered a crippling cyberattack in 2019. **CEO Thomas Pilz** talked with *Smart Industry* about how it feels to be a victim and what he thinks is the best way to defend against cybercriminals.

> We were forced to rebuild our IT infrastructure from scratch!
>
> **Thomas Pilz**
> CEO of Pilz Automation

What's the difference between machine safety and industrial security?

It's basically two sides of the same coin: one is safety, the other is security. They look the same but they're totally different.

How have IoT and Industry 4.0 changed the focus of cybersecurity?

They have caused a complete paradigm shift. In the past, security only concerned office environments; now, it has become vital for OT [operational technology] – the stuff that monitors and manages industrial process assets, as well as manufacturing and industrial equipment.

Pilz's technology is not only used to make industrial plants safe but also appears in places like the London Eye, cable cars, and luggage conveyors. Tell us about some of your projects.

Our projects spread across all the industries you mentioned – and we haven't even talked about the biggest one of all, which is ski lift manufacturing. The next time you're in the Alps or the Rockies and you're sitting in a Doppelmayr ski lift, please note we proudly supply the controls that make them carry you smoothly to the top. We also have our fingers in the food and beverage industry, just to name one.

What about service robots, an area you recently entered?

Service robots assist either a human or another robot to perform dedicated manufacturing tasks. This is an exciting field that's only been around now for six or seven years. Currently, we are making it fit into everything from nursing homes to supermarkets or industrial welding, as well as into manual assembly stations. That's what makes the field of service robots so fascinating.

One of your credos is "protecting people from machines is not enough. Machines must also be protected from people." Would you please explain?

Let me start with a statement from China's president Li Keqiang, who said that without cybersecurity there is no national security. Break that down to the OT shop floor and it means that without cybersecurity, there is no machine safety. Unfortunately, cybercriminals have found out that the Internet of Things and Industry 4.0 with their new and emerging IT infrastructures are prime targets. That's why you now also have to protect your machines from cybercriminals.

Oddly enough, your own company was the victim of a widely reported cyberattack in October 2019, which involved a very sophisticated Trojan horse and ransomware, which seems to prove that it can happen to anyone. What does it feel like to be the victim yourself?

You feel like Rocky being punched in the face by the big Russian, falling down, getting back up again, and fighting on as hard as you can to win that bout. That's how it feels.

In an interview, Susanne Kunschert, your sister and managing partner, said the company emerged from this disaster stronger than ever. How so?

We were forced to rebuild our IT infrastructure from scratch. We introduced new ways of segmenting, we introduced technologies, and we switched to the cloud. That was a real game changer. We implemented Microsoft Office 365, first on our smartphones and then on our new, hardened computers. Within only five weeks we were back up and running. It was a heck of a job but we succeeded. When the Covid-19 lockdown came and the government imposed mobile work requirements, we were prepared from the get-go.

What can the readers of *Smart Industry* learn from your experience?

First that functional safety is not security. Pilz is not a security company but we have learned a lot and are prepared to give expert security advice at the OT level. You need to get involved in security before you get hacked because, after all, the question isn't will you get hacked, but when. We work with a company that specializes in cybersecurity and that enabled us to hit back hard.

The second lesson is to work with your local law enforcement authorities. They have really good networks themselves and, in our case, the German police, Europol, Interpol, and the FBI worked together to take down the group that devised the shield under which it penetrated our systems undetected.

Finally, the third lesson is that, today, crime is a service; it's a business model that thrives on ransom payments. So, don't pay up – ever! The criminals need the money and, if we dry up the flow, it becomes uneconomical.

Western Digital

Thrives in Tough Environments

High Capacity, Zero Compromises

Empowering data-intensive industrial and automotive designs

High performance and endurance combined with industrial-strength quality and reliability

Able to handle large data volumes in demanding conditions

Stands up to wide temperature ranges and strong vibrations

Campus Networks

BUILD YOUR OWN 5G

Operating a private campus network offers several advantages and will help improve production and enable factory automation. **There are three options for building a 5G campus network**: self-build and operation; using a network service provider offering a private campus network as a service; or contracting a mobile network operator offering a 5G VPN by slicing their public network.

By Gerhard Kafka

> Continuous innovation is part of our corporate DNA.
>
> **Soeren Stark**
> Lufthansa board member

Private campus networks are designed and deployed by enterprises to optimize or enable business processes. Broadly, there are three drivers to deploy a private 5G network: to guarantee coverage, gain network control, and to meet a performance profile. Coverage will need to be improved in locations with harsh radio frequency (RF) or operating conditions or in remote areas where public network coverage is limited or nonexistent. Control is required to allow configurations that are not supported in a public network to be applied. Security and data privacy are also important controls and the need to retain sensitive operational data on-premises is crucial to high-tech industrial companies. Even though 5G has a clear performance advantage over LTE and Wi-Fi in cyber-physical industrial systems, maintaining performance profiles for demanding applications is still a requirement.

A January 2021 report by the Global Mobile Suppliers Association (GSA) has identified 37 countries or territories with private network deployments based on LTE or 5G, or at least with private network spectrum licenses deployed. In Germany, for example, the frequency band from 3,700 MHz to 3,800 MHz is reserved for local and regional 5G networks. The Federal Network Agency (Bundesnetzagentur), the German regulator, reported in December 2020 that 108 licenses for local 5G networks had been allocated.

A joint report from ABI Research and Ericsson, *Smart Manufacturing and How to Get Started*, explains the economic effects on return on invest-

ment (ROI) for factories. Deploying dedicated, cellular-enabled Industry 4.0 solutions can generate operational cost savings ROI of between 10 and 20 times over five years. In aggregate, these solutions can generate 8.5 percent in operational cost savings, which equates to $200 to $600 per square meter per year for a factory or industrial site.

Marc Sauter, head of mobile private networks for Vodafone's business division, believes, "It is possible to have a million private networks by the end of the decade. In Europe alone, we have about a million companies that could benefit from private mobile networks – with most in manufacturing, along with logistics and warehousing, utilities, oil and gas, and increasingly in health care."

The first stand-alone private network in the aviation industry has been installed in Hamburg at Lufthansa Technik. Together with service partner Vodafone and technology partner Nokia, Lufthansa's repair, maintenance, and overhaul (MRO) group is operating a complete, self-sufficient 5G network covering the core and servers all the way to the antennas. The system is based on the 5G standalone (SA) standard. Lufthansa can configure the network as required, such as specifying the relationship between upload and download rates. "He who relies today on new technologies will stand in front tomorrow," predicts Hannes Ametsreiter, CEO of Vodafone Deutschland.

One application in use is called virtual inspection, where the hyperfast wireless connectivity enables its civil aviation customers to have engine parts inspected remotely. A high-definition video link connects customers directly to the overhaul shop floor, improving efficiency and operational performance. Before the virtual link, customers had to travel to Hamburg with their components, which meant that engines were completely disassembled for inspection. With the new system, Lufthansa Technik can inspect individual engine parts collaboratively over the fast video link.

source ©: Lufthansa Technik

A Good Look
Engine parts inspection
using video stream.

Soeren Stark, an executive board member responsible for technical operations, logistics, and IT at Lufthansa Technik, says, "Continuous innovation is part of our corporate DNA and this is what drives us to constantly try out new approaches. The first application cases already impressively demonstrate the valuable contribution 5G technology can make to the aviation industry. It will also pave the way for numerous innovations at Lufthansa Technik that will benefit our company, our employees, and our customers."

The Challenge of Augmented Reality

How will 5G degrade when passing through aluminum alloy and carbon fiber? The challenge with the augmented reality system is to display the 3D overlays and give precise, near-real-time guidance to the technicians on how to fit cabling and cabin furniture as they make their way through the fuselage. The crew uses beam forming to direct the stream via the antenna to the tablets in the hands of the technicians, and the transfer performance hits 1.2 Gbps outside the hull and 800 Mbps inside it.

The 5G network has kept Lufthansa's MRO services business humming through 12 months of the Covid-19 pandemic, when consultations with airlines about engine maintenance and aircraft cabin refitting were forced to go online. ➔

Out of the Box
The Vodafone RedBox offers industrial customers a complete 5G network.

source ©: Vodafone

source ©: Lufthansa Technik

Augmented Reality

Cabin completions showing 3D design of a cabin interior in an empty aircraft fuselage.

Mercedes-Benz Cars and Telefónica Deutschland have deployed the world's first 5G campus network at the flagship Sindelfingen car manufacturing plant, near Stuttgart. "In Factory 56 we are significantly increasing flexibility and efficiency in comparison to our current vehicle assembly halls – without sacrificing our quality," says Ulrike Graze, the Mercedes-Benz manager responsible for Factory 56. The unit covers 220,000 square meters, which equates to about 30 soccer fields.

Industry 4.0 Becomes Reality at Last

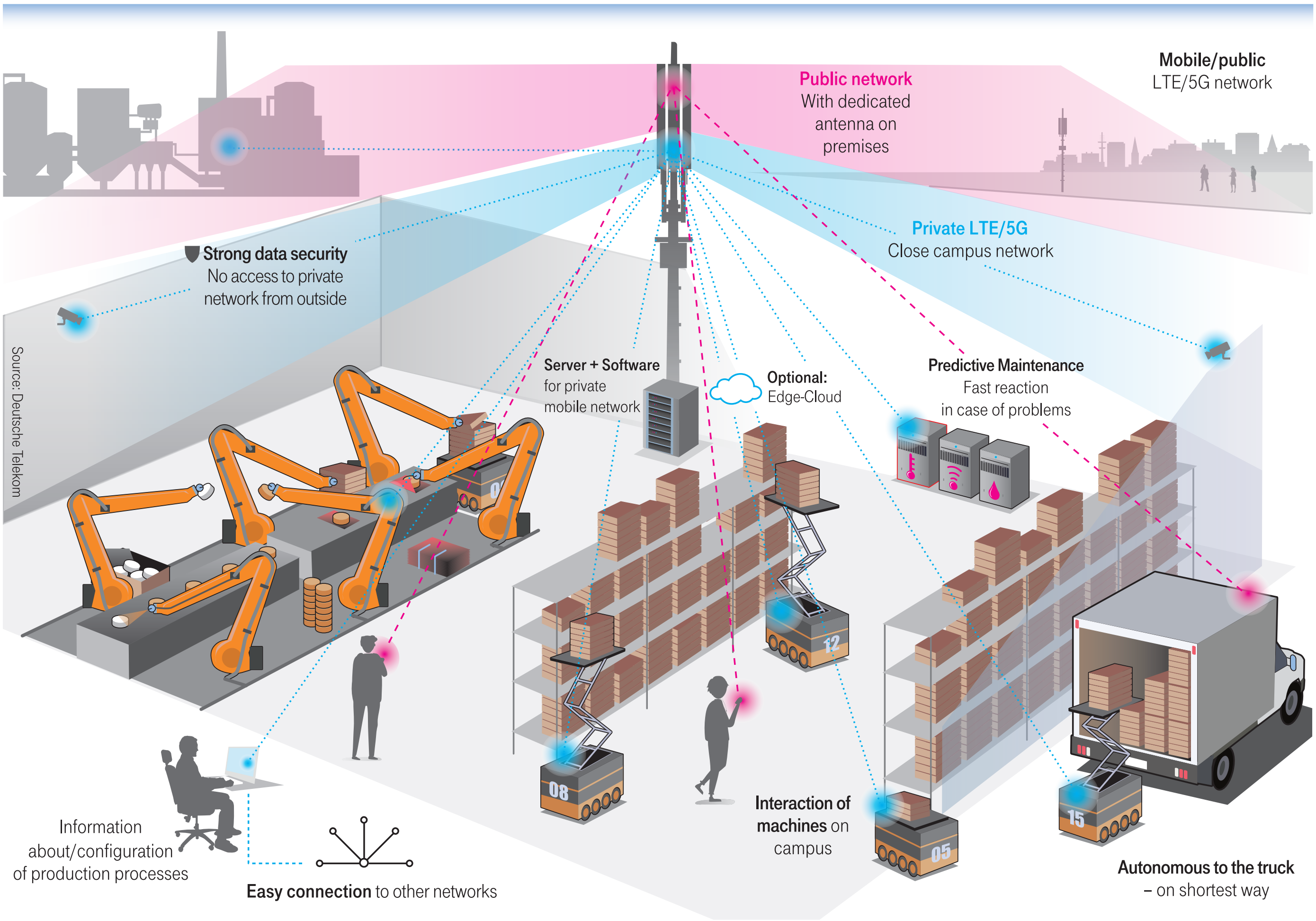
A core element of the new production facility – an all-digital, flexible, "green" factory – will be the 5G campus network installed by Telefónica Deutschland and O2 in cooperation with network equipment supplier Ericsson. The mobile communications mesh will connect machines and systems intelligently, securely, wirelessly, and in real time. The network is used in ongoing automobile production at Mercedes-Benz.

"With 5G, the concept of Industry 4.0 becomes reality. The Mercedes-Benz Cars plant in Sindelfingen is setting innovation standards here. The new 5G mobile communications standard is impressive with particularly fast data transfer rates, very high accuracy, and short delay times. 5G is becoming a huge efficiency lever in robotics, in the connection of production facilities, and, thus, in industry as a whole," says Markus Haas, CEO of Telefónica Deutschland/O2.

Mercedes-Benz is optimizing existing production processes in its plant with the help of new features, including data linking for product tracking on the assembly line. With a separate in-house network, all processes can be optimized and made more robust and, if necessary, adapted at short notice to meet prevailing market requirements. Furthermore,

Something for Everyone

Campus Networks are exclusive mobile networks for a defined local campus, a university, or individual buildings.


Mobile/public
LTE/5G network
Public network
With dedicated antenna on premises
Private LTE/5G
Close campus network
Strong data security
No access to private network from outside
Server + Software
for private mobile network
Optional:
Edge-Cloud
Predictive Maintenance
Fast reaction in case of problems
Interaction of machines on campus
Autonomous to the truck
– on shortest way
Information about/configuration of production processes
Easy connection to other networks
08
12
05
15

Source: Deutsche Telekom

source ©: Deutsche Telekom

source ©: Mercedes-Benz

A Network Is Born

The cornerstone ceremony for the new Mercedes-Benz Cars assembly hall in Sindelfingen was attended by Winfried Kretschmann, Minister-President of Baden-Württemberg.

5G links production systems and machines together in an intelligent manner, thereby supporting the efficiency and precision of the production process. A further benefit is that sensitive production information is not exposed to third parties.

Other German car manufacturers, such as Audi, BMW, Porsche, and VW, have also decided to deploy 5G campus networks – not to forget the electric-car maker e.GO in Aachen pioneering mobile edge computing and network slicing.

Hanover to Host 5G Exhibition Center

In partnership with Deutsche Telekom, Deutsche Messe is gradually transforming its exhibition grounds into an innovative multifunctional campus. Deutsche Telekom is ensuring high-performance 5G coverage over an area of 1.4 million square meters, implementing the campus network as a hybrid one. The showground will eventually have a private network that trade fair organizers and exhibitors can use for their applications. At the same time, attendees have comprehensive coverage through the public 5G network which covers the exhibition area.

With the 5G expansion, the Hanover site will be one of the largest 5G campus networks in Europe in terms of area. Initially, Deutsche Telekom is equipping five halls and the entire outdoor area, including adjacent parking lots, before moving on to all 30 halls and buildings. The aim is to create a unique test field for 5G where technology leaders from a wide range of industries can test their solutions.

"For Deutsche Messe, the early decision to have its own 5G campus network covering the entire exhibition center is a strategically important step. We are thus offering exhibitors and guest organizers of all trade fairs in Hanover the opportunity to present their 5G-enabled products, solutions, and applications live to an international audience," said Jochen Köckler, chairman of the Deutsche Messe board.

Siemens is also playing a role in this development. As one of the key exhibitors at the Hanover Messe, Siemens is setting up a private 5G campus network, with a focus on industrial use, in one of the exhibition halls. The network can be used by exhibitors during trade shows and, outside of trade show times, it can be used by companies for tests and field trials.

source ©: Deutsche Telekom

Rapid Growth

True 5G deployments of campus networks are predicted to reach one million by 2030.

5G Is Fair Game

The Hanover Fairground is being transformed into an innovation campus.

source ©: Deutsche Messe

eSIMs

THE GREAT IOT CONNECTIVITY LOCKDOWN

When you move house your devices go with you. It's not so simple in the global communications world but eSIMs promise to break through the barriers that tie us down.

By Michael Moorfield

With many of us around the world currently locked down in our homes, it's easy to find time to look around and see how many of your devices are currently connected to the Internet. Maybe it's your home computer, gaming console, laptop, your TV, children's tablet, smart speaker, mobile phone, watch – or even your vacuum cleaner and doorbell.

Now consider this: what if each of those devices had to be specifically made to order for it to work in your home network? What if all of them were locked forever to your current home network and service provider? If you ever decided to upgrade your network, move to a new house, give a device to a friend, or leave the country, all these products you paid good money for would no longer work.

> This model of connecting things is completely crazy!
>
> **Michael Moorfield**
> Director of Product
> Truphone Ltd.

This would be ridiculous. As customers, we wouldn't accept it and any connected future where massive numbers of IoT connections could thrive would be a pipe dream.

For any product that supports Wi-Fi, this isn't a real problem today. We all know and rely on the fact that you can configure Wi-Fi network settings and get things connected when your situation changes.

Now, let's think about outside the home. More and more things around us are getting connected to the Internet. Cars, streetlights, pollution sensors, traffic monitoring, security systems, online delivery lockers, health monitors, parking garages, energy meters, trackers for goods, pets, or your motorbike. All these things are getting smarter and more connected and they all seek to leverage the ease of use, security, and wide availability of mobile networks to make it happen.

Many Devices Remain Locked into a Network

For many of these products, the reality of how easy it is to change networks is very different. These newly connected things will remain locked to a specific mobile network. Forever. They have been specifically manufactured and configured to only ever work with one specific mobile network provider.

To me, this model of connecting things is completely crazy. This level of commitment requires nothing short of a crystal ball to know whether these products will work

first time when in the hands of customers and continue to work long into the future. If you happen to be wrong, you know the cost to change it will be immense.

A key reason for this method of connecting things lies in the little old SIM card. It's critical for securely connecting billions of devices around the world to mobile networks. All these new connected products require a SIM card to be pre-integrated into devices or included somewhere along the sales and distribution chain – and once it's there, it stays forever.

It is clearly untenable that the traditional SIM card be used for scaling billions of connected devices around the world and forcing them to be locked to a specific connectivity provider for their lifetime. It's for this reason that the Global System for Mobiles Association (GSMA) developed the worldwide standards for eSIM in the first place. Its focus has been to create a smart, rewritable chip that can be as secure as a normal SIM card but allows over-the-air control of a device's connectivity. Breaking the network-to-device lockdown without needing to be physically there. By using eSIMs, customers have the flexibility to select a contract with their preferred supplier with the confidence that their devices will remain operational even if the connectivity contract expires or fails.

But if it's so flexible, where are all the eSIMs? In practice, their true benefits are not being felt in the Internet of Things. Many in the industry are still being locked out of using them. Whether network providers are unable to support them or costs are prohibitively expensive, for many, the promised land of eSIM is being hollowed out.

Building Up Walls Instead of Tearing Them Down

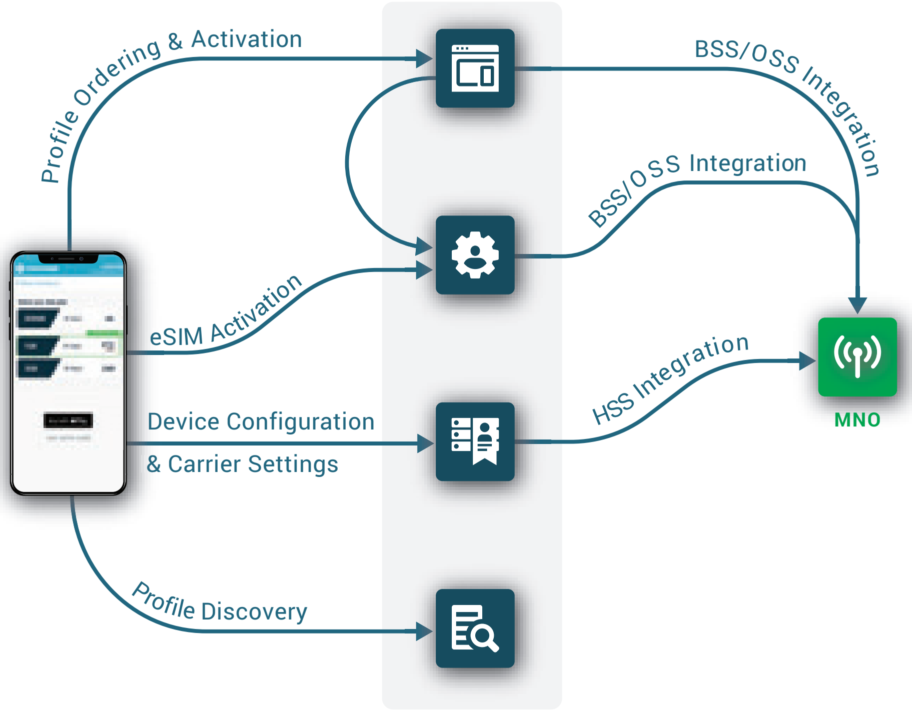
Despite the continued work in tightening standards to explicitly promote interoperability, there is wide evidence of devices being made every day that will remain locked to a specific network provider forever. In the latest consumer devices such as the Apple iPad and iPhone the tide is turning. Customers can easily download a mobile plan of their choosing over the air and get connected using eSIM without the need for an actual SIM card from a network provider – or a lifelong commitment. For many other IoT devices this is still far from a reality. It's unfortunate that, in a moment where openness and interoperability have never been more crucial to unlocking revenue, crucial players in the industry have responded by building their walls higher, instead of knocking them down.

The standardization of eSIM has paved the way to breaking down major barriers in connecting devices to mobile networks. It makes connecting new things easier than configuring your Wi-Fi password at home and provides users with the confidence and assurance that they will remain connected long into the future, whatever happens.

When it comes to connecting things to mobile networks, eSIM is the catalyst for change – we simply cannot reach the full potential of the IoT without it. Predicting the future is hard. Forever is a big ask from anyone and you would be right to fear such a commitment. Don't wed yourself to one option.

With the addition of the eSIM

on Apple's and Android smartphones, there has been huge growth in eSIM-enabled consumer devices. Today, mobile providers are almost required to provide support to customers who want to take advantage of features such as Dual SIM and connectivity management.



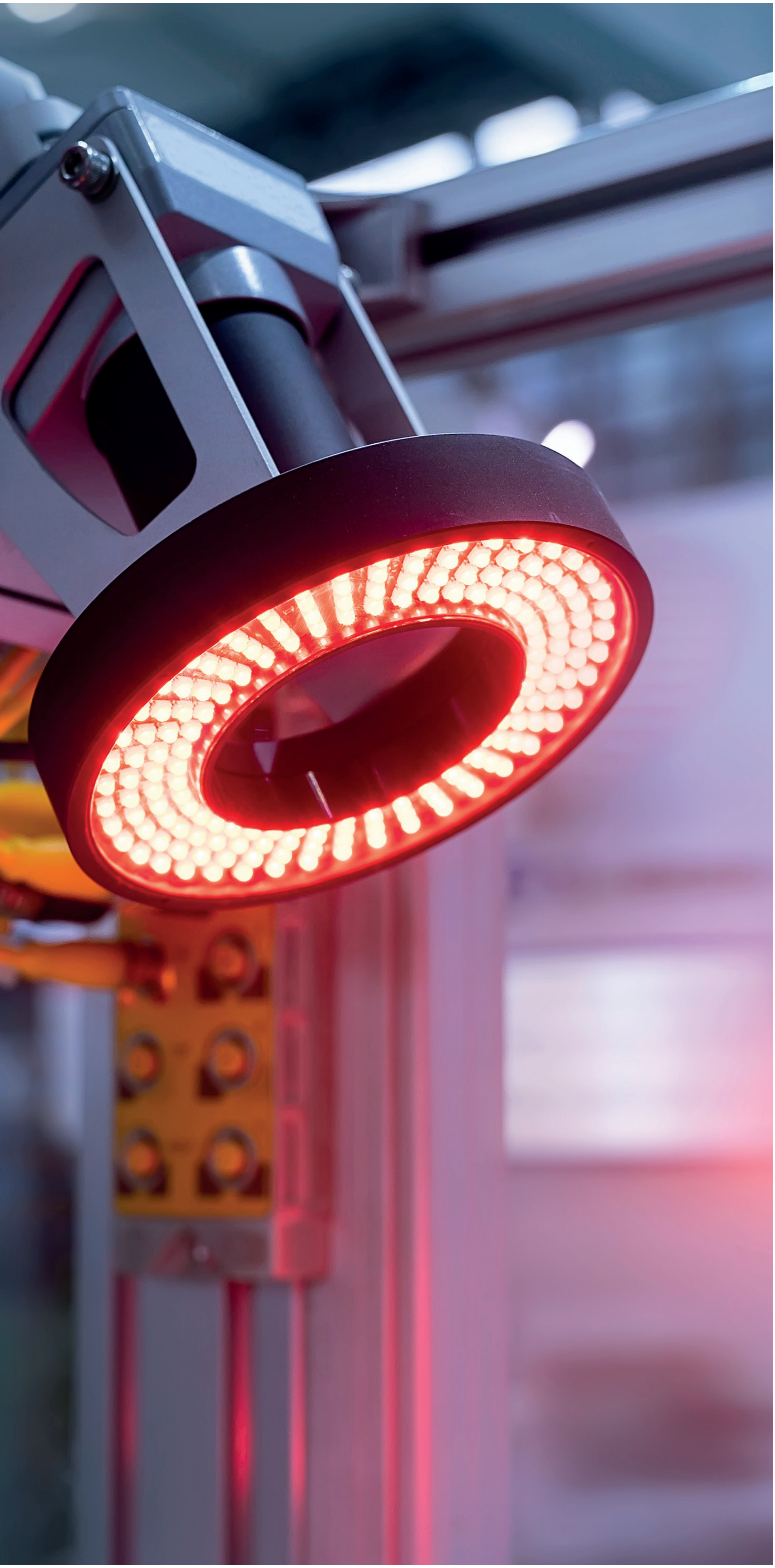
source ©: TRUPHONE LIMITED

Predictive Manufacturing

THE FUTURE OF MAKING

Predictive maintenance, **using IoT to anticipate and prevent breakdowns by collecting and analyzing machine data**, has been gaining momentum in recent years. Based on its successes, some innovators are applying the same kind of thinking to entire manufacturing operations and are even aiming to tie in visibility on the supply and demand sides.

By Allan Earls



In manufacturing, predictive analytics generally refers to gathering data about a machine setting or process and continually analyzing that data, explains Mark Wheeler, director of supply chain solutions at Zebra Technologies. "By monitoring the data on a regular basis, the manufacturer is in a position to correct an anomaly before it actually impacts product quality, yield rate, or some other critical outcome," he adds. By identifying and tracking individual items, if an out-of-spec condition is detected, it can be isolated to a specific piece of equipment for attention and a specific set of parts for inspection and rework.

"Information volume is at the core of achieving system, process, equipment, or functional predictability," says Saurabh Mehta, global head of markets, manufacturing, and logistics at Cognizant, an international business consultancy. Higher volumes of data make it possible to build predictive models based on longer and more dependable history. As an example, Mehta explains that the data related to product-quality problems under different operating conditions can be immensely helpful in building models that can then be related back to the design and manufacturing process. Tracking back in this way enables manufacturers to predict potential quality catastrophes before they happen.

Data accuracy is directly proportional to the level of confidence one can place in the decision processes based on the models that are built. As an example, the accuracy of physical or work-in-progress inventory capture would make the decisions about line planning much more dependable. "In the process industry, this accuracy would help build models that … would help minimize the off-spec or waste, thus improving overall process yield," Mehta says.

Based on things like existing root cause analysis practices, predictive manufacturing models help in ➔

source ©: Zebra Technologies

Where Are Your Assets?

Bluetooth smart beacons like these from Zebra Technologies offer real-time tracking and management of goods in complex logistical operations, including on-demand information about location and status of assets.

avoiding quality problems or major impacts and offer the ability to clearly define conditions under which quality problems most frequently occur. This enables manufacturers to clearly spec out their products and protect themselves. "A good example of this is a proper maintenance schedule that avoids significant damage for equipment whose components are known to fail after 5,000 hours of operation in defined ambient conditions," he says.

"Overall, the advent of predictive capability from a quality perspective not only provides engineering teams with the ability to correct quality problems during design phases but also makes them completely aware of the conditional quality problems that cannot be resolved, thus making the designs more reliable," Mehta adds.

Putting Predictive to Work

An example of an organization on the path to predictive is Alpla, a manufacturer of plastic packaging for brands like Coca-Cola and Unilever. The company uses Crate's IoT Data Platform to analyze data from tens of thousands of sensors. Processing is done in the cloud and a central control room monitors plant performance at local and remote facilities. From these insights, Alpla can identify trends at an earlier stage and its machine operators can be guided quickly to make necessary adjustments.

According to Mehta, the concepts of predictive manufacturing need to be applied in the contexts of the application or challenge, the larger business needs, and the extent of the potential impact. For example, the application of deep learning techniques to ensure a precision cutting process may be of less value than a simple measurement or control system. However, using deep learning is appropriate to predict quality variations given the complexity of the problem, as well as the magnitude of downstream impact.

> Investment in predictive manufacturing may require some vision.
>
> **Saurabh Mehta**
> Global head of markets, Cognizant

source ©: Cognizant

"Application of predictive manufacturing efforts without the context of the application and its larger business impact results in being either ineffective or over-effective," he says. "The other important point to remember is to align the predictive manufacturing efforts to larger organizational digitization or transformation needs. Without that, the business benefits would not be proportionate to the effort and the traction would be lost."

An Organizational Tune-up

Predictive capability can have a direct impact on productivity and can also help operators to work more efficiently. This may lead to the use of alternative materials in the design of a product – like composites, different types of lubricants based on conditions of use, or warranty parameters that provide heavy equipment fleet operators with guidance on how to manage their fleet and extend the life of key consumables.

"Enterprises have traditionally been challenged with converting real-time, historic OT [operational technology] data from legacy systems into higher-level IT insights," notes Keith Higgins, VP of digital transformation at Rockwell Automation. Data produced on the factory floor needs to maintain its rich context (such as process conditions, time stamps, machine states, and other production states) to provide maximum insights to factory staff.

He notes that aggregating the data generated by machines in processes previously required significant manual effort and the pulling of information from many disparate sources. “By implementing advanced analytics software, including machine learning, within their manufacturing systems, organizations can automatically capture high-speed, contextualized OT data from industrial controllers in real time and generate predictive insights and operational excellence across their enterprise,” he says.

Data creates new opportunities and some complexity challenges as well. Jonathan Luse, general manager of Intel Industrial Solutions, says, “With emerging technologies like 5G and Wi-Fi 6, it will be easier and cheaper than ever to gather new data from your operations. Around my organization, we talk about implications of the ‘Three Vs’ of big data – volume, velocity, and variety.” He adds that Intel sees increased volumes of data being collected at increasing rates, coming from a variety of sensors (and linked systems). Luse notes that this can create both opportunities and new problems: “The ‘garbage in, garbage out’ concept holds true, and not all data is equally important, however it’s still important to gather as much data as possible to use it to dynamically discover actionable insights.”

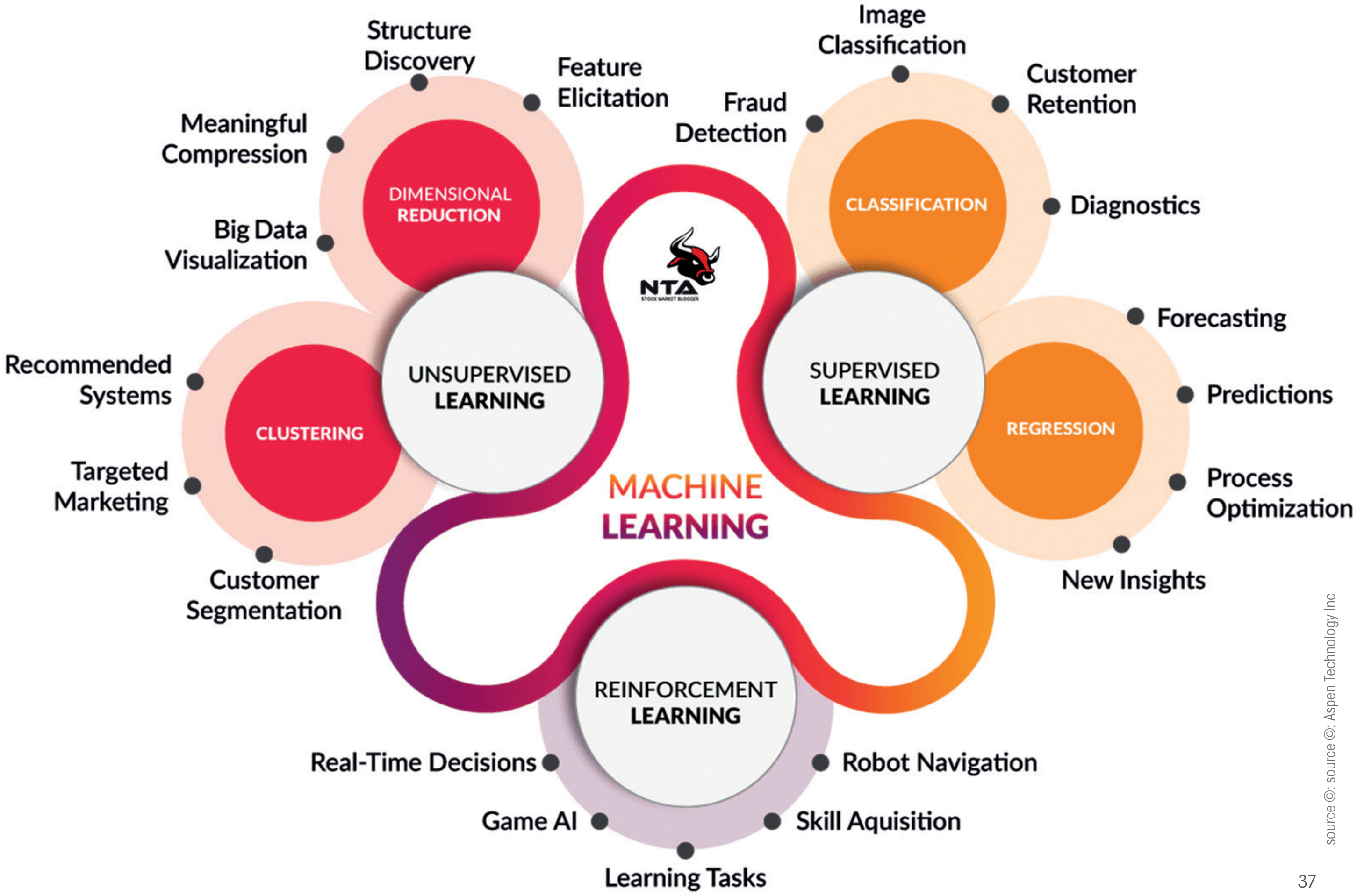
With all that data and so many analytical activities, the rise of the Industrial Internet of Things (IIoT) is giving impetus to a new digital solution category – the Artificial Intelligence of Things (AIoT), says Bill Scudder, general manager for AIoT solutions at AspenTech. This new field is seeing the combination of AI with IIoT to enable the next generation of industrial AI infrastructure, allowing organizations to achieve more efficient IIoT operations and seamless human–machine workflows, to harmonize industrial data management, and the ability to transform raw ➔

> Data creates new opportunities and new challenges.
>
> **Jonathan Luse**
> CEO at Intel Industrial Solutions

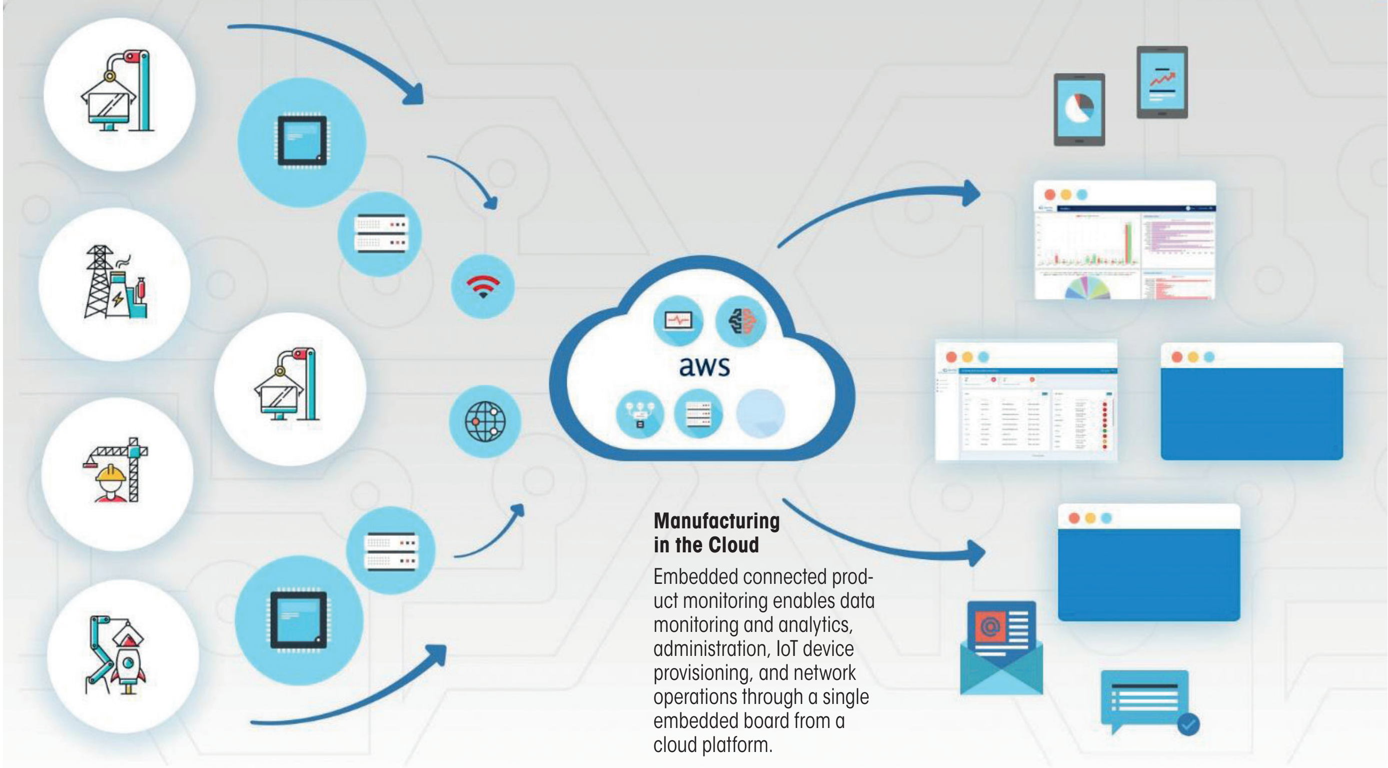
source ©: Intel Corporation

Teaching AI

One of the real strengths of machine learning is that there are different types of learning algorithms which can be used, including supervised, unsupervised, and reinforcement.



source ©: source ©: Aspen Technology Inc



Manufacturing in the Cloud

Embedded connected product monitoring enables data monitoring and analytics, administration, IoT device provisioning, and network operations through a single embedded board from a cloud platform.

source ©: Tritos

data into tangible business outcomes rapidly, he says.

The concept of predictive manufacturing effectively extends an enterprise digital strategy. It should help reduce costs, increase quality and throughput, and prepare the organization to be more agile, says Naren Gopalkrishna, digital product manager at GE Digital. As the organizations mature in their predictive manufacturing journey, several other aspects of optimization are driven forward, such as predicted observations and prescriptive actionable insights.

Organizations need to have a certain level of digital transformation maturity to successfully implement the predictive manufacturing concept. "The digital strategy should align with the larger manufacturing strategy and it should also consider the business problems that must be addressed," says Gopalkrishna, adding that the IT and OT teams need to work together.

> IoT is making predictive manufacturing possible.
>
> **Mats Samuelsson**
> CTO at Triotos

source ©: Tritos

source ©: Aspen Technology Inc

> The Artificial Intelligence of Things transforms raw data into business outcomes.
>
> **Bill Scudder**
> General manager for AIoT solutions at AspenTech

Predicting the Downsides

At Cognizant, Mehta's view is that predictive manufacturing is a strong concept but implementation is often lacking in terms of providing sufficient volume, granularity, quality, and information accuracy. As an example, a temperature measurement at the output of a process can be effectively used to control quality in real time, avoiding quality issues by retrospectively analyzing the data. Lack of appropriate measurement (sensory) and/or intake frameworks would lead to the absence of this data, or the inability to use it even if it's measured.

Zebra's Wheeler says predictive manufacturing may require investment in visibility infrastructure to provide real-time data plant-wide. "Justifying this investment may require some level of vision of the broad uses and value of leveraging this visibility," he adds.

Mats Samuelsson, CTO at Triotos, a company that builds overlay solutions on the Amazon Web Services (AWS) IoT cloud platform, sees the combination of better ways of collecting and processing data from new IoT technologies, plus improvements in machine learning, analytics, and AI, as a game changer. "They will certainly be combined with integration of existing and new control technologies for steady improvements in how manufacturing and production are planned and operated," he says. "The question is which strategies enterprises will embrace to cost-effectively seize the opportunities, such as predictive manufacturing, that IoT is making possible," he concludes.

IoT Security

IDENTITY OF THINGS

Every device, app, service, and interface in IoT needs its own identity, which operators can use to track and analyze activity. This is not only used to identify problems but also **to protect the systems from attacks,** attempted fraud, and espionage.

By Oliver Schonschek

Martin Kuppinger

Mark Child

Romain Fouchereau

Bernhard Schaffrik

source ©: Braun.Social, Wikimedia Foundation Inc.

Now You See Me, Now You Don't
In IoT, identities must be based on cryptography. Provisioning large IoT systems with reliable, unique, secure standards-based identities is a major challenge at the moment.

The more you have, the more you get: identity plays a key role in securing IoT, and the number of digital identities to manage tends to grow exponentially – many more than existing identity and access management (IAM) systems need to support, says the IoT Working Group at Cloud Security Alliance.

The security industry is changing and IAM is no longer solely concerned with managing people but also managing the hundreds of thousands of "things" that may be connected to a network. Some practitioners have begun to refer to this new identity ecosystem as the Identity of Things.

Smart Industry asked leading analyst firms about the importance of identity management, the major challenges, and the ways to implement identities for IoT.

Every device, app, service, and interface in IoT needs its own identity. Why is that?

Martin Kuppinger, KuppingerCole (KC) An IoT device will need to interact and communicate with other devices, applications, or services of some kind to be useful. It's important to trust that these IoT devices can prove they are what they claim to be, or represent. Otherwise, hackers could use these IoT devices to attack other devices, applications, or the services they interact with, as well as the data transmitted from these devices, which could be stolen or compromised.

The first step in an IoT trust relationship is the ability of an entity to identify and prove itself through the act of authentication. Any kind of device needs a unique identifier, if only to differentiate it from another one.

For large fleets of IoT devices this is a basic operational requirement – deployment, maintenance, monitoring of IoT devices is impossible without unique identities. Data generated by IoT sensors is much less useful without identifying where it comes from. Most use cases require this data to be tamper-proof and not forged by attackers and, for most cases, these identities must be based on cryptography. Provisioning large IoT systems with reliable, unique, secure standards-based identities is a major challenge at the moment.

Mark Child, IDC IoT devices communicate with core systems in countless ways, whether it's physical access systems checking credentials, warehouse scanners updating inventory, or temperature sensors communicating with industrial control systems.

These connected devices typically do not have the same robust security associated with operating systems for PCs or servers and, as a result, they may be targeted by hackers as an entry point through which to penetrate the network.

In some cases that may be the hacker's goal: as an entry point and, possibly, as an egress route through which corporate IP may be exfiltrated. In other cases, looking at the examples above, the aim might be to allow unauthorized personnel to access a secure site or to sabotage production operations.

> IoT devices communicate with core systems in countless ways.
>
> **Mark Child**
> IDC

Bernhard Schaffrik, Forrester Research (FR) The elements of IoT systems perform a variety of actions while accessing sensitive corporate data. Therefore, they actually represent a kind of identity, albeit non-human.

Managing all IoT assets like identities allows the application of known administration processes to ubiquitous IoT assets. If you don't know how many software bots, physical robots, or IoT devices are connected to your network, and how many of these devices store or interact with critical data, you expand your threat surface, leading to unmanaged zombie accounts that malicious actors will use to carry out attacks. This usually leads to reputational damage and financial loss.

What are the use cases for IoT identities in security and for IoT analytics?

IDC Implementing IoT security, specifically device identity, allows

➔

the organization to put authentication and access controls in place, ensuring that the system recognizes the device and that communication from the device is legitimate.

Baseline behaviors can be established for each device and, through analytics, the system can seek to detect anomalous behavior. The system can then trigger an alert for a human controller to check the device or request, or it can trigger an automated response, quarantining or isolating the device to prevent the transmission of malware to the organization, or the exfiltration of data from the organization.

FR Because most deployed IoT assets act like network-accessing computers, the whole management life cycle has to be applied to them as well: from discovery to monitoring, compliance, and retirement. Not knowing your landscape of IoT assets carries comparable risks to not knowing your application landscape.

Beyond the operational risks, at some point you will need to clean up your IoT landscape. Who wants to embark on collecting, documenting, and consolidating all these assets? Why repeat the same old mistakes we made with IT asset, architecture, and configuration management?

What is the current situation with IoT identities? Are IoT implementations lacking identity solutions?

KC There is a wide range of IoT types that sense or actuate something supporting personal, enterprise, and industrial use cases. Thus, there is little consensus on IoT identity standards, only a set of best practices depending on the type of IoT being used.

I would argue that many IoT projects try to use existing solutions for IoT – the obvious one is using public key infrastructure (PKI). Unfortunately, traditional PKI architectures don't scale well for large IoT deployments. Also, provisioning each device at manufacture time is a tedious process, so some vendors are offering ways to turn physical devices into cryptographic material, like physical unclonable functions based on variations in semiconductors.

> Organizations focus today on human instead of on machine identity. This needs to change!
>
> **Martin Kuppinger**
> KuppingerCole

Depending on the IoT device's type and capabilities (for example, CPU or storage type), the identifier can also range from an embedded identity, such as a serial number or certificate that is inserted in the device during manufacturing, to a hardware embedded secure element, like a Trusted Platform Module (TPM) cryptoprocessor. For devices that can't accommodate these embedded options, less secure methods are sometimes called for, such as analyzing environmental and behavioral characteristics, or a combination of one or more device characteristics, to coarsely identity it.

Although these methods are mostly proprietary, vendors do often offer a standardization layer on top of them, for example through the use of public key infrastructure mechanisms to provide a strong, unique, and immutable identity. Other vendors focus on creating their own cryptographic architectures better suited for large-scale deployments or on offering more fine-grained access management through cryptography.

Organizations focus today more on human identity than IoT/machine identities. This needs to change. 5G will be a major driver for much wider deployments. The slow-but-growing list of platforms or IoT-as-a-Service solutions will help with the management of IoT fleets. Unfortunately, there doesn't seem to be a lot of effort in standardization and interoperability across different platforms. Perhaps we should look at organizations like Kantara for interesting developments, rather than Amazon Web Services or Microsoft.

IDC We see a huge spectrum [of identity solutions]. Rising numbers of attacks, often widely reported in the media, have driven many IoT device manufacturers to implement more robust security controls in their products.

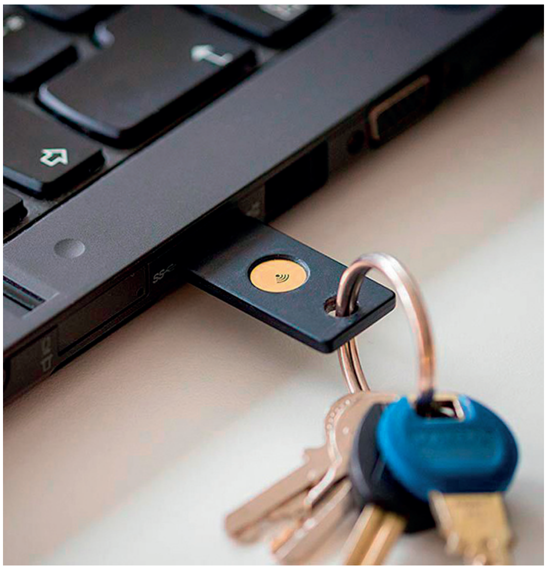
Organizations, particularly those in critical infrastructure sectors that have frequently been targeted, are much more aware of the security risks and vet their suppliers more closely, often including security criteria in their requests for proposal. There is a push for standards, particularly on mature western markets. This may represent the thin end of the wedge, however.

Connected consumer devices, everything from headphones and baby monitors to fridges, TVs, and even sex toys, are frequently shipped without any significant security built into them. For manufacturers, production costs, time to market, and profit margins are the business imperatives and, to them, security represents a cost.

Three things can change this. First, the implementation of strict standards and certifications. However, this is very challenging to roll out universally, particularly given the huge spectrum of devices being developed with Internet connectivity. Second, pushback from customers impacting demand but, when

IoT Devices under Heavy Attack

Rising numbers of attacks, often widely reported in the media, have driven many IoT device manufacturers to implement more robust security controls in their products.



source ©: KuppingerCole

How to Know Who's Who

Use Cases for IoT Identities

- IoT identity visibility (for example, IoT discovery on networks or PKI certificate management)
- Device management life cycle, from device registration to end-of-life or removal
- Device and platform security – encryption of communications and data, authentication to other IoT devices, applications, or services, validation/authorization (from access key information to identifying device permissions)
- Integration protocols and standards (including real-time APIs, representational state transfer, MQ telemetry transport)
- Monitoring of devices
- Compliance (data privacy and other standards or regulations)
- IoT analytics and reporting (real-time analytics, risk profiling, anomaly detection, artificial intelligence, and machine-learning-related services and tools)
- Connecting IoT identities with existing identity and access management systems

it comes to the consumer market, there is typically insufficient awareness to drive a sufficiently robust response to impact a manufacturer and cause it to improve its product. Third, the widespread reporting of hacked devices in the media – however, by then, in most cases it's already too late.

FR We are observing the whole spectrum from very sophisticated identity solutions implemented for IoT systems, to not even considering leveraging them for a company's IoT system.

One frequent question is if an existing IAM solution can be reused to secure IoT assets. The answer is that, while you can leverage your existing IAM platforms where possible, new tools and approaches will be required to bridge the gap between human and nonhuman identities. For example, in contrast to humans, machines never sleep and high-volume, high-velocity cryptographic key management becomes overwhelming; ID platforms or ID-as-a-Service might not be optimized for IoT identities.

How can we build IoT identities? What are the major challenges?

IDC Network access control (NAC) that enables organizations to gain visibility of devices, manage authentication and authorization, and enforce policies on users and devices. PKI can be a solution, it is based on existing standards and can work for many use cases.

Going further in identity, PKI provides secure and encrypted communications and authentication between devices, services, and users. Every device or thing can be given a unique identifier. Solutions exist from many vendors like Thales, DigiCert, nCipher (now known as Entrust), PrimeKey, and GlobalSign.

As with other security solutions, challenges come from different angles – from the lack of existing or available skills in managing PKI, to a lack of ownership in identifying who is responsible for deployments or, more generally, the lack of investment in IoT security.

According to IDC's 2020 European survey, only 42 percent of organizations embed security during the planning of a new initiative (including IoT deployments), the rest bringing it either as an afterthought or not at all (9 percent).

FR Extend your existing IAM platforms and use purpose-built tools to secure IoT identities, while aligning to a zero-trust model. Gain visibility into your IoT identities. Take inventory of the types of machine identities in your organization: where they reside, what they have access to, what permissions they have, and how they are managed and secured (or not). Understand the scope of your exposure, determine your maturity levels, and begin work on a remediation plan.

> ” Conduct annual security training for IoT asset owners and operators.
>
> **Bernhard Schaffrik**
> Forrester Research

Assess your current IAM solutions and providers, extend where possible. Traditional IAM controls may not work for the high-velocity, complex nature of new machine identities with human operators. However, centralize the directory or identity governance or privileged access vaults of both human and machine identities whenever possible, but be prepared that specific performance, usability, or protocol support requirements may mean you need added purpose-built tools and approaches.

Conduct annual security training for IoT asset owners and operators. All users working with IoT assets should go through cybersecurity training to understand how to manage their environments. Staying up to date on security protocols and risks will help companies avoid breaches resulting from user error.

Align your long-term strategy on the zero-trust founding principles. Focus on some of the main tenets of zero trust, including assumed breach and least principle.

Smart Utilities

COMING IN FROM THE COLD

Texas froze and the utilities stopped flowing. Gas supplies reduced by half and the electricity generators stopped turning. It seems **polar conditions can happen anywhere, so how can utilities use IoT to ensure uninterrupted delivery** to their customers?

By Gordon Feller

During the last decade, utility companies have been using their deployment of advanced metering infrastructure (AMI) for little more than automating the collection of billing data using smart meters. Some utilities are now extending this to improve operational data management to get the most out of their investment. This not only improves daily processes like billing, contract management, and customer service, but also helps them to instantly find power outages, predict which transformers are about to fail, monitor power quality, and identify grid balancing problems.

Utilities are continually improving AMI so they can ensure seamless installation, integration, optimization, and migration, while future-proofing their networks by introducing new advanced technologies.

As they go along, the companies are applying the lessons they learn and developing solutions to fill any gaps as they are identified. This approach is especially important in cybersecurity. No longer solely about defense security, it is also about the ability to limit organizational liability when harm occurs from a cyber incident. The companies are adopting, or developing, smart solutions designed to mitigate these exposures in a rapid, highly cost-ef-

fective manner. These tools address cybercrime and privacy concerns from a perspective which sees risk in terms of technology, process, people, and supply chain. A new type of cybersecurity monitoring service has become a big element of this, but the convergence of traditional and industrial networks with IoT devices is becoming increasingly more problematic.

Utilities are aiming toward a distinctive synergy of highly secure, integrated, automated demand management technology based on open standards. They are also aiming for extensive consumer-based demand-capacity market aggregation. This dual focus on technology and on the consumer market is enabling intelligent utilities to meet the challenges that lie ahead, providing the next generation of fuel supply mixes by including reliable and secure demand resources.

Houston, We Have a Problem

In February, a deep freeze devastated Texas and the *Texas Tribune* newspaper's front page revealed that the 29 million residents were just minutes away from a power outage that could have lasted for weeks or even months. All electricity and heating production, from both fossil and wind sources, was not installed with extreme cold weather in mind. In particular, ➔

methane gas wells and pipelines froze shut, reducing supplies by almost half.

As the energy companies begin the long repair process, the state's leaders are also taking the problem seriously and looking ahead to a world filled with new climate-change realities, such as an increase in the frequency of the polar vortex weather that caused the big chill. They're asking questions about how to achieve grid reliability when winter electricity loads are primarily sourced using natural gas.

In regions where natural gas is used for both electricity generation and the heating of buildings, extreme cold weather events place enormous stress on distribution. These incidents, as they become more frequent and less predictable, challenge the ability to meet demand. The suppliers now realize that this is more challenging than they'd ever expected. To achieve greater system stability, it's necessary to smooth grid demand by managing end-user demand through power cuts and mobile generators. Energy companies are evolving natural gas demand response (NG-DR) programs and deploying technology for dispatch during extreme cold weather events.

> Utilities are facing significant challenges to meet a changing fuel supply mix.
>
> **Dave Paradise**
> VP for smart grid at IPKeys

source ©: LinkedIn Corporation

One emergent strategy that embraces IoT technologies is being used by smart utilities to implement controls that reduce load through automation. It provides a secure and inexpensive means of preserving precious grid resources while minimizing the impact on consumers by rotating the use of selected equipment. Sharing the available resources by turning off equipment for small periods of time means everyone can enjoy the essential resources of heat and hot water.

Preparation and planning that includes demand response provides a tangible method of mitigation for incidents like the recent Texas fiasco. Such events are not unique; spikes in electricity and gas consumption occur whenever extreme conditions impact the grid. Though the Texas grid operator had issued a warning that the incoming snowstorm might bring record electricity usage, it didn't anticipate the freezing of gas wells and pipelines. Managing less critical loads, such as hot water boilers, washer dryers, or even stoves, would have lessened the negative impacts on the grid.

IPKeys Power Partners a smart-grid technology provider, has developed IoT devices to enable real-time, power-demand management capabilities. By implementing several actions – such as weather-based, load-consumption forecasting, preheating, dual fuel switching, and smart resource cycling – utilities can increase resiliency and deliver reliable supply during adverse weather events.

Robert Nawy, CEO of IPKeys, says, "This IoT technology and demand management approach helps reduce the need to build more pipelines. It also provides a 'virtual pipeline' for those polar vortex days that we're seeing more often."

The Way to Save
Jim Boch, Chief Engineer at IPKeys, demonstrates the Integrated Automated Demand Management (IADM) platform, which gives utilities reliable and secure demand resources and potentially saves billions of dollars in plant replacement investments.

source ©: IPKeys Power Partners

Heat of the Moment

On the road to becoming intelligent utilities, power companies are working hard to acquire and adopt IoT technologies. Companies like IPKeys are building products based on Open Automated Demand Response (OpenADR), which offers a highly secure, two-way information exchange protocol, based on open standards, for building certified and

source ©: IPKeys Power Partners

Smart Box

The Energy Interop Server & System (EISS) BOX 3.0 by IPKeys allows real-time telemetric control of energy consumption, which can potentially lead to huge cost savings for utilities.

secure servers and devices for smart grids. Development of the standards is guided by the OpenADR Alliance, whose stated aim is to "standardize, automate, and simplify demand response and distributed energy resources." The resulting framework enables utilities and aggregators to manage growing energy demand and decentralized energy production cost-effectively, while enabling customers to control their energy consumption. The Alliance is supported by IPKeys Power Partners, Pacific Gas and Electric (PG&E), SoCal Edison, and the US Department of Energy's Lawrence Berkeley National Labs.

IPKeys' demand management and response solution is based on its Energy Interop Server and System (EISS), which provides server-side communications and client-side interfaces to give utilities and their customers greater control over power consumption and economies. According to Nawy, "Additional benefits are realized by using this natural gas efficiency approach. We enable capital savings and cost deferral, and we help reduce and control peak demand in ways that take into account system capacity, weather, and demand forecasts. Ultimately, NG-DR creates an environmentally friendly way to create a more dynamic, flexible gas system that better serves the customer's real-time needs."

Jim Boch, chief engineer at IPKeys, adds, "NG-DR data also enables a new perspective for system modeling and load planning. Whenever natural gas distribution systems are strained and delivery is jeopardized, customers can use our technology platform. They are delivering a result the customers want: greater reliability."

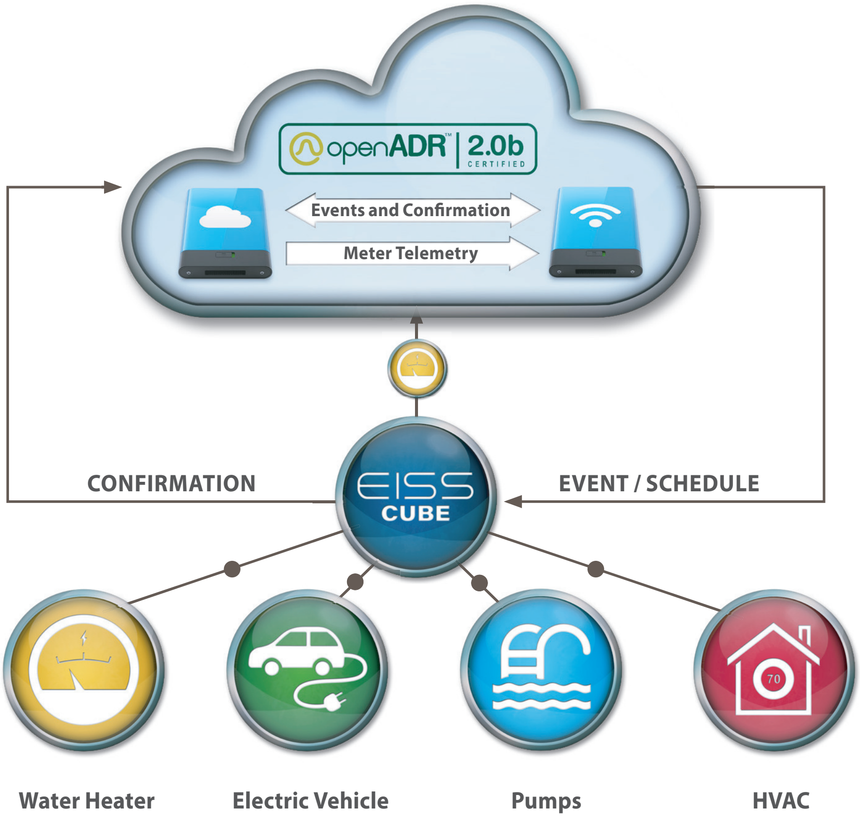
The smart meter investments in the electric market are not so common in the natural gas field. The ability to measure the real-time demand reductions in gas would be an expensive retrofit. The IPKeys platform solves previous challenges of natural gas meter reading in real time by adding control of gas-consuming appliances, without the need to invest in an AMI network. Smart meters enable measurement and verification (M&V) to provide granular interval metering and ensure load reductions can be made on a non-invasive basis.

Demand response programs have long been used to curtail summer electric loadings, but they have not yet been adopted by gas companies or their customers during the winter months. For this reason, NG-DR provides much-needed relief during demand spikes and moments of supply constraint, which are now being heightened by increasing environmental stress.

Natural gas pipeline suppliers are looking to their electric utility counterparts for best practices that show how to implement cutting-edge IoT technologies. These are critical to the fortification of their networks and grid-resiliency operations. NG-DR moves utilities closer to their "intelligent" goals, making it possible for them to serve existing customers during extreme weather events without building new pipelines. It also makes it possible to use existing assets and couple them with advanced IoT technologies.

Back and Forth

EISS® Cubes are small two-way transmitters designed to monitor and manage the electrical activity of a variety of residential/small-business electrical devices such as lighting controllers, distributed generation, HVAC units, plug-in electric vehicle chargers, and simple industrial control units.



source ©: IPKeys Power Partners

Disaster Prevention

WEATHER OR NOT?

From prediction to recovery, **IoT is helping humans to cope with extreme weather and other threatening phenomena on our fickle planet** – effectively putting Mother Nature on the defensive.

By Allan Earls

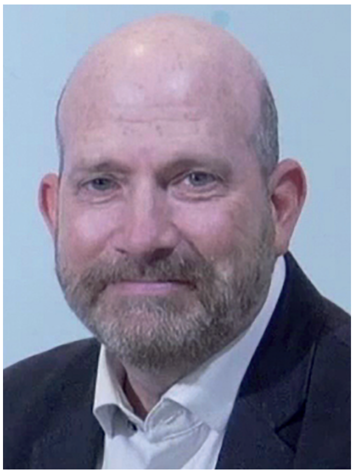
More than a century ago, British writer Oscar Wilde asserted that "conversation about the weather is the last refuge of the unimaginative." Today, though, there really is something to talk about. Hurricanes, storms, floods, and tornadoes, not to mention drought, wildfires, and other natural disasters, are, by some measures, becoming more frequent and certainly more costly, causing nearly a trillion dollars of economic losses annually in the United States alone. Fortunately, IoT innovators around the world are harnessing technology to make extreme conditions more predictable and to help people weather the weather better, as well as helping to manage other dangerous natural phenomena.

It can be somewhat sobering to realize that recording and measuring the weather is a relatively new activity, only begun in an organized way, fitfully, toward the end of the 19th century and then only conducted at scale and with rigor much more recently. A limiting factor was the cost of instruments and the complexity of gathering data from them, originally an entirely manual process. Now, through ubiquitous inexpensive sensors (as well as computers and sophisticated software and communications networks) a much more fine-grained view of the weather is emerging.

source ©: American Meteorological Society

> Climate and weather change call for unprecedented levels of accuracy.
>
> **Bill Gail**
> CEO of Global Weather Corporation

> Instead of sending crews out, we use remote devices and built-in intelligence to send us alerts.
>
> **Matt Smith**
> Senior Director, Itron



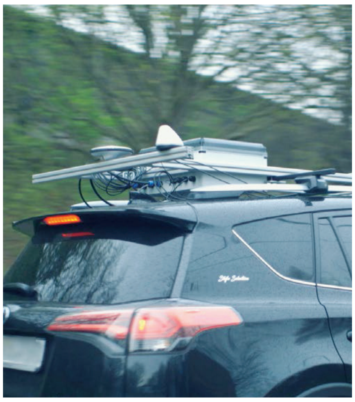
source ©: Smart Energy International

The results are said to be already improving human life and safety. In Liberty Lake, Washington State, Matthew Smith, senior director of grid management at Itron, a provider of technology for energy and water resource management, agrees. He says recent advances in technology, such as smart sensors and advanced analytics, can help communities better predict, prepare for, and respond to natural disasters. For example, a sensor on a utility pole can now detect in real time if a pole is down. Remotely detecting damage and outage severity this way can accelerate response times.

"Rather than sending crews out to 'drive the lines' to discover problems, cities or utility companies can use remotely connected devices and line and fault sensors to acquire much-needed intelligence and send repair crews with the equipment needed to restore service quickly," says Smith.

Similarly, smart meters can aid in natural disaster mitigation. With smart meters, organizations know instantly when and where the power is out, thanks to built-in intelligence which can diagnose problems remotely and send an outage alert as soon as it happens. In Houston, when Hurricane Harvey made landfall in August 2017, more than 250,000 people in Texas lost power. "Equipped with smart grid technology prior to this disaster, CenterPoint Energy was ➔

source ©: Imec



source ©: Imec

Test as You Go

Testing and validating new communication, data, and sensor technologies is a job for connected cars in the Smart Highway project.

source ©: Round Table 21 Tienen

> Hi-res images and temperature sensors can be integrated into protective equipment.
>
> **Wouter Charle**
>
> Manager for hyperspectral imaging technology at Imec

able to recover and reconnect people to power quickly, avoiding an estimated 45 million outage minutes for its customers," says Smith. In addition, distribution automation devices, such as smart-grid switches, allowed the utility to quickly isolate problems and restore service to customers.

Another area where many people are impacted by weather is when traveling. Bill Gail, cofounder and CEO of Global Weather Corporation (GWC), is working on how to deal with one of the weaknesses of smart, connected vehicles – the weather. He says climate and weather-related challenges are driving a need for unprecedented levels of accuracy. This challenge cannot be met with traditional weather-data resources – it requires innovations such as road-level precision data, and more, according to Gail.

> Our sensors can help to reduce fire risk in the western parts of the US.
>
> **Tim Barat**
>
> CEO at Gridware

source ©: Gridware

Designed for the mobility industry, GWC's RoadWX weather forecast provides new levels of detail to increase safety and provide critical decision support for navigation planning, autonomous vehicle availability, fleet management, and driver safety alerts. The forecast provided is based on machine learning, sensor data gathered from vehicles, Road Weather Information System (RWIS) sites, and other, more traditional, sources of weather information.

From Ice to Fire

It provides a forecast from the present time to up to 48 hours into the future. According to the company, the RoadWX forecast can now distinguish between five different kinds of road surface conditions – dry, near dry, wet, slush, and ice or snow, providing for optimal routing and better tuning of driving behavior to actual conditions.

Weather can contribute to starting and sustaining wildfires and, here again, technologists are using sensor technology and "smarts" to stay ahead of the flames. As of late 2020, some 44,000 individual wildfires in the US had scorched nearly 7.7 million acres of land, one of the highest ever annual totals and mostly in western states.

An airborne network of information tools can also help. One such tool is drone technology, which is largely used to collect information about the location and magnitude of ongoing fires, to protect firefighters from potential dangers and alert the public to impending danger.

Wouter Charle is team leader and manager for hyperspectral imaging technology at Imec, a research and innovation organization in nanoelectronics and digital technologies. According to Charle, the organization has built several "hyperspectral" technologies, designed to provide images in greater detail than traditional visible-spectrum camera systems and applicable to both forestry management and wildfire surveillance. Another wrinkle of the technology is added by putting similar camera technology and temperature sensors into the firefighters' protective equipment to allow supervisors and firefighters to accurately assess the level of danger.

Gridware is another IoT company that is building a network of sensors to try to reduce fire risk in the western US. Many of those fires have been traced to sparky interactions between animals or vegetation and the power transmission lines. Long stretches of power lines often run through areas that are hard to access and maintain – detecting a fire in these regions before it grows exponentially has always been difficult. One costly and unpopular solution has been to shut down power in areas considered to be at imminent risk of fire.

Improvement Needed

The solution that Gridware envisions is built on attaching an IoT guard on each utility pole which can then continually report on damage or equipment failures when they are still manageable, with very precise indication of exactly where the problem lies. Providing masses of data that can be monitored and analyzed is key to enabling preemptive corrections or rapid response and repairs to be made.

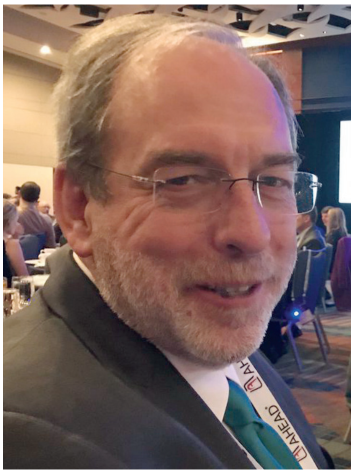
"We are exfiltrating data with a combination of cellular, mesh, and satellite connectivity," explains Gridware CEO Tim Barat. The company provides an end-to-end solution that provides decision makers with the critical information they need to manage their infrastructure. "We also expose APIs that plug raw or processed data directly into existing analytic systems," he adds.

Water, Water Everywhere

Although wildfires are the primary destructive force at work in the western US, in other parts of the country and around the world, it is water – riverine flooding, tidal events, and so on.

Semtech, a supplier of analog and mixed-signal semiconductors and advanced algorithms, has worked with environmental technology firm Green Stream to create a system comprising LoRa (Long-Range) devices and wireless radio frequency technology with Senet's LoRaWAN-based network to connect flood sensor systems. The entire project is built around standard, low-cost components – the kind that are propelling IoT growth in these and other new applications. According to Jim Gray, CEO of Green Stream, "In many coastal towns and communities, rising water as a result of tides or rain can present a large threat."

> In coastal towns, rising water due to tides and rain present a large threat.
>
> **Jim Gray**
> CEO of Green Stream


source ©: Twitter

source ©: GreenStream Technologies

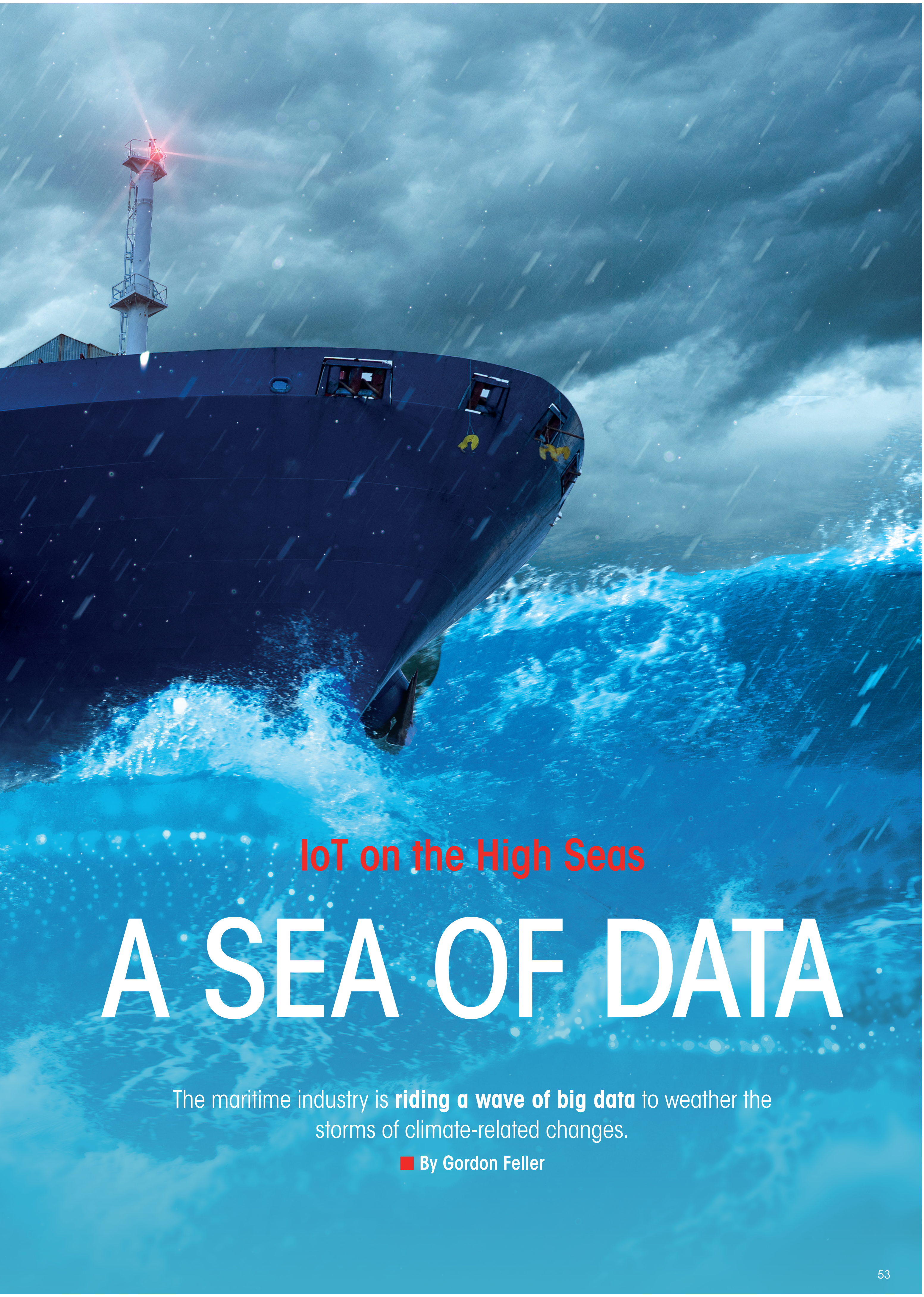
An Eye on the Sky
At Washington's Liberty Lake, Itron monitors weather conditions and water resources through smart sensors and advanced analytics to better prepare for disaster.

Semtech says Green Stream's flood monitoring uses ultrasonic sensors and LoRa-enabled gateways. Data moves over the LoRaWAN network, which can support on-demand build-out and management of IoT connectivity. The sensors are autonomous, solar-powered, wireless devices which don't require external power, so they can be mounted on many kinds of infrastructure near bodies of water.

IoT isn't just about responding to disasters, it's also about fine-tuning. For example, Schneider Electric, the French energy management and automation company, has connected more than 4,000 of its weather stations in disparate rural areas to its big data and IoT-enabled WeatherSentry platform to create more precise forecasts. Using the technology, agricultural interests can prepare better than before for frost conditions or respond to excessive rain – or to droughts – that could impair crop production.

Further out on the leading edge, Google is building a worldwide earthquake alert system. If a user opts in, the accelerometer in their Android phone will become part of a network designed to detect earthquakes in real time.

Taken together, this emerging world of outdoors IoT will give humans unprecedented insights and allow us to, if not control, at least exercise a much greater ability to work with Mother Nature.



IoT on the High Seas

A SEA OF DATA

The maritime industry is **riding a wave of big data** to weather the storms of climate-related changes.

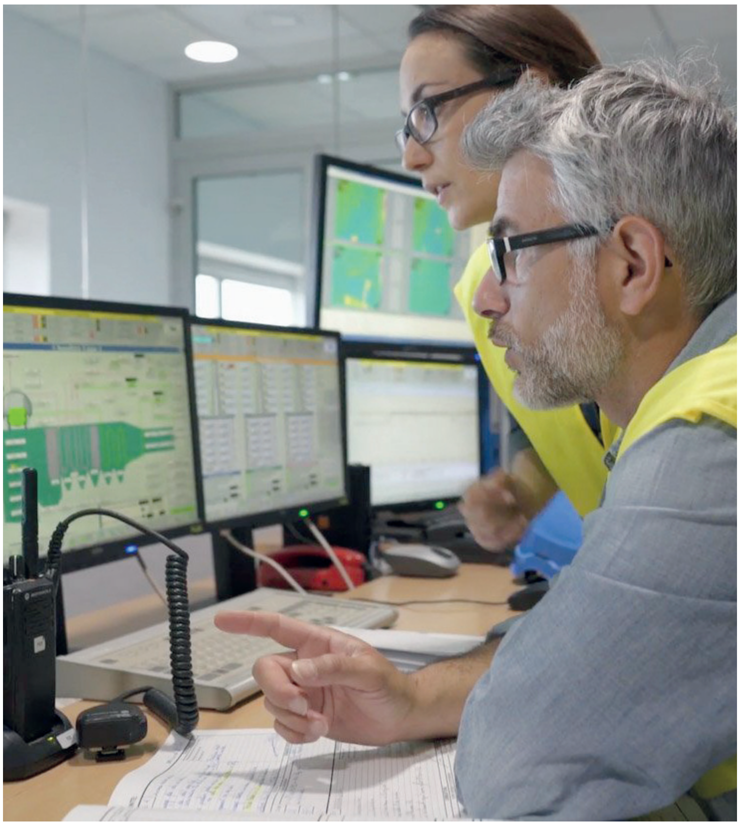
■ **By Gordon Feller**

More than 90 percent of the world's trade volume is moved by sea, amounting to more than $4 trillion worth of goods every year. This places immense pressure on shipping companies to remain on schedule, protect the cargo ships and crews, and ensure profitability – not trivial tasks. The maritime industry comprises an intricate system of transportation with around 90,000 vessels crossing paths as goods are transported from one continent to another. This makes it hard to visualize the world's main shipping routes or to comprehend the industry's complexity.

To further complicate things, ports and vessels are subject to forces of nature which are becoming harder to predict. This means that shipping companies must be able to adapt to changing situations and act fast. Real-time big data analytics is helping them to navigate these unexpected challenges more efficiently.

Big data analysis extracts and scrutinizes information from data sets that are too large or complex to be dealt with by traditional data-processing application software. Real-time capabilities mean that those insights are delivered immediately after collection.

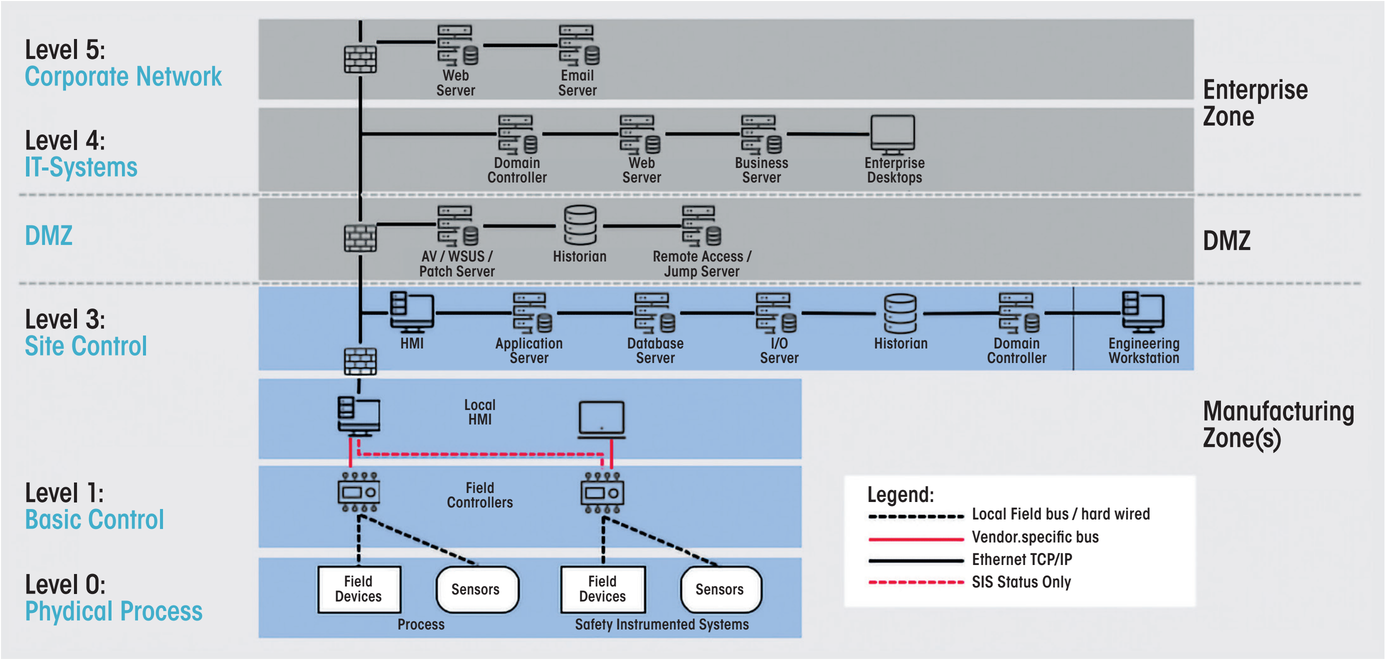
Maritime companies generate data from numerous sources in several formats. Actioning this fixed, siloed, and inconsistent information is time-consuming and a major pain point for shipping companies, but the inflow of data can be collated and organized in a cloud-based system using big-data tools. The system analyzes and spits out the relevant data in real time, which can promote better decision-making. Nothing is left to intuition or chance, unlocking



Keeping Watch

Protecting vessel networks against brute force or denial-of-service (DoS) attacks, as well as unintended/accidental operator actions calls for continuous monitoring of network IP levels, network mapping, and asset discovery.

source ©: Mission Secure



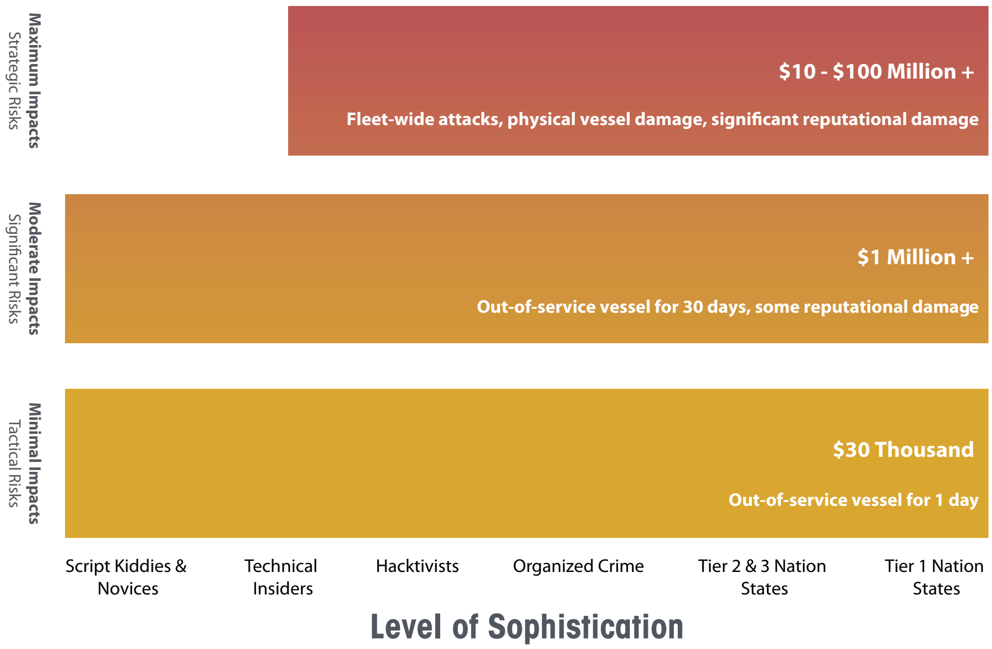
Never Let Go

As maritime organizations review and adjust their security architectures, one of the recommended frameworks for them to adopt is the Purdue model. The goal is to stop hackers from taking over navigation and communications systems, open or close critical valves, or take over propulsion and rudder controls.

source ©: Mission Secure

opportunities to drive greater efficiencies.

Maritime Cybersecurity Business Risks



source ©: Mission Secure

Efficient Maritime Operations and Logistics

Overall operations and logistics become much more efficient with real-time data. Companies can obtain information through GPS trackers and RFID tags to help locate ships and containers immediately. Data technology also helps synchronize communication to manage ship arrivals, berthings, and departures safely and efficiently. In cases of an emergency, nonavailability of labor, or terminal allocation problems, real-time data helps managers to plan shipping routes and speeds accordingly.

Climate change is making this ability to pivot increasingly necessary. Ocean conditions – currents, waves, and wind – are more unpredictable than ever, making the use of real-time data to streamline decision-making and support ad hoc navigation vital to ensure companies can maximize returns.

Fuel-Efficient Routing

By having access to sea-state observations, vessel operators can reroute according to current conditions while optimizing fuel efficiency. Inefficient weather routing often leads to an increased time spent at sea, which not only disrupts and delays the supply chain but can also increase fuel burn and CO^2 emissions.

In addition to increasing voyage earnings, fuel-efficient routing also reduces greenhouse gas (GHG) emissions, supporting the latest reduction strategy developed in 2018 by the International Maritime Organization (IMO). This initiative envisages that the total annual GHG emissions from international shipping should be reduced by at least 50 percent by 2050, compared to 2008 figures. As documented in its report, the IMO calculated that vessels released 1.12 billion metric tons of carbon dioxide in 2007. Emissions therefore need to be reduced by 560 million metric tons, equivalent to the emissions from 102 million cars.

One key conclusion to draw about the real world is that the real-time data helps to reduce fuel costs and helps to bring down GHG emissions. It's possible that the maritime industry could become bigger and better – and more lucrative – while releasing fewer GHG emissions.

The convergence of information technology and operational technology on board ships – and their connection to the Internet – creates an increased attack surface that requires greater cyber risk management.

On the IT side, the chances of cyberattacks can be mitigated through proper implementation of encryption techniques, such as blockchain technology. From an operational standpoint, IMO maintains that effective cyber risk management should start at the senior management level – embedding a culture of cyber risk awareness into all levels and departments of an organization. One can read more about this in the Baltic and International Maritime Council's (BIMCO) "Guidelines on Cybersecurity Onboard Ships."

Knowledge is power. By implementing real-time insights in daily operations, shipping companies are well-prepared to navigate anything that comes their way. Based on how this year has gone, it certainly doesn't hurt to have an edge on the unexpected.

The New Piracy

Ships and other vessels may seem like unusual targets for cyberattacks. But with their growing use of industrial control systems (ICS) and satellite communications, hackers have a new playground that's ripe for attack.

Full Steam Ahead

With modern Mission Secure platforms, IT organizations and ships' crews can observe and map on-board network connections and defend against intrusions through the use of logical security zones and other protections.

source ©: Mission Secure

Sustainable Investment

IOT FOR GOOD

The pandemic has served as a reminder of how fragile our society, infrastructure, and business models can be. It's also highlighted how **technology can carry us through the disruption of 2020 and create more resilient and sustainable business models** that offer a better future.

By Bee Hayes-Thakore

BlackRock CEO Larry Fink's regular letter to CEOs highlights environmental, social, and governance (ESG) criteria as the major key to creating enduring value for all stakeholders. For those not familiar with the jargon, ESG are the three metrics that measure the sustainability and societal impact of a company's investment in the pursuit of improved financial performance. His comments are backed up by a staggering 96 percent increase in sustainable investing since 2019.

Factoring corporate social responsibilities (CSR) into our organizations is nothing new, but it is taking on new meaning as our attention turns to importance in a post-pandemic world. As governments act on climate change and sustainability, they increasingly

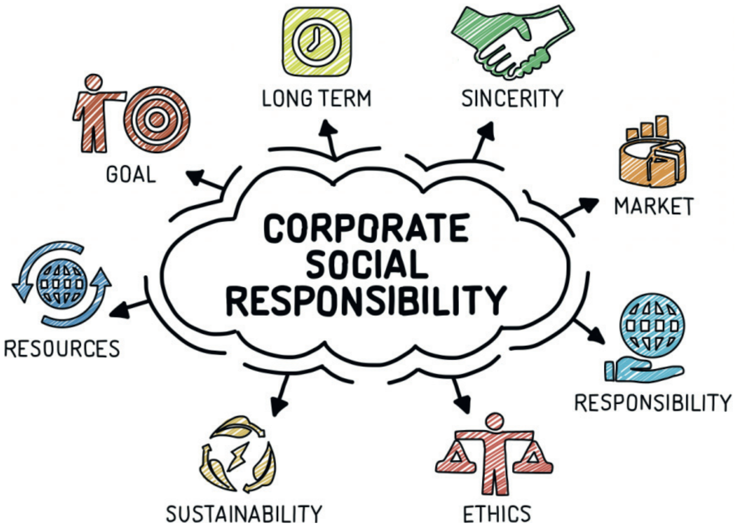
expect companies to do the same. At the same time, consumers and clients are also increasing the pressure on companies to show commitment to sustainability topics. An important driver in Q4 2020 was the policy agenda of the newly elected US president Joe Biden, who immediately returned the US to the Paris Climate Agreement upon his arrival in office.

As a global leader in digital security and securing IoT devices, we at Kigen see in our discussions how IoT and sustainability are rising up the leadership agenda. External data supports it too: according to IoT Analytics, the terms "IoT" and "sustainability" are being used with increasing frequency, with the word "sustainability" being mentioned 52 times per 100 earnings calls in Q4 2020. That's a 23 percent increase compared to Q3 and an 86 percent increase compared to the same quarter in 2019. This renewed interest in sustainability means companies from all sectors are reassessing how their products, services, manufacturing, and supply chains can become more sustainable.

A World Economic Forum report notes that IoT projects can contribute to the 2030 Agenda for ➔

> Companies are reassessing their products, services, and manufacturing.
>
> **Bee Hayes-Thakore**
>
> Senior Director for Marketing and Partnerships at Kigen

source ©: LinkedIn Corporation



source ©: TheGivingMachine

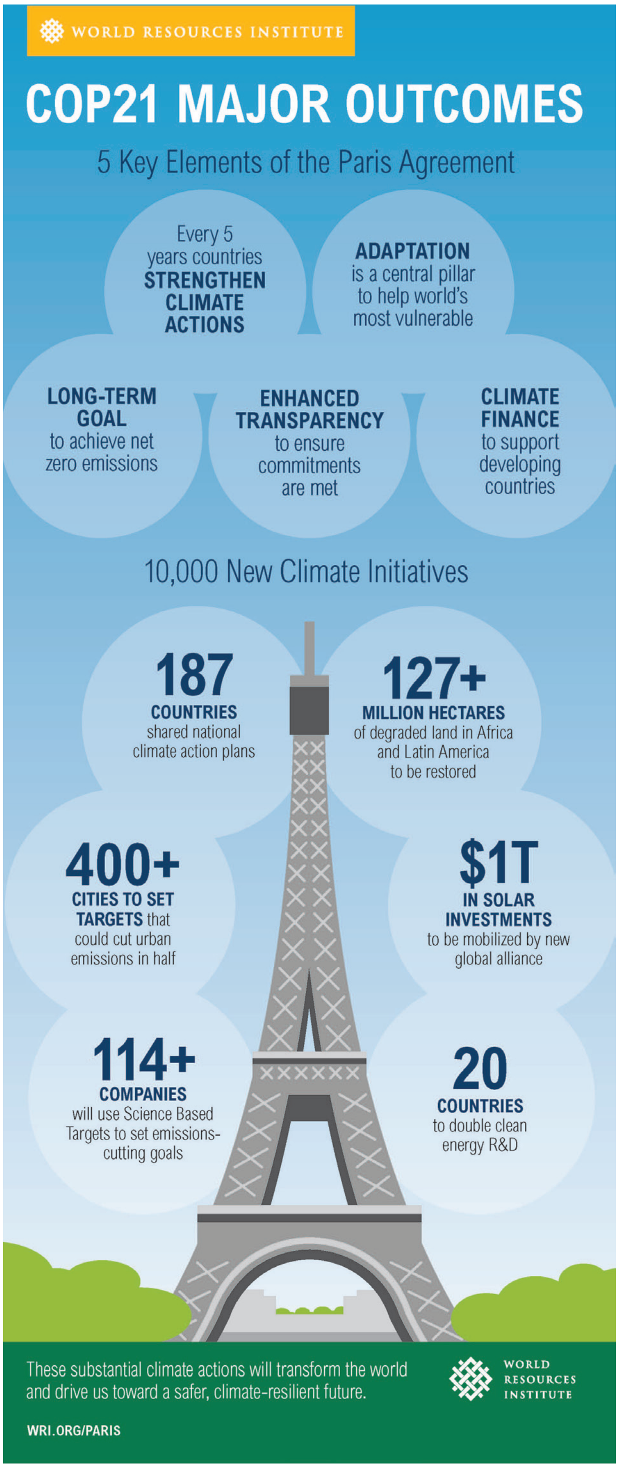
Sustainable Development

Corporate social responsibility (CSR) is the responsibility of an organization for the impacts of its decisions and activities on society and the environment that is consistent with sustainable development and the welfare of society.

Sustainable Development, including 17 Sustainable Development Goals (SDGs) set by the United Nations. These goals encompass efficient water use, fighting climate change, and ending hunger and food insecurity, among others. The IoT can become a force for good by offering actionable insights that lead to more sustainable decisions. Here are three key areas where IoT is making an impact in sustainability:

Back on Track

With the US under Joe Biden back on board, hopes that the Paris Climate Accord, or COP21, will achieve its goal of reducing greenhouse gas emissions are on the rise again.



WORLD RESOURCES INSTITUTE

COP21 MAJOR OUTCOMES

5 Key Elements of the Paris Agreement

Every 5 years countries **STRENGTHEN CLIMATE ACTIONS**

ADAPTATION is a central pillar to help world's most vulnerable

LONG-TERM GOAL to achieve net zero emissions

ENHANCED TRANSPARENCY to ensure commitments are met

CLIMATE FINANCE to support developing countries

10,000 New Climate Initiatives

187 COUNTRIES shared national climate action plans

127+ MILLION HECTARES of degraded land in Africa and Latin America to be restored

400+ CITIES TO SET TARGETS that could cut urban emissions in half

$1T IN SOLAR INVESTMENTS to be mobilized by new global alliance

114+ COMPANIES will use Science Based Targets to set emissions-cutting goals

20 COUNTRIES to double clean energy R&D

These substantial climate actions will transform the world and drive us toward a safer, climate-resilient future.

WRI.ORG/PARIS

WORLD RESOURCES INSTITUTE

source ©: World Resources Institute

Smart utility companies are finally making headway in their effort to modernize infrastructure to optimize efficiency and improve sustainability. According to UNESCO, 70 percent of the water used for crops around the world is fresh water. So, developing intelligence around our resource usage and efficient irrigation ensures sustainability and productivity.

Seamless cellular connectivity, particularly LPWAN networks such as NB-IoT and LTE-M, have enhanced the penetration of smart metering solutions and near-real-time intelligence of consumption or wastage data. With eSIM and remote SIM provisioning, smart meter manufacturers are quickly innovating to comply with regulatory specifications and higher cybersecurity standards and expand their supply chain through ecosystems committed to interoperability.

For smart-grid-ready solutions, flexibility is key. This flexibility also opens up new possibilities in how data can generate revenue streams for utility providers, positioning them as broader service providers. The example of pioneering work by Iskraemeco, a Slovenian manufacturer of metering solutions, offers a blueprint for anyone managing a greater diversity in resource generation or transport as the world moves to smarter grid intelligence. As the IoT guidelines on sustainability from WE Forum highlight, the global shift to a more resilient, reliable smart grid is dependent on addressing how utility companies can avoid lock-ins, reduce fragmentation, and build stronger customer relationships with end users.

Micromobility presents a tremendous opportunity, having stormed from city to city in just two years, helping to address some of the most vexing transportation challenges facing urban areas: congestion, emissions, air quality, and inconsistent access to transit. According to research, if the share for e-bike riding rises to 11 percent, we could see a 7 percent decrease in CO^2 emissions from the urban transport sector by 2030 – potentially accounting for over 50 percent of urban trips in the US and 70 percent in cities like London.

Behind the scenes, micromobility solutions are complex. They connect a diversity of stakeholders – government and city councils, product manufacturers, and platform operators – across a fragmented value chain and force them to work together to develop innovative ways to make transportation safer, cleaner, more efficient, and more fun. Their success lies in the simplicity they present to the users, who will only change their behaviors if the services offered are significantly more convenient, trustworthy, and reliable. Those who sign up to use e-scooters also offer up a great deal of personal and sensitive data, including billing information and other involuntary analytics, such as location and individual vehicle information. To ensure that the early benefits of greening our cities are realized, companies need scalable security models standardized for trusted services and privacy frameworks. GSMA's IoT-SAFE security scheme is a perfect example supporting this market's growth, strengthening the promise and social contract with users.

Smart Tracking

The Covid-19 pandemic has laid bare many of the long-standing vulnerabilities and risks lurking in organizations' supply chains. It has intensified the need for better data in understanding operations and supplier traceability and transparency – all critical to meeting the commitments to sustainability and better planning. The key to automated, predictive, and prescriptive operations management in the post-Covid-19 world lies in the interconnectivity of digi-

Everything under Control
IoT-based smart farm monitoring systems for paddy fields measure water levels, moisture, temperature, and humidity through sensors installed in the field.

tal tools, physical infrastructure, and their underlying data streams. Smart businesses are embracing that insight, and data-driven thinking, from the initial design through to the complete customer experience, is critical to stay ahead of the competition. Take the example of Bayer, the global leader in pharmaceuticals and life sciences, who have set a target to support 100 million smallholder farms to produce for our growing global population ecologically. This requires sustainable means of intensifying food cultivation and helping farmers worldwide take advantage of the best-quality seeds and crop protection. With over 130 production facilities globally, Bayer not only wants to ensure that high-quality product reaches their customers at the right time but also synthesize it with over 30 different streams of data to offer a farmer-centric solution to enable better yield.

Often, the challenge at such scale lies in the simplification through empowerment, rather than taking away hundreds of millions of farmers and traders from their core focus. Bayer turned to use an innovative, low-power cellular-connected IoT tracking solution enabled by the integrated iSIM. By doing so, the information needed to predict adverse events such as delayed weather patterns or changes in local rainfall all becomes an opportunity to contribute toward sustainability for the planet and our people.

With the evolution of the SIM and the advent of iSIM, the story of IoT is being rewritten, opening new opportunities for companies to address global challenges and meet their sustainability goals. The most successful businesses will be the ones that facilitate the exchange of data in a streamlined and interoperable manner that leads to actionable insights, presenting benefits for all. Technology is an enabler, as trust and transparency increasingly become hallmarks of progressive businesses that customers choose for their needs. What areas of IoT do you think are most exciting for smart businesses to meet their sustainability goals? Join Kigen's conversation #futureofSIM on LinkedIn.

बेटर लाईफ फार्मिंग
उदघाटन समारोह
बेटर लाईफ फार्मिंग सेन्टर अलावलपुर जिला गाजीपुर
मुख्य अतिथि - मा0 सूर्य प्रताप शाही जी
मंत्री-कृषि,कृषि शिक्षा एवम कृषि अनुसंधान (उ०प्र०) सरकार
दिनांक –5 - 09 - 2020
स्थान– मुबारकपुरनेत, अलावलपुर –गाजीपुर
BAYER
Bayer
IFC International Finance Corporation
YARA
NETAFIM
DeHaat
agribazaar
big basket

Bringing the Farmers Around
Bayer, the global leader in pharmaceuticals and life sciences, has set a target to support 100 million smallholder farmers to switch to sustainable means of food cultivation.

source ©: Better Life Farming

Microsoft Windows IoT

BACK TO THE ROOTS AND UP IN THE CLOUD!

This autumn Microsoft release the next version of **Windows 10 IoT Enterprise LTSC.**

With Windows 10 IoT Enterprise 2021 LTSC you leverage your existing knowledge to build and manage Windows IoT devices with powerful tools and technologies to quickly unlock data and drive digital transformation.

It helps you connect your devices to each other, your network, and the cloud, so you can use data to drive real business insight and create new business opportunities. Some changes are well known from the Windows 10 Enterprise SAC versions.

Like the support for ARM platforms. As well as the point, that Windows 10 IoT Enterprise LTSC will only be available as 64bit software version.

> ” Windows 10 IoT Enterprise Part of a comprehensive IoT platform from Microsoft.

Reduced OS footprint

One of the biggest changes will come with the possibility to reduce the baseline OS footprint (OS image + reserved space for quality updates) to <8 GB storage. This will be realized by removable OS packages and an in-memory footprint reduction.

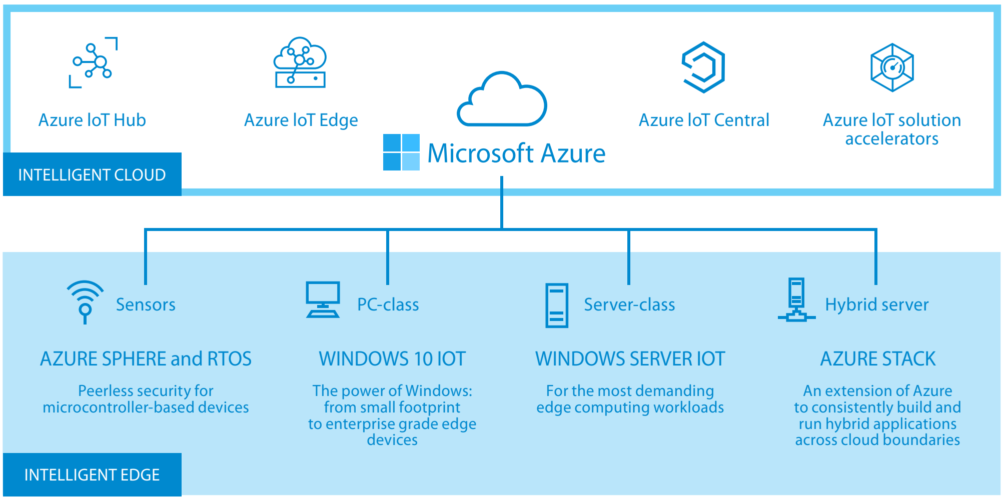
In addition you will be able to safely disable System Services. This allows the build of low-cost devices with 16 GB storage / 2GB RAM.

Dual Focus Touch & Input

With Windows 10 IoT Enterprise 2021 you can build an IoT device with dual input and dual monitors to provide an interactive experience for two users who will use the device simultaneously (two in-focus apps). That's a huge improvement for Point-Of-Sale devices and Medical devices, to name just a few. One additional point to mention here is the Kiosk mode, which is now available in Edge (Chromium).

Microsoft IoT Platform

Seamless from IoT Edge to Cloud


Azure IoT Hub
Azure IoT Edge
Microsoft Azure
Azure IoT Central
Azure IoT solution accelerators
INTELLIGENT CLOUD
Sensors
PC-class
Server-class
Hybrid server
AZURE SPHERE and RTOS
Peerless security for microcontroller-based devices
WINDOWS 10 IOT
The power of Windows: from small footprint to enterprise grade edge devices
WINDOWS SERVER IOT
For the most demanding edge computing workloads
AZURE STACK
An extension of Azure to consistently build and run hybrid applications across cloud boundaries
INTELLIGENT EDGE

Device Update Center

IT organizations have long recognized the productivity and security benefits of using Microsoft throughout the organization. The same benefits accrue to organizations that run Windows 10 IoT on their embedded and mobile devices, too. Microsoft implemented a new way to certify and control the update rollout to your appliances through Device Update Center service.

This Azure subscription service provides a full range of device management tools across IoT cloud, enterprise cloud, and on-premises.

This Service Business Model for Device Builders is already available for Windows 10 IoT Core.

Soft Real-Time

The soft real-time support in Windows 10 IoT Enterprise 2021 allows developers to build software and systems around timing assumptions. It offers real-time performance with a small-time window for program completion. So an improved Quality of Service for time-bound use cases is available and you can easily develop apps via familiar Windows APIs. Keep in mind, it's not a hard real-time OS.

Visit us now at www.msembedded.biz

Security Update Support

Another big change will be the support for the OS. Windows 10 Enterprise 2021 will come with 5 years of support. Since Microsoft is heavily committed to their IoT partners, Windows 10 IoT Enterprise 2021 LTSC will still have 10 years of Microsoft support and 10 years of product availability.

Improved IoT UX

If you choose frequent updates to keep devices safe and functional, Windows 10 IoT Enterprise LTSC is additionally tailoring this experience so that your device maintains a branded experience.

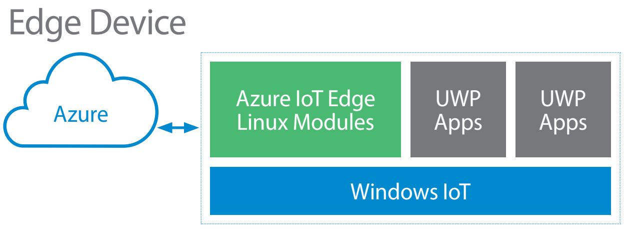
Making the update experience less “distinctively Windows” and remove references to Windows from the update settings is one change.

Keeping your device on brand for its designated purpose and removing references to “computer” or “PC” from update settings is another one. You can now customize the update screen background color to match your branding and configure accent color settings.

Shell Launcher v2

Shell Launcher v1 was unable to run UWP apps. With Shell Launcher in Windows 10 IoT Enterprise 2021 LTSC, Microsoft introduces a modern Shell Launcher experience that can:

- Automatically launch a Win32 / UWP app on user logon
- Suppress a set of Windows user experiences by default (Start menu / Taskbar / Action Center, etc.)
- Monitor lifecycle of the primary app and restart it when exit
- Allow launching other apps from the primary app acting as a custom shell
- Manage app views with multi-monitor support
- Support configurations via WMI / MDM


Edge Device

Azure

Azure IoT Edge Linux Modules

UWP Apps

UWP Apps

Windows IoT

> Built on the foundation of over 1 billion active Windows 10 devices.

Azure IoT Edge for Linux on Windows (EFLOW)

Windows 10 IoT Enterprise 2021 LTSC is optimized for IoT Workloads, to run Win32, UWP, and containerized Linux workloads side-by-side with interoperability between them. Microsoft simplified the Azure integration by running Azure IoT Edge modules in a Linux container. That gives you the best-in-class device security, with additional lockdown and branding capabilities, to easily create appliances, kiosks, digital signs, HMI, gateways, etc.

	IoT Core	IoT Enterprise	IoT Enterprise 2021	
Better Azure IoT Edge Support			✓	Run Linux version of Azure IoT Edge on Windows (EFLOW)
Run Linux Workloads in Containers			✓	Run Linux AI modules from Azure Marketplace (EFLOW)
Full Range of Intel Silicon		✓	✓	Support Device Portfolio Expansion
Small Footprint	✓		✓	Min HW spec = 16GB/2GB, smaller than current IoT Enterprise, but not as small as IoT Core (4GB/1GB)
Appliance Features	✓		✓	More Lockdown & Branding Control
OEM Controlled Update	✓		✓	Validate & manage updates using Device Update Center
On-Prem Device Management	✓	✓	✓	Manage devices wit familiar SCCM and WSUS tools
Full Win32 Support		✓	✓	Leverage existing Win32 software &expertise

Smart Elevators

GIVING IOT A LIFT

It would take the world champion in stair-climbing half an hour of running to get to the 163rd floor of the world's tallest building, Burj Khalifa in Dubai. As the tower's elevator runs at a maximum speed of 36 km/h, this trip normally does not even take two minutes. But speed isn't everything: **elevators are becoming intelligent, connected** – and can even leave the building.

By Rainer Claassen

Archimedes constructed the first elevator in 236 BCE, but it wasn't until the 19th century that the technology came into widespread use. Steam-powered elevators began moving heavy loads in mines and factories. Only much later were lifts installed in office buildings. Without them, cities would look very different today.

The elevator in its present form was invented in 1854, and not a lot has changed in the way it's moved since then. The system has been the same: one cabin, one shaft, and one rope, traveling up and down. Designs that included one cabin with one shaft caused ridiculous wait times, especially in busy office buildings where there was only one car moving up and down, a few people at a time.

Next came the double-decker elevator. Since the two cabins were stacked, it could move several people at once. However, the building had to be constructed or, if possible, renovated with taller ceilings to allow for the height of two cabins. Also, extra power was needed to move two cars at the same time, even if one cabin was left unoccupied.

In 2003, the twin elevator was invented to offer more efficiency, flexibility, and convenience for passengers and building owners. It allowed two cabins to move independently in one shaft, giving 30 percent more room and reducing the footprint by the same percentage.

Because of the increasing concern for efficiency and time savings, elevator tech innovation was long overdue. According to research on elevator scheduling by Columbia State University students, New York City office workers spent a cumulative 16.6 years waiting for an elevator, and 5.9 years inside elevators, in 2010.

Rapid Transport

High-rises and skyscrapers only exist due to elevators. As more and more people move to modern-day megacities, the need for rapid transport not only to, but also within, buildings is growing. Here, "smart" elevators will play an increasing and increasingly vital role. According to ThyssenKrupp, a German engineering company, mid- to high-rise buildings offer the most economical and environmentally viable solution to the numerous urban challenges. ThyssenKrupp believes taller buildings provide more working and living quarters without increasing their footprint on the ground. They even say that tall buildings allow planners to have smart grids by enabling centralized, intelligent energy control.

However, one of the main challenges with building up is elevator mechanics. Since conventional elevators aren't really created for buildings this tall, more shafts are needed to support them.

Upwardly Mobile

Analysts at Global Market Insights Inc., a management consulting company based in Selbyville, Delaware, valued the global elevator market at $82.29 billion in 2020, and they expect it to grow at an annual rate of 2.5 percent from 2021 to 2027. The five biggest players in this market are Kone Elevator from Finland, Mitsubishi Electric Corporation from Japan, Swiss Schindler Group, US-based Otis Elevator Company, and Japanese Fujitec Company Limited – the latter reported an annual revenue of 13.38 billion yen ($122 million) in 2020. All of these companies operate globally.

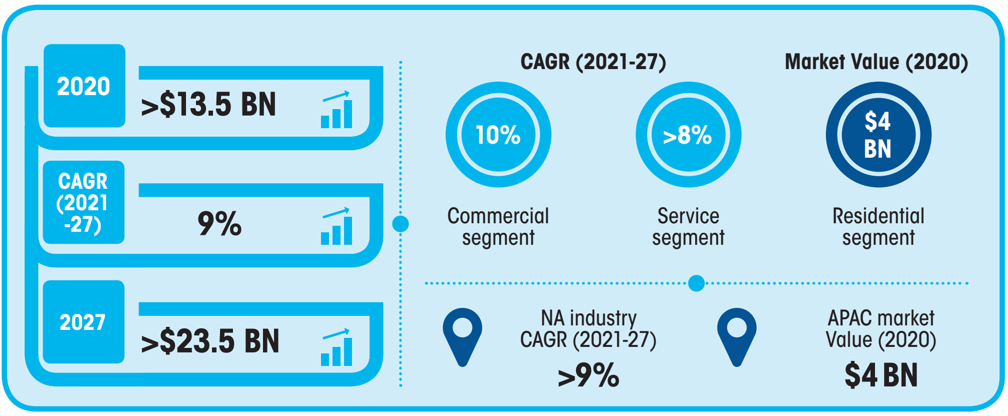
Add to these a raft of regional and niche players who play important roles in their own home markets, such as Hillenkötter + Ronsieck in Germany (brand name: Hiro) or Weigl in Austria. China constructed the world's biggest elevator, a 120 m long vertical shiplift constructed as part of the Three Gorges Dam on the Yangtze River in China, with the help of German engineering companies.

Elevators are an essential part of the building, so it is crucial that they operate at all times. Even though regular checkups are required, downtimes are often longer than necessary: it may take some time until a malfunction is even noticed, and it can take even longer for the information to arrive at the maintenance company. And by the time a technician finally turns up, he may have to wait for necessary parts – or return with the right tools to do the job.

One of the companies that addresses these issues on a global scale is Bosch Service Solutions. In an interview, their Senior Product Manager Michael Baer explained how the company retrofits old- ➔

Uplifting Numbers

The world market for smart elevators will continue to grow by leaps and bounds, but only a handful of manufacturers are true global players.



source ©: Global Market Insights Inc

IoT Takes Elevators to the MAX

source ©: TKelevator

Making the Right Connections

One of the pioneers in elevator digitalization is TK Elevators. They announced their IoT platform MAX in 2015. Since then, they have connected more than 200,000 elevators worldwide to it.

The system was developed in cooperation with Microsoft. The dedicated wireless network is provided by Vodafone. There are three data centers in the USA, Europe, and East Asia. Collected data from all installations is analyzed in real time – whenever a connected elevator is not functioning, a service ticket is generated immediately. Included data gives clear hints to the technicians on where the problem is most probably located. In many cases, technicians will already carry the necessary spare parts with them when they drive to the affected building. The fast service reduces downtime. Necessary maintenance can also be done at times when it does not interfere with the functioning of the building. The results are massive reductions in downtime, better service, and – most importantly – increased peace of mind for operators.

Interview

Bosch Service Solutions has developed a solution they call Bosch Elevator Monitoring. It allows adding communication skills to existing elevators. *Smart Industry* talked with **Michael Baer, Senior Product Manager at Bosch Service Solutions.**

Bosch has developed a system that gives older elevators access to digital technology – why don't you concentrate on new installations?
Many existing elevators – especially in office buildings – are over 20 years old. It is costly to replace them – but when an elevator stops running the costs continue. Ideally, they should never stop running. That's why we decided to develop an intelligent system to help reduce downtime for older installations that can easily be installed in any existing building.

source ©: Xing

> An elevator should never stop.

Michael Baer
Senior Product Manager at Bosch Service Solutions

How long does it take to install the hardware?
We wanted to have a system that can be installed on any elevator in less than 30 minutes. The sensor box we developed together with our partner SafeLine makes this possible. It is attached to the roof of a cabin with another sensor attached to the door. Then the car has to do one stop at each floor – and the installation is complete.

Can elevator data be collected independently from the manufacturer?
Absolutely – intelligent algorithms allow the box to detect relevant data from all types of elevators. After a first data analysis within the box, important data is transferred to cloud servers via a 4G connection. The antenna was specially designed to connect in surroundings with low network coverage to ensure reliable data transfer.

How is the data analyzed – and how can building operators make use of it?
If an elevator stops working, our system will detect this immediately. But the sensors also notice smaller disturbances. Technicians may then take a closer look at the installation and do necessary maintenance before the elevator stops working. Traditionally elevators were checked after fixed intervals. Elevator Monitoring allows these intervals to be adjusted to the actual wear and tear. In many cases, technicians will not only know where to look for the error in advance but also which spare parts to bring. This reduces downtime and saves the building operator a lot of money.

er elevators with IoT technology (see interview).
An elevator never stands alone – it is always integrated into a building. And digital integration has become crucial to modern elevator construction, as sensors and smart interfaces become part of the ecosystem of smart buildings.
Retrofitting existing elevators with intelligent systems that can connect to the building's infrastructure is traditionally the job of small specialist companies, among them firms like Datahoist, InsideM2m, or Robustel. But these systems are increasingly being displaced by corporate giants interested in getting a toehold in what looks increasingly like a highly lucrative market for the future. By 2025, the developing world, as we understand it now, will be home to 29 megacities with populations of 10 million or more, the *Guardian* newspaper writes.

> Elevators will soon know where you're going without having to press a button.

Hyun-Shin Cho
Head of Digital Transformation at TK Elevators

source ©: thyssenkrupp AG

A Lift That Thinks Ahead

Hyun-Shin Cho, Head of Digital Transformation at TK Elevators, explains: "Our latest systems allow full integration into smart buildings. This also includes the access management. When you enter a building with an appointment, the system will already know where you are heading for. Through a smartphone or a wearable, you will be informed which lift to take – and will be brought to the floor where your appointment is scheduled without even pushing a button. This can make a huge difference – not only in times of a pandemic."
While integrated sensors can help to find the location of defects even in complex systems with many components, it is still rather complicated to actually predict when a certain component will stop working – since almost every elevator is an individual construction, it will take

some time in acquiring and analyzing data from many systems until this will be possible on a large scale. Companies are currently working with their best and most experienced service technicians to set up digital twins of different configurations – and to analyze the data collected from elevators. As more and more of it accumulates, the opportunities for precise analytics grow.

Standardized data interfaces utilized by all manufacturers could accelerate this progress. But we are not likely to see them soon: as companies usually make more money from maintenance than from building elevators, they have little interest in making their data available to competitors easily.

Giving the Future a Lift Up

Hyun-Shin Cho expects the importance of user experience to grow in the near future. While low power consumption has been one of the main interests of clients in the past years, they now are mostly interested in digitalization and integration – and a positive user experience.

Another project from TK Elevators may add to this: they are planning to bring the first ropeless elevator to the market soon. The company sees many advantages in this system. As the cabins are moved by electromagnetic forces, several cars can move in the same shaft independently. And they are able to move horizontally as well as vertically. The system saves a lot of space too – shafts can be up to 50 percent smaller. And it also has the potential to change the possibilities of architecture: two buildings on opposite sides of a road can be connected by elevators running horizontally between them.

The system may also be used for transport outside of buildings – and in so doing make big changes in the way we move around in the future.

Intelligent elevators already help make the world more comfortable in hotels: Savioke Relay is a robot that autonomously delivers items to guest rooms. To be able to do this, it must be able to ride in elevators. KONE Elevators and Savioke have connected their systems to make this possible. Elevators arrive automatically at the floor where the robot has to enter and takes it to its destination. Alexander Foster, director of rooms at EMC2 Hotel in Chicago, where the system was first deployed, said: “We find that our guests have higher expectations now more than ever, especially in this technology world where everything’s connected to social media. When they get here, the robots and their relationship with the elevators blow their mind.”

New elevator will offer significantly shorter wait times, increased capacity, a smaller footprint, and substantially reduced weight and mass. Lift systems with multiple cabins that travel up one shaft and down the other in one continuous loop similar to a circular train system on a vertical plane are already entering the market.

And the best part? Passengers don’t even notice a difference, and the doors open every 15 to 30 seconds. The future of elevators, it seems, looks very uplifting indeed.

The Tower of Rottweil

🟥 Look – No Ropes!

When you take a ride on the autobahn from Stuttgart to Lake Constance, you cannot fail to spot an astonishing building: in Rottweil, German elevator producer Thyssen-Krupp built a 246-meter (807 ft) high tower, where they test and certify new elevator technology. They hope to significantly shorten development times for future skyscrapers and developments already under construction. In the tower there are 12 shafts – it features elevators going up to 18 m/s (more than 60 km/h) and others that work without ropes. But the company also runs test towers in Cheonan (Korea) and in Zongshan (China) – a fourth one will be finished in Atlanta in 2021.

source ©: TKelevator

source ©: KONE

Going Up!
Digitization, integration, and standard data interfaces will soon make for shorter wait times and a more positive experience for people riding in elevators.

Precision Fishing

NET BENEFITS

Sea fishing is becoming less sustainable as the taste for seafood increases in pace with the world's population. It is clear that **trawler fleets will have to employ smart technologies to bring about precision fishing** so that depleted species can be left undisturbed while thriving shoals are harvested.

By Gordon Feller

source ©: DigiCatch

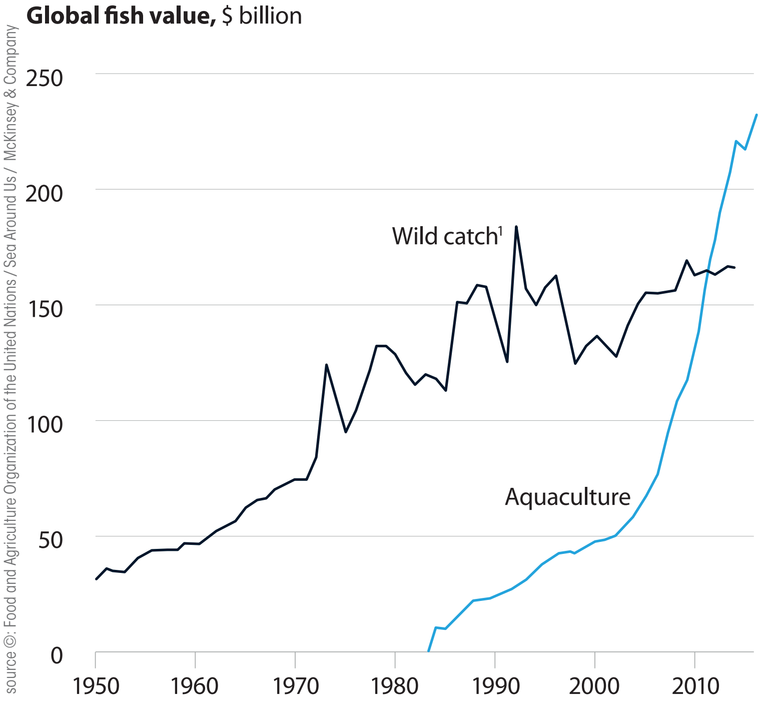
Lighting the Depths

DigiCatch's high-intensity lighting system is remotely dimmable and works at depths of up to 100 fathoms.

Seafood is the animal protein of choice for over 17 percent of the world's ever-growing population. One 21st century fact that many governments don't appear to have fully absorbed is that people are eating more fish than ever. From 1961 to 2016 there has been a 3.2 percent annual increase in demand for seafood. Driven by the rise in global population, total world fish consumption is projected to increase by another 20 percent between 2016 and 2030.

Despite this, the $500 billion (€419 billion) seafood industry has several major problems. Overfishing, climate change, pollution, habitat destruction, and the use of fish for other purposes besides human consumption all threaten the global seafood supply. The quest to harvest enough fish and the need to satisfy soaring consumer demand will continue to exert incredible pressures on marine systems. It now takes five times the effort to catch the same amount of fish as it did in 1950. The reason for this is quite simple: so many species that we depended on are now in scarce supply.

The introduction of new and advanced precision-fishing tools and technologies is beginning to help companies optimize and reduce the waste in their operations. According to several recent reports (including McKinsey & Company's 2019 report *Precision Fisheries: Navigating a Sea of Troubles with Advanced Analytics*), if large-scale fishing companies around the world would adopt these new technologies more enthusiastically, they could decrease their ➔



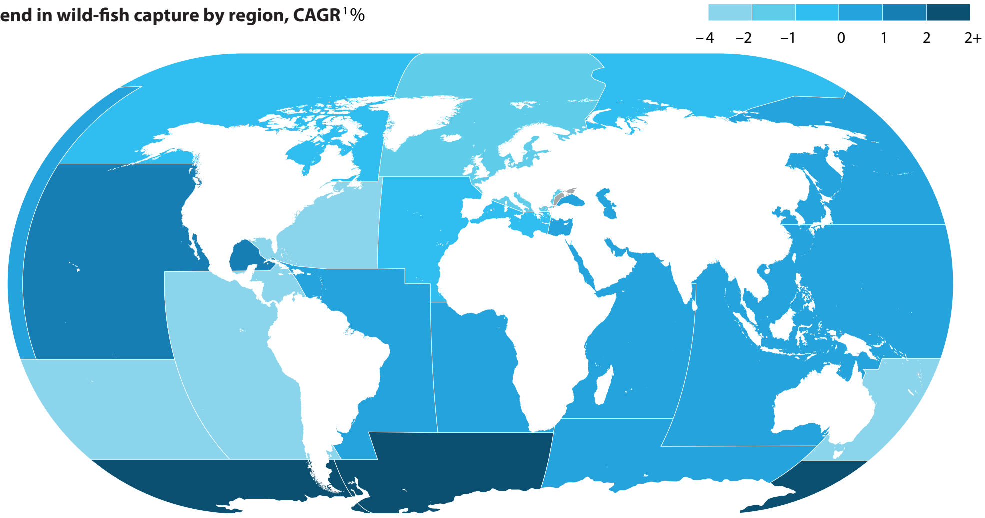
source ©: Food and Agriculture Organization of the United Nations / Sea Around Us / McKinsey & Company

Diminishing Returns

The quest for fish is a billion-dollar business. But as demand grows, so do the costs as supplies of wild fish are becoming increasingly scarce.

[1] Excludes aquatic mammals; alligators, caiman, and crocodiles; seaweeds; and other aquatic plants

Trend in wild-fish capture by region, CAGR[1] %



source ©: Sea Around Us, 2014 / McKinsey & Company

annual operating costs by around $11 billion (€9 billion).

Precision-fishing technologies will not only help improve commercial fishing, it will also improve the ability for managers to adaptively govern various fisheries around the world more sustainably. It is projected that precision-fishing technologies could increase industry profits by as much as $53 billion (€44 billion) by 2050 (as noted by McKinsey's 2020 report *How Advanced Analytics Can Help Restore the World's Fish Supply*) while also doubling the level of total fish biomass in the ocean.

More fish are harvested by trawling than any other method of fishing. The problem with trawl fishing is waste. It is inherently a "blind" activity and on average one in every four fish caught is typically the wrong species, known as bycatch. According to some estimates, global bycatch may amount to 10 percent of the world's haul, totaling 16 billion pounds (7.3 billion kilograms) of waste per year.

Several companies are developing precision harvesting and traceability products to reduce waste, improve data availability, and improve sustainability in the seafood industry. Their tools directly address overfishing and dwindling fish stocks with clean technologies and advanced analytics.

Eyes in the Net

One such company is SmartCatch from California's Silicon Valley. It has developed DigiCatch, a turnkey system that allows trawler skippers to harvest their targeted species with greater precision. At its heart is a real-time, high-definition smart camera system that gives the fishermen "eyes in their net." The camera is in a 1.2-meter metal tube which also contains powerful lighting and sensors for temperature, salinity, and water depth. The images and data can be viewed from the ship's wheelhouse, allowing fishermen to move on when they see stocks are low or when fish are the wrong size or species.

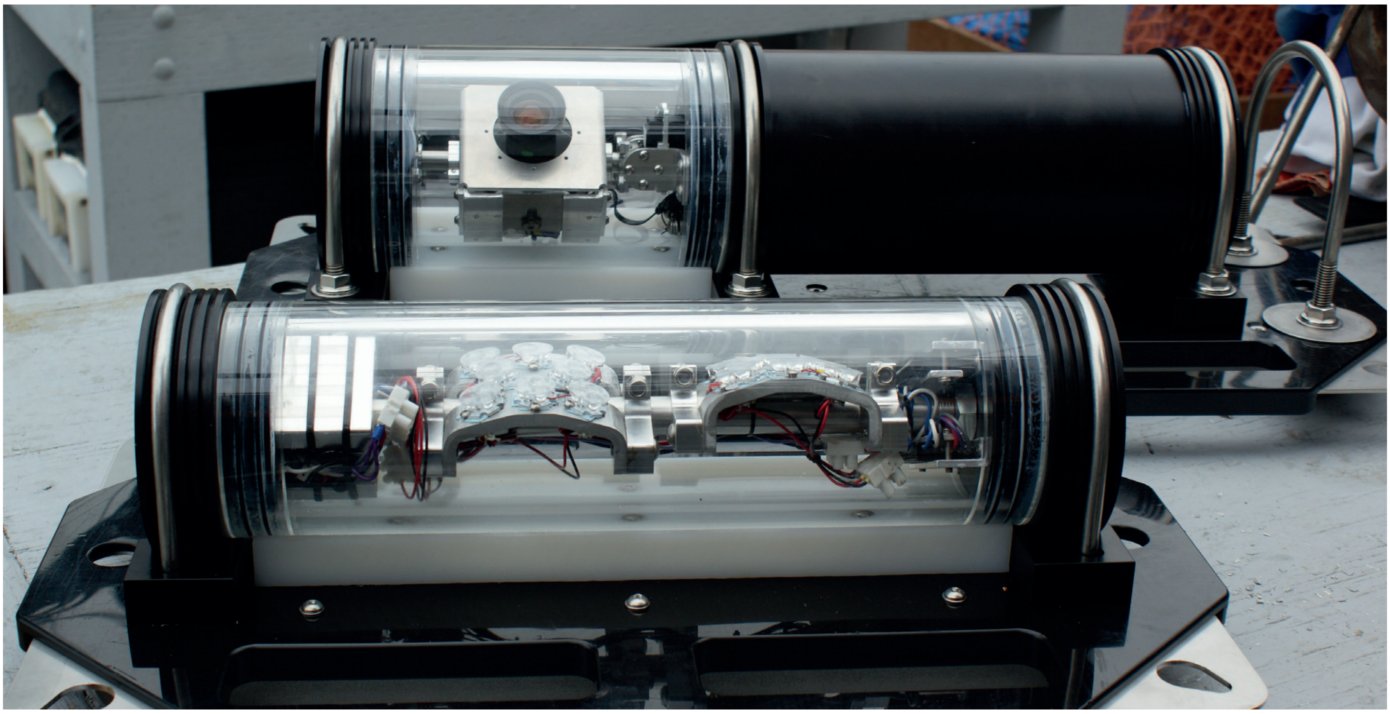
This operational transparency supports fishing optimization while avoiding unwanted species and reducing negative ecological footprints. The real-time camera works

Thanks for All the Fish

Thanks to IoT, trawler skippers can search for and harvest their targeted species.

Wheelhouse Fishing

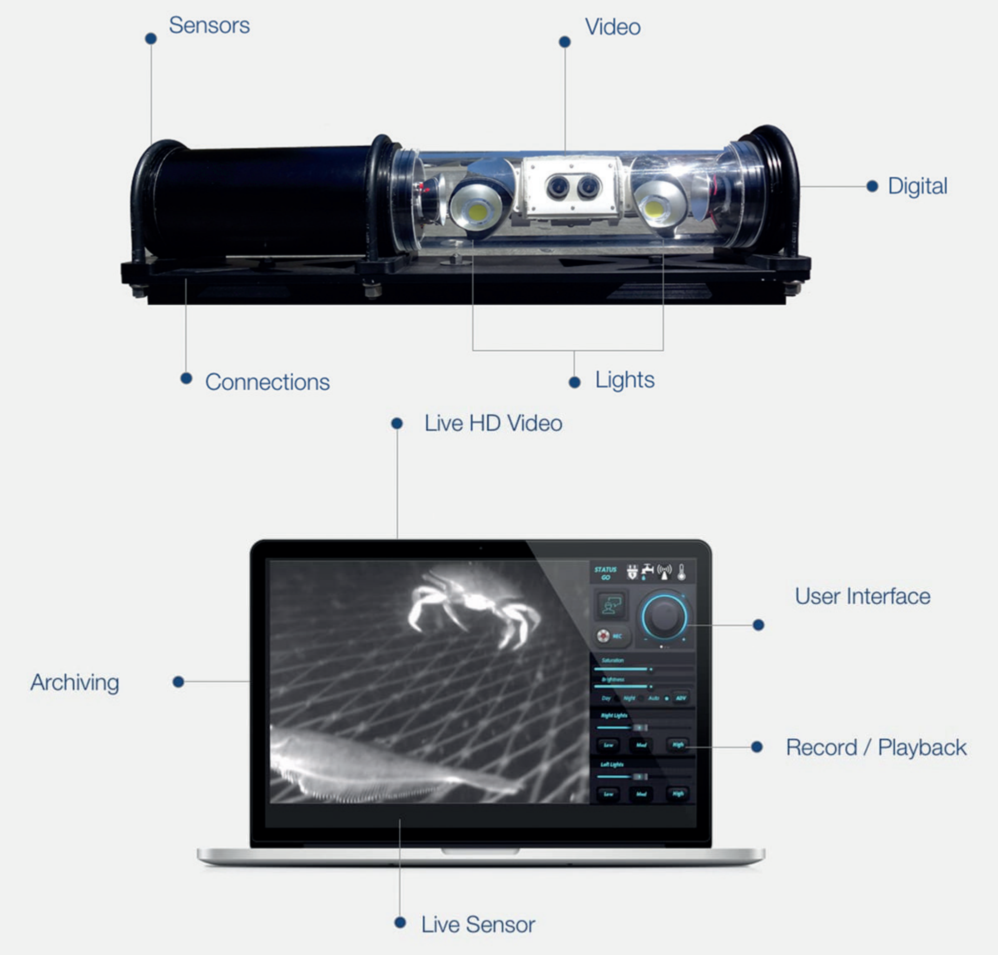
Images and data can be viewed directly without the need to leave the ship's wheelhouse.



source ©: Author

[1] Compound annual growth rate of marine capture, 1994–2014. Anchoveta, fished along the coast of Peru and Chile and one of the biggest single-species fisheries, is excluded from the analysis because of its highly variable stocks related to El Niño conditions and past collapse events due to overfishing.

on any coax sonar cable system and retrofits any type of trawl net.



source ©: Musings Magazine

Watching the Catch
SmartCatch has a real-time camera that can sort out unwanted species of fish and help protect the environment at the same time.

Since regulations alone cannot eliminate overfishing, fisheries need more progressive solutions to stay on a sustainable trajectory while minimizing their environmental impact. The integration and growth of advanced analytics in seafood harvesting is on track to solve many of the supply chain waste challenges. “If the governing agencies and fishing related companies get it right, linking the physical and digital worlds could generate up to $11.1 trillion a year in economic value by 2025,” according to McKinsey.

SmartCatch’s DigiServices features and IoT devices are designed to facilitate the real-time collection, organization, analysis, and storage of seafood data. The connected products and digital services leverage big data, artificial intelligence (AI), digital video, deep analytics, and cloud computing. The company is currently developing AI integration across the systems to relieve captains from always having to view the screen, recognize and count fish, and pull the data needed to help drive efficiencies and profits.

SmartCatch’s future plans for hardware devices and software aims to facilitate the capturing and “brokering” of critical data for fishermen, catch processors, buyers, and certification agencies. This includes blockchain authentication of fishing data and provenance – ultimately, the value the company’s product roadmap promises will extend across the entire value chain.

Best Connections

Cloud technology is a chief enabler for these capabilities. Computing technology has continued to become a lot cheaper and we use cloud computing for massively available storage, massively available compute power, so you can now do things with predictive analytics and science to change the way a business works, instead of relying on traditional manual processes.

Technologies like SmartCatch’s IoT system are using cloud benefits to convert physical data into actionable insights, as well as improving biosecurity by connecting the data from the first mile – harvest and processing – to the last mile, which means the actual consumer. The more that tools like this are put out there, the more likely businesses are to achieve more favorable outcomes faster and with greater profitably.

The key to these IoT systems is that they are not just focused on generic species or type information, they also place an emphasis on what is specific to each fish. Among these areas of focus would be: where and when the fish was harvested; its attributes; quality testing information in a consumer-friendly view; benchmarking against industry standards; how and where the fish was processed; how it was handled; sustainability information; and similar relevant information.

According to Rob Terry, SmartCatch’s founder and CTO, “In the future when someone is interested in eating fish, I can easily imagine them being able to scan in a smart QR code on a store package, or even a restaurant menu, and the display appears with everything they would ever want to know about their piece of fish.”

source ©: Facebook

> Get everything you want to know about your piece of fish.
>
> **Rob Terry**
> Founder and CTO of SmartCatch

Robotic Floor Care

CLEANING UP AFTER COVID

In a pandemic, cleaning becomes more complex and cannot be put off till outside normal working hours. **Intelligent machines are helping to free up human hands** for other tasks and ensure safer environments.

By Michel Spruijt

As Europe begins to open up again, business owners and managers are adapting to a world that must effectively live alongside the stresses of Covid-19 – and new questions are being asked. How can we ensure that our employees and customers feel safe? How can we comply with standards and requirements that appear to change from week to week?

It's within this environment that cleaning has emerged as a core component of restoring confidence in everyday living. It's at the heart of rebuilding trust, and businesses must ensure a more detailed and more consistent clean to showcase their commitment to a successful reopening. With workers being asked to do more and customers worried about indoor

source ©: Brain Corp

infection, automation provides a compelling solution.

Enter commercial robotic floor care, where industrial-grade cleaning machines perform tasks in public spaces without a human operator. While automation in robotic cleaning has been gaining traction for the past five years, the pandemic has put it front and center. Companies like Ahold Delhaize and Walmart have noted their commitment to cleaning with the help of robotics, and environments beyond retail, such as airports, schools, and hospitals, are following suit.

Brain Corp, an AI company that currently powers over 14,000 cleaning robots, has seen a surge of interest over the past 12 months. Its BrainOS-powered machines saw usage increase by 24 percent in April 2020, compared to the same month the previous year, and a 15 percent increase in the year overall. What's more, a significant percentage of this uptick occurred during daytime hours, showing that businesses are cleaning more frequently and operating the technology during peak times.

source ©: Brain Corp

> We've seen a surge of interest over the past 12 months.
>
> **Michel Spruijt**
> General Manager at Brain Corp, Europe

Robotic floor care provides businesses with a number of key benefits, all of which are even more important with the realities of a pandemic:

- "Clean" has become a new brand value. Companies can effectively show their commitment to a more frequent, consistent cleaning program with robotics.
- The machines are an effective tool in helping cleaning staff get the job done. With increased levels of expectation around surface cleaning and sanitization, cleaning robots can complete dull, repetitive tasks in parallel.
- Advanced solutions can operate safely around people and adapt to changing environments, ensuring a cleaning program that's being deployed around the clock.
- Robots provide businesses with automated performance reports so managers can constantly monitor, prove, and optimize their fleet.

The deployment of these technologies is expected to continue an upward trajectory through Covid-19 and beyond. While recent events have certainly accelerated adoption, we're likely to see robotic floor care take its place beside other typical, automated solutions over the next few years. Like manufacturing arms and washing machines, cleaning robots will be viewed as effective tools that help make our lives easier, safer, and more productive.

Cleaner Is Cooler

While automation in robotic cleaning has been gaining traction for years, the pandemic has put it front and center. Companies have committed to cleaning with the help of robotics, and environments beyond retail, such as airports, schools, and hospitals, are following suit.

source ©: Brain Corp

Interview

THE KING OF KEGS

Every year at Munich Oktoberfest*, large wagons piled high with wooden beer barrels are pulled through the streets by teams of huge draft horses. But the logistics of beer has come a long way since those days. Today, beer is usually shipped in stainless steel, and hence reusable, kegs. **Adam Trippe-Smith is the CEO of Konvoy, an Australian start-up** that is in the process of bringing keg management into the Age of IoT.

By Tim Cole

You have been described as a serial "beerpreneur." Sounds like you don't just enjoy a glass or two; it's your lifeblood.

That's true. At first, I worked for a brewery, then I started a keg rental business and now, with Konvoy here in Australia and New Zealand, we are pioneering a new tracking system which uses wireless IoT beacons on the casks.

So essentially, you have reinvented the keg business.

That's the way we like to think about it. I mean, kegs have been around for many, many years, but they were really just a dumb asset. In the last ten years, all of that has changed. Individual kegs can be tracked using either a barcode or an RFID tag. Konvoy is moving even further into the IoT world by adding a whole new realm of information not only for the owner of the keg who rents it to the breweries, but also for the users of the kegs, the producers, pubs, the warehouse, and the wholesalers. In effect, we're turning the keg into a smart asset using data and analytics.

How big a factor is human error in conventional keg tracking systems?

In the past, every time a keg moved out of our warehouse to a brewery, and from there to a pub, a bar, or a restaurant, it had to be scanned manually. Obviously, that takes time, and people make mistakes or get lazy. In fact, we found that only about 70 to 75 percent of all keg movements were actually being recorded.

So, what's the solution?

Using an IoT beacon, we can track the keg's location as well as providing temperature information so we know if the beer has been kept cool enough during transport. All this is data which just simply didn't exist in the past.

*The Munich Oktoberfest was cancelled in 2020 and 2021 due to the Covid-19 pandemic.

> All this data just simply didn't exist in the past.
>
> **Adam Trippe Smith**
> CEO of Konvoy

The Konvoy system runs on the Sigfox wireless low-power network. In fact, you jokingly refer to it as "Kegfox." Wouldn't it have been simpler to use cellular?
When we launched last year, we looked at every alternative but our main problem is the data cost. Bearing in mind that prices for cellular have been dropping, you're still looking at about 25 Australian dollars [€16] per year to just track one keg. Compare that to the cost of using the Sigfox network, where you're talking about low single-digit dollars per year – a huge difference. If you think of the keg itself costing roughly a hundred dollars, then there's a limit on what you can afford to invest in a tracking device, in data costs, and in running the network. Yes, cellular can transmit more data – but we don't send much data. After all, we're not transmitting photos or anything like that; all we're doing is taking location and temperature readings. For that, Sigfox is perfect.

If you ship beer, say from Sydney to Perth, when it's returned the keg's empty and you're essentially moving air across the continent half the time. Can tracking technology help make better use of a keg?
Konvoy eliminates all that waste because the keg that we started with at the brewery in Sydney will eventually wind up for reuse at a brewery in Perth. It never travels back across the country empty. This means you can use it more often, so you can purchase fewer kegs. Thanks to all this information, keg owners can reuse them quickly.

What are your plans for the near future?
We're tackling two problems at once: the first being our keg rental business, the other the tracking side which we're happy to let others use to monitor their own keg fleets. Once we've mastered that market here in Australia, we intend to expand into multiple geographies. That's where the real opportunity for growth lies – and we're pretty excited about bringing that to the world.

Where's My Beer?
Instead of scanning manually, Konvoy uses IoT beacons to track the keg's location and temperature to make sure it has been kept cool enough during transport.

L18
L

IoT in stolen vehicle recovery

IT'S A STEAL!

With the use of motor vehicles still on the rise, **auto theft has become an increasing problem.** New technologies are needed to protect vehicles.

By Nicolas Andrieu

Every year, about 3.5 million vehicles are stolen worldwide. 700,000 across Europe. During 2020, 121,500 vehicles were stolen in France, which is an average of one vehicle every four minutes. Although the number decreased by 13% compared to 2019 due to the COVID-19 pandemic, according to the Coyote Secure's theft observatory, it is estimated that the value of stolen vehicles is around one billion Euros in France alone.

Even though the owner of the vehicle is often the most negatively affected, insurance companies are also impacted financially, while the vehicle manufacturers' reputation comes into question.

Despite the efforts made by vehicle manufacturers to improve security, motor vehicle theft remains common and, according to Interpol, the use of the Internet has contributed to a dramatic increase in the resale of illicit automotive components in recent years, making it a major concern for law enforcement, automotive manufacturers, regulatory agencies and public health organizations.

Additionally, methods used for stealing cars are becoming increasingly sophisticated and are now able to override anti-theft devices. As a consequence, the Stolen Vehicle Recovery (SVR) market is expected to grow between 5%-6% by 2023.

> IoT-based solutions can be used to prevent theft across many industries.

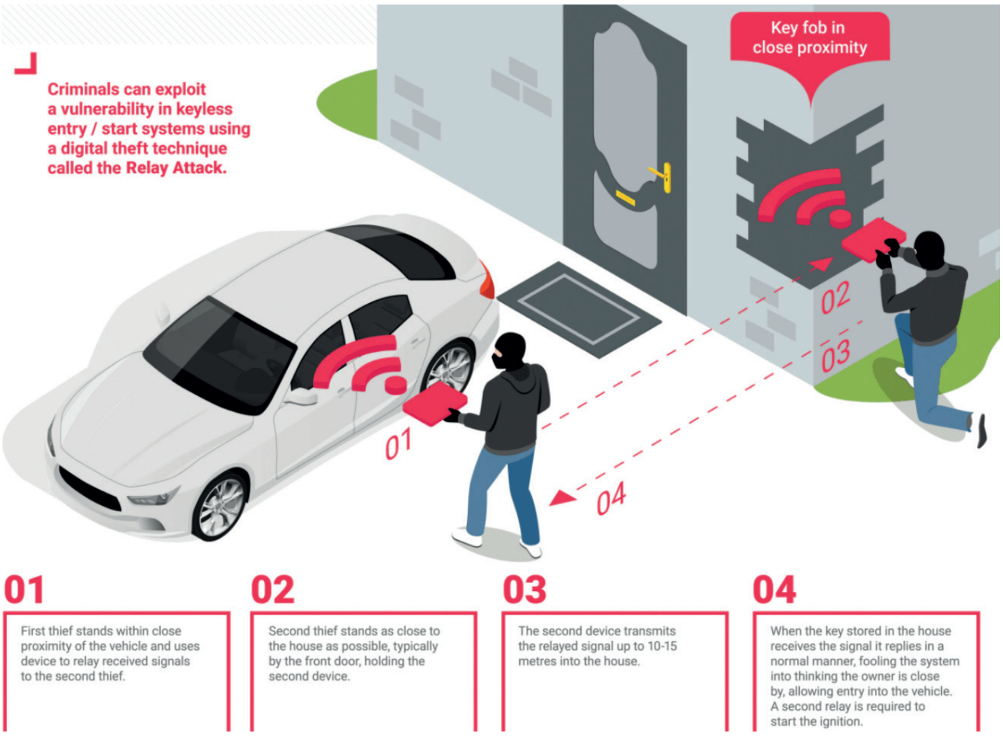
source ©: ITU

Nicolas Andrieu is Executive Vice President Europe, Middle East & Africa Sigfox

Today, 85% of thefts are carried out with the help of electronic means. Most anti-theft cellular solutions are connected to the central command of the vehicle in order to power the device, thus allowing it to have multiple uses.

Cellular Solutions are Great for Thieves

For thieves, cellular solutions are a great opportunity to find and quickly disconnect the device, ultimately decreasing the chance of retrieving the vehicle. This method, known as mouse jacking, can easily be used by anyone equipped with a portable signal jammer, an inexpensive tool which can be bought on the Internet and leaves no →



Criminals can exploit a vulnerability in keyless entry / start systems using a digital theft technique called the Relay Attack.

Key fob in close proximity

01 First thief stands within close proximity of the vehicle and uses device to relay received signals to the second thief.

02 Second thief stands as close to the house as possible, typically by the front door, holding the second device.

03 The second device transmits the relayed signal up to 10-15 metres into the house.

04 When the key stored in the house receives the signal it replies in a normal manner, fooling the system into thinking the owner is close by, allowing entry into the vehicle. A second relay is required to start the ignition.

source ©: Thatcham Research

Keyless Theft

Thieves are often harnessing sophisticated technology to hack into your car's computer, meaning they don't even need a key fob to start the vehicle and can drive it away in a matter of minutes.

trace of a break-in. This is proven by the fact that, in France, 80% of stolen vehicles were already using an anti-theft device.

When car owners notice that their cars are gone, it is often too late as only one in five are recovered, and 30% are damaged. Even if the car is found, insurers can refuse to compensate the victim if there is no trace of break-in. Last but not least, the recovery process is usually lengthy and gives thieves enough time to dismantle stolen cars or ship them to the other side of the world. In Europe, thieves generally move cars quickly from one country to another to avoid the police. Although the EU has developed a robust program to monitor the traffic and develop a common database for stolen vehicles, the probability that a stolen vehicle will be moved to another country remains high.

Cost can be a Barrier to Technology Adaptation

Although counter measures exist, they are often expensive to roll out and to maintain. In fact, the SVR market may look to security systems such as biometric technology, radio frequency identification, and ultrasonic sensors. However their cost, the potential failure of electronic components and the amount of time needed for the installation are factors that could slow the growth of the global stolen vehicle recovery market and become a barrier to technology adoption.

In this context, SVR companies are facing many challenges as well as intense competition. Therefore, those companies are seeking technical alternatives that provide the same security as a private network (jamming resistant), at a lower cost and with the same customer experience.

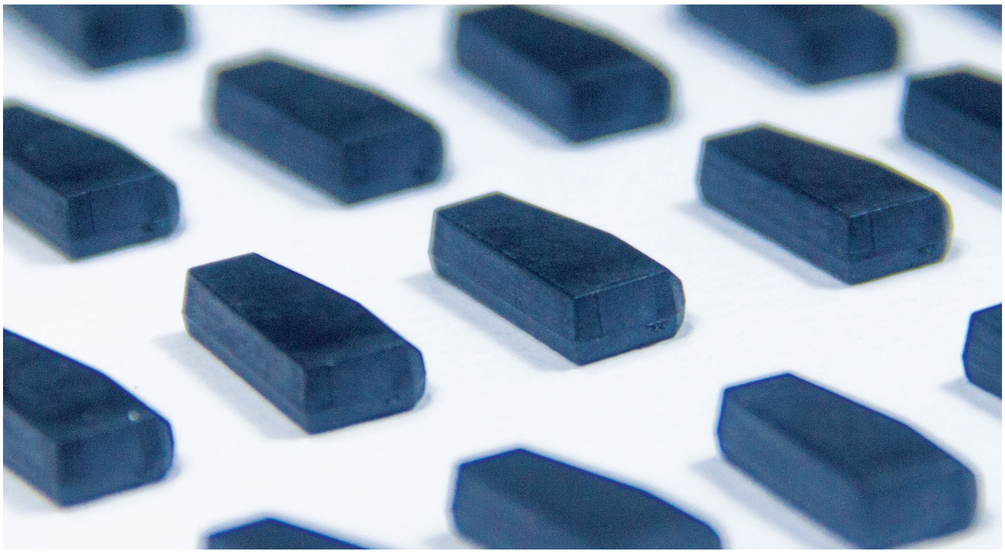
Unlike cellular or Bluetooth networks, IoT networks are able to meet three essential prerequisites to facilitate stolen vehicles recovery.

IoT devices can provide one solution which will emit signals in different regions for the same price. Since IoT devices require low electrical consumption, battery costs are also lowered, further decreasing overall hardware costs. The battery consumption of an IoT device can also be precisely calculated and monitored - this critical information reduces high maintenance costs, and the need to replace the device when it is not actually necessary.

Unlike traditional security systems, IoT devices and networks offer a new proposition to SVR companies. The devices are small

Hot Solution

Transponder-based "smart key" solutions prevent vehicles from being "hot wired" after entry. Research shows that the uniform application of immobilisers reduced the rate of car theft by 40%.



enough to be concealed inside a vehicle and quick and easy to install as there is no need to connect the device to the on-board diagnostics of the car and dismantle the panel, which would be the case with a wired solution, thus eliminating installation costs and faulty installations. Additionally, IoT based solutions offer a long-life, battery-based device, which can be placed in multiple spots within the vehicle, rendering the detection of the device by a thief complex.

Most Stolen Vehicles are Hidden Underground

Another advantage of IoT devices is that they are not attached to a specific base station or network and thus offer a wide range area of coverage. Moreover, they are capable of recovering messages from the faintest signals, while other technologies are affected by jamming, strong interference (e.g. in cities like London or Paris) or the lack of network in underground locations. This is important, as 43% of stolen vehicles are hidden in enclosed and/or underground locations to avoid being found. In France, this practice has almost doubled between 2017 and 2020, proving that professional thieves have discovered that mobile phone networks and GPS will stop working once underground.

In fact, IoT solution providers have developed geolocation capabilities based on network triangulation which can provide an estimation of the stolen vehicle's location. The network provider receives regular data from the car and, as soon as a jamming attempt is detected, the device switches to recovery mode. This means that the network will estimate the vehicle's location for every message received, allowing the security company to dispatch the nearest recovery team. Consequently, even if a jammer is attempting to block the signal, Stolen Vehicle Recovery companies can monitor whether the vehicle is moving from one place to another, or in which area it is parked.

Similar IoT-based solutions can be used to prevent theft across several industries. For example, the logistics industry has witnessed a rise in global cargo theft, with goods worth about one billion Euros stolen each year. In this context, solutions to safeguard cargo transportation assets are becoming necessary, and asset-tracking solutions based on IoT are offering a new way to secure goods for a reasonable price.

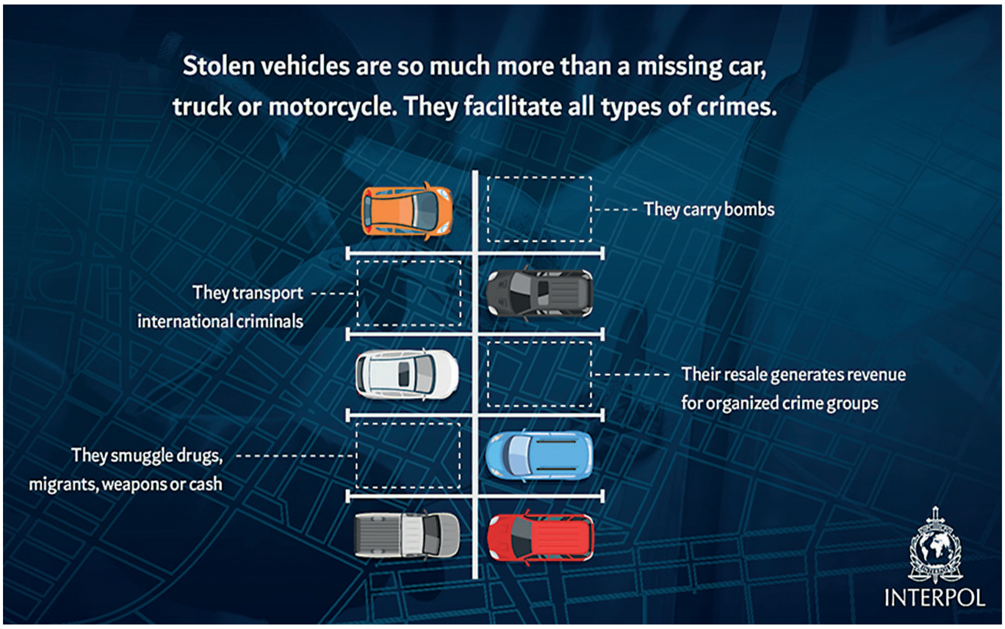
As the demand for SVR and asset-tracking solutions grows rapidly, stakeholders need to find reliable, easy to install and cost-effective solutions to meet the needs of their customers. Although many options are available, IoT based solutions are currently the most suited to meet all prerequisites and best support victims, authorities and insurance firms when a car or cargo is stolen.

Quick Escape

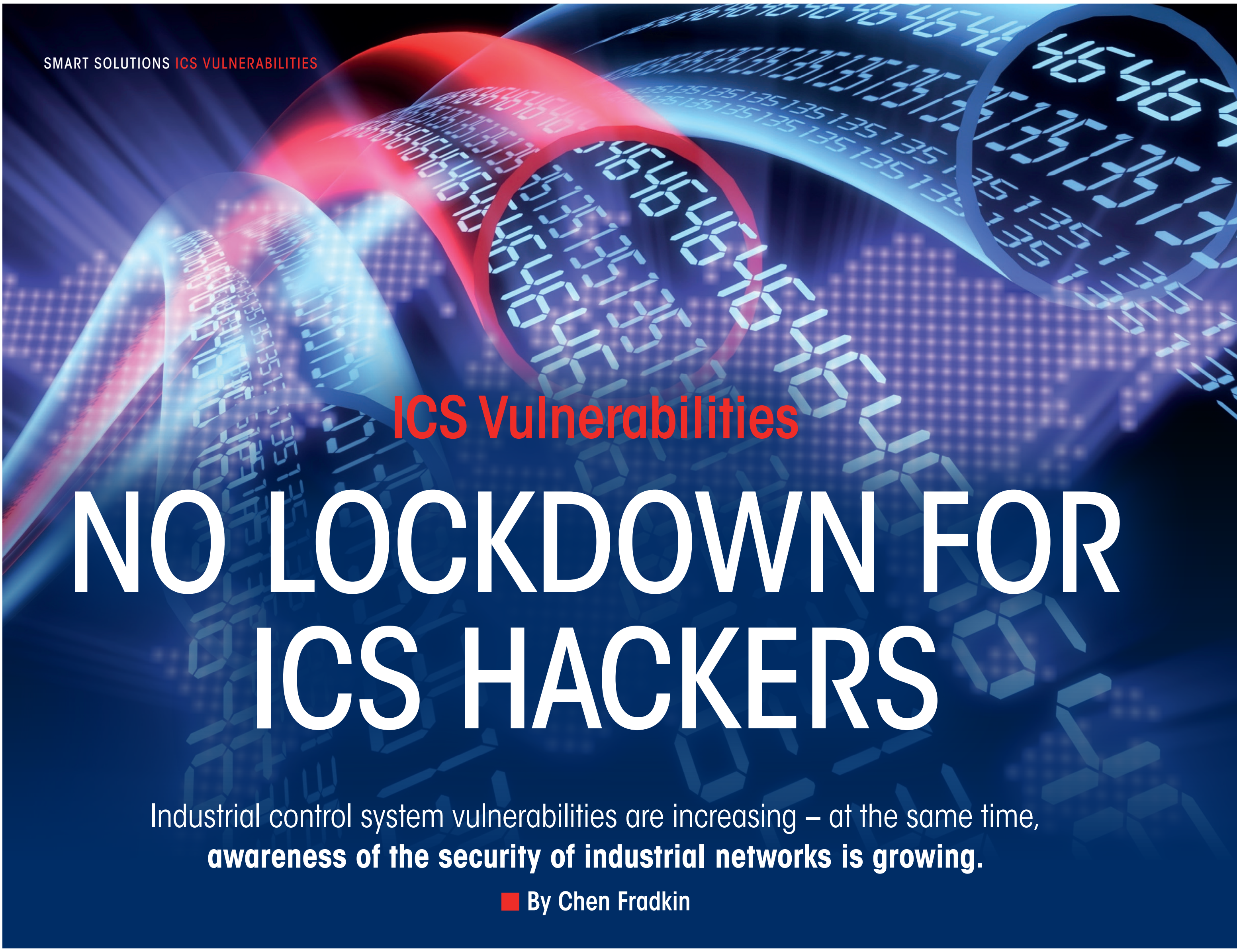
In Europe, thieves generally move cars quickly from one country to another to avoid the police.

Unintended Consequences

Stealing cars is often just the first step towards a wide range of criminal activities.


Stolen vehicles are so much more than a missing car, truck or motorcycle. They facilitate all types of crimes.
They carry bombs
They transport international criminals
Their resale generates revenue for organized crime groups
They smuggle drugs, migrants, weapons or cash
INTERPOL

source ©: Interpol



ICS Vulnerabilities

NO LOCKDOWN FOR ICS HACKERS

Industrial control system vulnerabilities are increasing – at the same time, **awareness of the security of industrial networks is growing.**

■ By Chen Fradkin

Few of us will have fond memories of 2020, a transformative year that forced businesses worldwide to rethink and reprioritize remote workforces, their impact on productivity and business continuity, and the expanded attack surfaces ensuing from those changes.

Opportunistic attackers went especially low throughout 2020, elevating extortion and ransomware attacks within their arsenals and targeting critical infrastructure and services, such as manufacturing, health care, electric and water utilities, and food and beverage. This dynamic created a race between attackers, researchers, and defenders to find exploitable vulnerabilities, especially in industrial control systems (ICS), supervisory control and data acquisition (SCADA) systems, and operational technology (OT) protocols and networks.

These systems and communications protocols oversee industrial processes in dozens of industries, and any weak spot could be a beacon to threat actors keen on accessing the internals of an industrial enterprise and either disrupting or modifying processes central to the business.

Cybersecurity specialist Claroty has attempted to define the vulnerability landscape around industrial cybersecurity and presents a comprehensive look at ICS vulnerabilities disclosed publicly during the second half of 2020. Here are its most important findings.

ICS Security Research and Disclosure Trends

- During the second half of 2020, 449 vulnerabilities were disclosed affecting ICS products from 59 vendors. More than 70 percent of those flaws were assigned high or critical Common Vulnerability Scoring System (CVSS) ratings, down from more than 75 percent in the first half of 2020. CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities.
- The number of ICS vulnerabilities disclosed in 2020 increased by 32.89 percent compared to 2018 and 24.72 percent compared to 2019. The likely primary factors for the increase are heightened awareness of the risks posed by ICS vulnerabilities, and increased focus from researchers and vendors on identifying and remediating such vulnerabilities as effectively and efficiently as possible.
- Disclosures in the second half of 2020 showed that vulnerabilities in ICS products are most prevalent in the critical manufacturing, energy, water and wastewater, and commercial facilities sectors – all of which are designated as critical infrastructure sectors.
- Third-party companies were responsible for discovering 60.8 percent of the vulnerabilities, making them the most dominant research group in ICS security.

Among all third-parties, 22 were reporting their first disclosures, further evidence of growth in the ICS vulnerability research market.

Threats and Risks from ICS Vulnerabilities

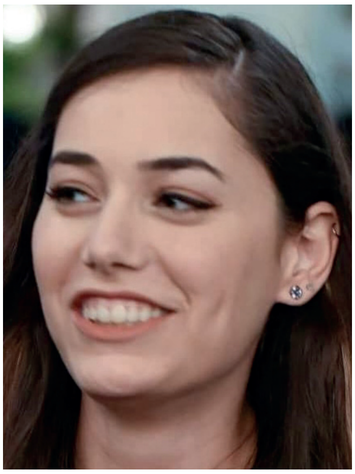
- Vulnerabilities exploited through a network attack vector (that is, remotely exploitable) stood at 71.49 percent.
- Based on the Purdue model, both the basic control level, which includes all the controlling equipment (devices that open valves, move actuators, start motors, and so on), and supervisory control level, encompassing human/ machine interfaces and supervisory control systems (line control programmable logic controllers, engineering workstations) were affected by 46.32 percent of the vulnerabilities found. The Perdue model is a reference model that shows the interconnections and interdependencies of all the main components of a typical ICS.
- Multiple types of products operating at various OT Purdue model levels, IoT and network devices accounted for 14.7 percent of vulnerabilities found. This category mostly contains vulnerabilities in third-party components.
- A worrying 89.98 percent of vulnerabilities don't require special conditions to exploit and an attacker can expect repeatable success every time.
- In 76.39 percent of the vulnerabilities, the attacker is unauthenticated prior to attack and doesn't require any access or privileges to the target's settings or files.
- If exploited successfully, 65.7 percent of the vulnerabilities can cause total loss of availability.

It's important to remember that industrial control systems and other field devices have extensive shelf lives. Unlike IT software, applications and hardware appliances that have regular update and buying-turnover cycles, ICS gear, and operational technology are designed to last considerably longer. Much of this equipment runs critical infrastructure and manufacturing processes in industries that are pivotal to the global economy. Taking down an industrial control system or specific process-oriented device for a firmware or software update is no simple feat in industries where uptime, reliability, and safety are paramount.

Digital Transformation and Convergence

Some of the increased focus on ICS vulnerabilities from security companies and independent researchers – not to mention threat actors – mirrors the convergence of IT and OT networks. These synergies will enhance the efficiency of industrial processes and save money across the board – but they can also increase the attack surface available to adversaries. Some attacks that originate on IT networks via well-known vectors (such as phishing, malware, or exploits of known flaws) may cross over to industrial networks. Engineering workstations, for example, traverse both networks and can be a linchpin that allows denial-of-service or ransomware attacks to affect both IT systems and ICS devices, thus impacting industrial processes.

The second half of 2020 saw a significant number of remotely exploitable vulnerabilities reported to vendors and disclosed by organizations such as ICS-CERT, CERT@VDE, and Mitre. It is important for defenders to focus on comprehensive remote access solutions that are ICS and OT-specific and understand the communication protocols at play there. Network segmentation and network-based detection are fundamental to defense-in-depth and are also mandates to protect converged IT/OT networks.



source ©: Facebook

> Weak spots are beacons to threat actors keen on disrupting central processes.
>
> **Chan Fradkin**
>
> Senior security research analyst at Claroty

Maturation of ICS Security Research

The steady growth of reported ICS vulnerabilities is noteworthy in terms of maturation but, currently, it's also largely limited to three vendors: Schneider, Mitsubishi, and Siemens. A large majority of the products with disclosed and patched vulnerabilities in the second half of 2020 belong to those three leading vendors; the other vendors combined had fewer products affected by vulnerabilities. However, that doesn't mean these vendors have cleaner, more secure products, it's more of an issue of accessibility to equipment for a growing number of researchers.

Adversaries and Exploits

Threats continue to surface from nation-state actors (cyberattacks against the Israel Water Authority and the SolarWinds supply-chain attack) and cybercriminals (the inclusion of ICS processes in the Snake ransomware kill list). Breaching the corporate perimeter is the first hop on the Purdue model, and while network defenses may be enhanced, incidents such as the SolarWinds attack demonstrate the fragility of some perimeter-based defenses and the eventuality that these attacks will land on ICS and supervisory control and data acquisition (SCADA) equipment.

Compounding the risk is the fact that attacks against ICS devices and OT networks tend to be targeted. While ICS and SCADA vulnerability research is maturing, there are still decades-old security issues yet uncovered. For now, attackers may have an edge in exploiting them, because defenders are often hamstrung by uptime requirements and an increasing need for detection capabilities against exploitable flaws that could lead to process interruption or manipulation.

DOCUMENTATION

BEWARE OF BACKDOORS!

The early '60s were a more innocent age than ours. Federico Fellini's *La Dolce Vita* gave moviegoers a glimpse into the carefree world of the jet set. Those who could afford it flew from continent to continent within just a few hours. Tickets and passports were only checked at the gates. This changed dramatically on July 23, 1968. Three Palestinians, demanding freedom for their jailed compatriots, hijacked an Israeli plane on its way from Rome to Athens. Almost immediately, airports began to change and security checks became part of flying.

At that time, the US was at the forefront of the push for more security in the air. Security devices became better and better and today are to be found almost everywhere: in courthouses and public buildings, schools, and sports stadiums.

Where IT security's concerned, it's a completely different story. Since the Crypto Wars of the 1990s, US agencies have been chipping away at security by demanding that companies include backdoors in their software and hand over duplicate encryption keys to the authorities. When governments objected, the US National Security Agency simply exploited loopholes and kept this knowledge to itself.

For many years, mathematician and cryptographer Bruce Schneier and other security experts have tried to talk politicians out of this dangerous nonsense. Despite this, the so-called useful security hole project keeps cropping up under a different name all around the world. The latest example is the EU Parliament, which passed a resolution in November 2020 calling for measures to undermine secure end-to-end encryption with skeleton keys and state-sponsored Trojan horses – malware that performs a range of malicious actions while misleading users of its true intent. The deliberations aren't over yet but the project appears to be on track.

> ”
>
> There are no good security loopholes.
>
> **Bernd Schöne**
>
> is a veteran German Internet journalist and an expert on cybersecurity.

The Five Eyes, an intelligence alliance formed by the US, the UK, Canada, New Zealand, and Australia, is following a much more perfidious strategy. Instead of demanding that developers build backdoors into their apps, the Ghost Protocol would require the owners of messaging services to copy the encrypted message to a third party, a law enforcement agency that owns a private key.

Thankfully, a coalition of technology companies, privacy experts, and human rights groups published an open response to this, claiming "it would undermine the authentication process … introduce potential unintentional vulnerabilities, increase risks that communications systems could be abused or misused." That seems to have stopped the Ghost Protocol in its tracks, at least for now, but who knows what is really going on in the secret world of multinational snooping?

One thing is sure – it doesn't matter if you hide a duplicate key under the doormat or in a bank safe, if there is a duplicate key somewhere, someone will eventually find it and use it.

In IoT solutions the concept of predictive maintenance is an important driver. The object of this concept is to change parameters in time to protect a device in imminent danger of breaking down. The industrial saboteur wants the exact opposite – to maximize wear and suppress alerts. So obviously, anyone selling or using IoT should fight tooth and nail to ensure that data handled by these systems is encrypted from start to finish. If governments say they just want to read communications in justified cases, who can guarantee that such tools will stay in reliable hands? Nobody!

The only conclusion here is to be wary of all backdoors and duplicate keys – there are no good security loopholes.

Bipolar transistors

Diodes

Analog & Logic ICs

MOSFETs

GaN FETs

ESD protection, TVS, filtering and signal conditioning

IoT Provisioning

SECURITY FROM THE GET-GO

Security is a rising concern in the embedded market – and for good reason. As hackers become ever more capable, the industry is coming to realize that security is a process, not a feature. It needs to start the day you begin thinking about a new product or service and it ends on the last day when you decommission them.

The assumption made by many developers is that security is a feature of a product that can be implemented just like any other feature. This is an easy way to look at security because, in that way, either you have security or you don't. This is why people often have a hard time grasping the fundamentals of security, which is the process and not the product or feature. It is a gradient that starts with no security at all and ends with military-class security. You have to analyze where your needs are and how to implement them.

The process of implementing security can be split into several key steps: the requirements and specifications decisions, the design phase, testing, production, distribution, operations, and, finally, the end-of-life stages. The steps where provisioning becomes critical is clearly the distribution and production phase – and that's where Avnet has been a key player for 100 years. In fact, as we celebrate our centenary this year, it still makes sense for us to offer services around that part of the process, as well.

Supply networks need to be extremely flexible. A company may want to produce its products in Asia, Europe, or in America, both North and South, but that can result in an untrustworthy manufacturing environment. Device credentials and software can be exposed during manufacture, which can lead to counterfeit products and reliability issues, Trojan horses in the infrastructure, low performance, and high warranty costs.

> Threats are different but the tools to solve them are the same.
>
> **Martin Milter**
> Head of Cybersecurity EMEA for Avnet Silica

As a licensed distributor of Microchip's Trust Platform, a family of pre-provisioned, preconfigured, or fully customizable secure elements, Avnet Silica aims at closing that gap by delivering pre-provisioned parts to the market. Our partner NXP Semiconductors has a similar solution where some security credentials are already provisioned before it is even distributed to the OEM. We also have a strategic partnership with Trusted Objects, a software company specializing in IoT security, to enable us to offer a scalable end-to-end security solution for low-power devices. This relationship allows customers to comprehensively secure their IoT devices while speeding time to market, reducing costs, and managing complexity.

Whenever necessary, we can do the provisioning in a closely tailored way, so it fits a customer's needs exactly. Avnet Silica operates its own process-secure programming facility near Munich, Germany, which has access restrictions on different levels and a different sensitivity level. We provision the parts of each system and ship them directly to the manufacturer, effectively mitigating most of the risk. All the proprietary information that needs to be programmed into the product is already there from the get-go.

One key challenge is that there's very little standardization today. Threat analysis and mitigations may differ from system to system but the tools to solve them are the same. That is why Avnet Silica offers a toolbox where customers can pick and choose the tools they need to get to the right security level. We are constantly expanding that toolbox to offer more complete security by covering an ever-wider part of the security process.

GET YOUR FREE COPY OF THE NEXT SMART INDUSTRY

Free copy here: smart-industry.net/subscription

Smart Sensors

HOT STUFF

Fire watches, or vigils, have existed since Ancient Rome. Today, instead of people, the latest generation of sensors do all the work much more reliably – and a lot cheaper. The **fire detectors work together in a network** and sound the alarm via the cloud.

By Bernd Schöne

Healthy sales volumes and highly integrated chips mean it has never been so cheap and easy to buy reliable protection against fire damage. For as little as €42, you can get an Internet-enabled IoT device with minimal energy consumption that will last ten years without maintenance.

> Smoke and fire detectors are becoming smarter than ever.

Smoke Detectors

Smart-home smoke detectors can do even more than sniff the air. In the event of a fire, all the detectors in the house will sound the alarm and absent residents will be notified by SMS or email. These systems can also light escape routes or raise blinds and shutters to facilitate rapid evacuation. Some manufacturers even populate and integrate their detector hubs with their intrusion detection systems. Monitoring is done via an app or web interface and calls for help from the emergency services can be made from anywhere at the push of a button. A fire causes minute specks of soot to be released into the air and a modern fire detector contains a scattered-light sensing chamber to monitor for these particles. In this air trap, a light-emitting diode (LED) shines light of a single color through the air in the sensor and a photodiode registers any light scatter caused by soot particles. More expensive systems use two colors, which enables the size of the soot particles to be determined. The detectors may also test for other fire indicators by measuring the ambient temperature, as well as checking

the concentration of carbon monoxide in the air.

Aspirating smoke detectors (ASDs) use suction systems to draw air through pipes into the sensor. Application areas include listed buildings and museums or dusty environments such as animal enclosures. Intake filters remove larger dust particles which would clog the detection chamber. ASDs often use laser diodes as the light source in the scattered-light chamber to detect even the slightest particle scattering.

➔

Bosch Smart Home System

Watching Out for Intruders as Well as Fire

source ©: Wagner eCommerce Group GmbH

The Bosch Smart Home system is a multisensor infrastructure which integrates fire detection, home security, and heating controls.

The Bosch Smoke Detector not only guards against fires and gas leaks but also has a motion detector which can be linked to other intrusion detectors (door or window contacts and surveillance cameras) to offer complete security.

The Smart Home system uses the Zigbee wireless protocol to communicate between the numerous detectors. A Bosch Smart Home Controller gateway connects the Zigbee network to the Internet via a router, which allows alerts to be sent directly to a smartphone.

Honeywell Faast XM System

Sucking Up Smoke

source ©: Honeywell International Inc.

Suction systems are the specialist units among smoke detectors. They draw in the air via a pipe system (aspiration tubes) which can be up to 320 meters long, making them ideal for use in listed buildings or rooms with suspended ceilings. In addition, larger particles in the airflow are filtered out, making suction systems suitable for use in dusty environments, such as production environments or animal enclosures.

The detection chambers usually use expensive IR laser diodes (as used in DVD players) as their light source instead of the usual LEDs. This increases sensitivity and “noise” immunity enormously. The picture shows the Honeywell Faast XM system which has two scattered-light detection chambers supporting up to four aspiration tubes. Each unit can be connected directly to a local bus network and onwards to the Internet via Ethernet and TCP/IP.

source ©: Honeywell Fire Safety

Honeywell Smart4 IRX-751CTEM-W

No More False Alarms

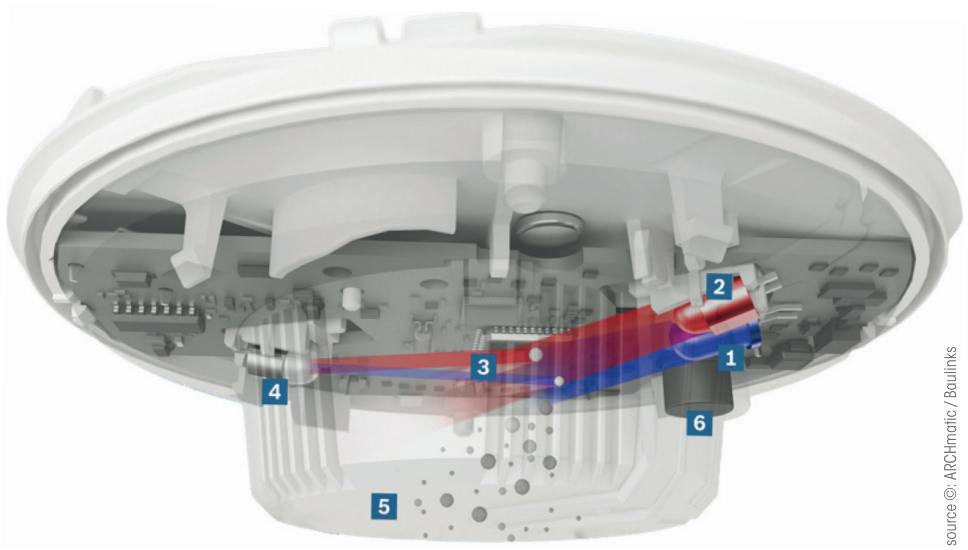
The Honeywell Smart4 IRX-751CTEM-W combines four sensor types: carbon monoxide, IR, smoke, and heat. The Smart4’s microprocessor dynamically adjusts the unit’s detection profile as it monitors the inputs from the sensors. In this way, transient “noise” can be detected and ignored to offer immunity from false alarms and improved fire detection.

Bosch 420 Series Detectors

Two Eyes Are Better Than One

Based on the idea that two eyes are better than one, the Bosch 420 Series detectors boast dual-optical chambers for extra sensitivity and flexibility. All sensor signals from the chambers are continually evaluated by the internal electronics and linked together with the aid of an integrated microprocessor.

Because the chambers are linked, the detectors can be used where light smoke, vapor, or dust due to operational conditions is present. Apart from fire and carbon monoxide detection, the 425 LSNi can identify the presence of hydrogen and nitrogen monoxide.

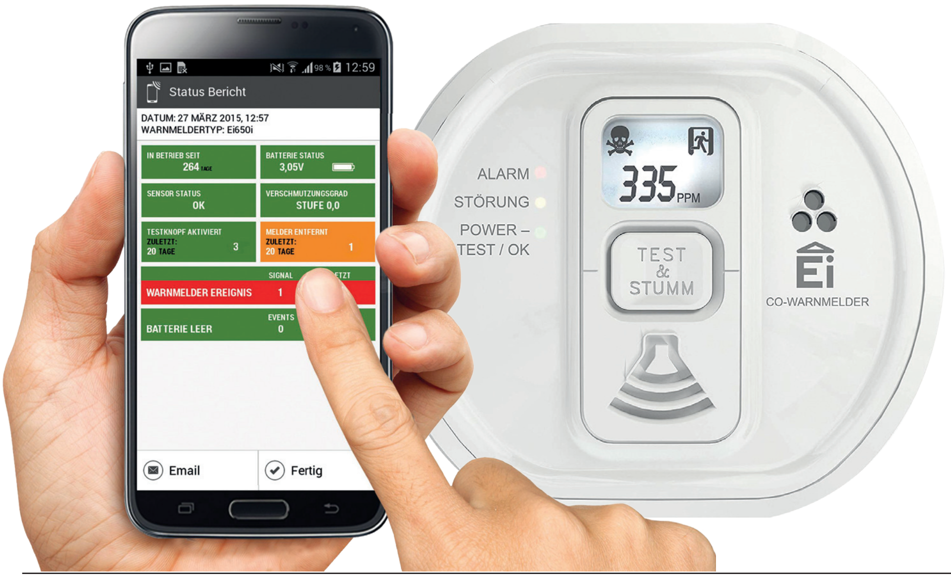


source ©: ARCHmatic / Baulinks

Ei208iDW Carbon Monoxide Sensor

Digital Canary Bird

Around a hundred years ago miners could only protect themselves from deadly mine gases, such as carbon monoxide, by using canary birds to give a warning. Today's electronic canary is the smartphone app, such as the one from Ei Electronics. The company's Ei208iDW carbon monoxide sensor connects to its Internet app not only to send alarms but also to provide information on air quality trends. The detector's long-life 3 V lithium battery lasts about ten years.



Status Bericht

DATUM: 27 MÄRZ 2015, 12:57
WARNMELDERTYP: Ei650i

IN BETRIEB SEIT 264 TAGE

BATTERIE STATUS 3,05V

SENSOR STATUS OK

VERSCHMUTZUNGSGRAD STUFE 0,0

TESTKNOPF AKTIVIERT ZULETZT: 20 TAGE 3

MELDER ENTFERNT ZULETZT: 20 TAGE 1

SIGNAL

WARNMELDER EREIGNIS 1

EVENTS

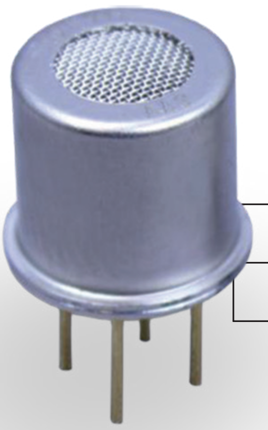
BATTERIE LEER 0

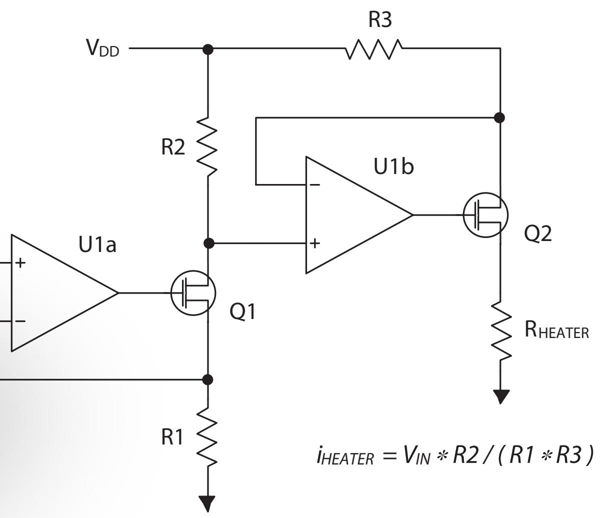
source ©: Amazon.com, unn / UNITED NEWS NETWORK GmbH

Renesas SGAS711

Gassing Up

There is an obvious need to detect the presence of flammable gases before their concentration levels approach explosive proportions. The SGAS711 by Renesas is a solid-state chemiresistor sensor designed to detect flammable gases in air. The SGAS711 sensor uses an integrated heater with highly sensitive MOx material tailored for detection of flammable gases. The device is ideal to be used as a methane gas sensor, propane gas sensor, hydrogen gas sensor, liquefied petroleum gas sensor (LPG sensor), and more.





$i_{HEATER} = V_{IN} * R2 / (R1 * R3)$

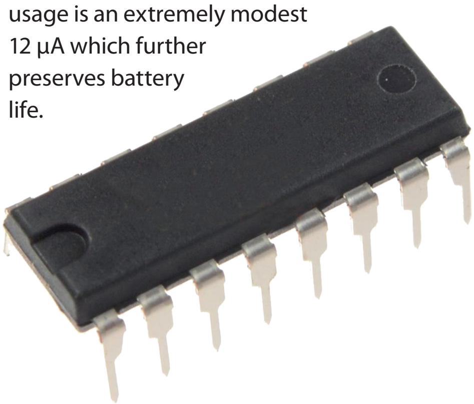
source ©: RS Components GmbH, Sensnology AB

NXP MC145010

Setting a Standard

The MC145010 microprocessor by NXP is already used in millions of homes. It has become the standard chip in low-cost smoke detectors. In a scattered-light chamber, a photodiode receives the light emitted by the internal LED. Motorola's chip evaluates any changes in the amount of light received by the photodiode to determine if smoke is present and, on detection, the chip can cause a warning light to flash and set off a piezo-electric horn.

The MC145010 can operate at voltages between 6V and12V, so it will continue to work even with weakening batteries. Its current usage is an extremely modest 12 µA which further preserves battery life.



source ©: Amazon.com

source ©: Kleinschmidt GmbH

Draeger Gas Detector

A Warning from the Cloud

An industrial gas detector from Draeger can be equipped with up to six sensors. Status queries and alarms are sent via SMS if required and more-detailed data can be sent periodically via email. A cloud service records name, type, and concentration of gases and other relevant data. Optionally, gas concentrations can be displayed in an online table or a single trend on a visualization panel that can be accessed on a local network through a web browser.

Flir-One Camera

See the Fire before It Starts

The Flir-One camera is Flir Systems' entry-level model to the world of thermal imaging. It is intended for service engineers who want to get an at-a-glance overview of overheating, defective components so they can intervene before a fire breaks out. The camera connects to an Android or iOS smartphone's USB socket, allowing photos and videos to be sent from the field. The resolution is 160 pixels by 120 pixels and the camera can record temperature differences of up to 0.1°C.

source ©: SCV SA

Flame Detectors

Flame detectors are inexpensive, low-power sensors that detect infrared radiation, especially the flickering of flames. When the sensor is triggered, a microprocessor activates an alarm. More expensive systems use additional ultraviolet detectors. These IR plus UV units are more expensive but give fewer false alarms.

At the more expensive end, thermal-imaging cameras are the newest components of fire protection. Unlike IR sensors, they are designed to detect potential fires long before they break out by helping to identify areas of sharply rising temperature. Thermal imaging is particularly useful in areas, such as hay storage shelters or waste dumps, where spontaneous combustion can occur, or to monitor the heating effect of wear and tear on machinery.

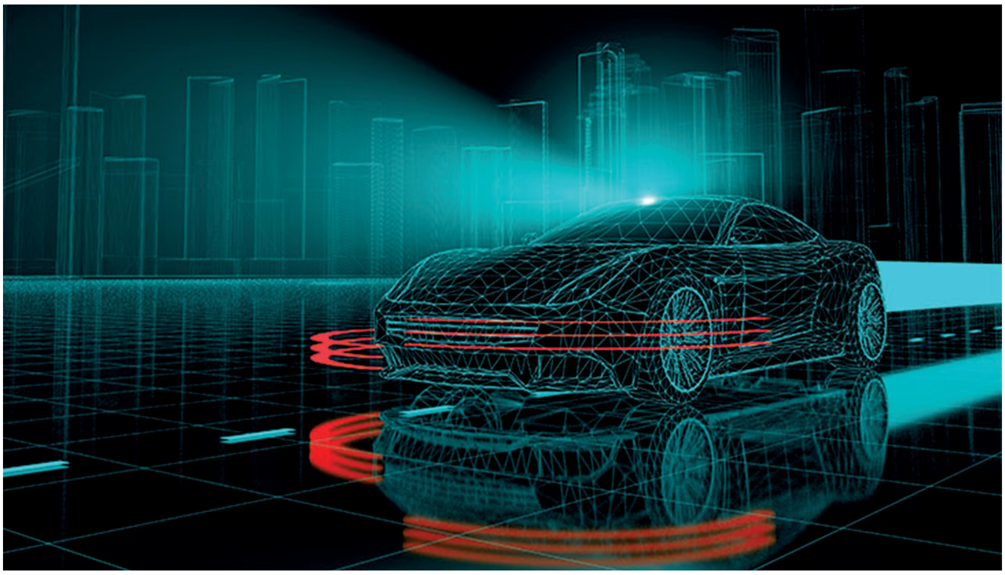
Thermal cameras may be more expensive but their advantage is that they can be used from a distance to view and protect a wider area. The resolution is much lower than visible light cameras, much less than 1 megapixel, but indicating where the problem area lies rarely requires high definition – though higher resolutions are available at extra cost.

Gas Detectors

Gas detectors are often installed alongside smoke detectors to sense natural-gas leaks, which could lead to a fire or even an explosion. They are usually designed to detect poisonous carbon monoxide, too, which could be leaking from gas cookers or central heating boilers. Carbon monoxide is colorless and odorless and can cause headaches, fainting, and, in higher concentrations, death.

Some detectors also monitor for sound changes to detect the ultrasonic noise created as pressurized gas is forced through a crack in a pipe. Early warnings would mean that remedial actions could be taken before a buildup happens.

SMART COMPANIES



source ©: Robotics and Automation News

Xilinx

Flintstones and Jetsons

A puff of smoke trails from Fred Flintstone's bare feet as he physically propels his wood and stone car down a prehistoric road. It's safe to say that we've collectively taken technology well beyond this crude (and, of course, fictional) point in automotive history.

> Self-driving vehicles will integrate onto US roadways in the coming years.
>
> US National Highway Traffic Safety Administration (NHTSA)

The drive to perfect autonomous vehicles is creating numerous opportunities for innovators and a healthy acquisition market. AMD is seeking a role in this future and its latest target is Xilinx, the inventor of field-programmable gate arrays (FPGAs). FPGAs not only offer a field-upgradable alternative to hard-wired application-specific integrated circuits (ASICs) but can also be used to speed up the development of ASICs.

Onboard field-programmable gate arrays (FPGAs), systems-on-a-chip (SoCs – integrated circuits that contain all or most components of a computer), and artificial intelligence (AI) are steering the automotive industry further toward fully autonomous vehicles. It's still a long road to the advanced automation of the cartoon flying car that collapses into George Jetson's briefcase.

This is the gray area in which today's automotive hardware engineers find themselves. According to the US National Highway Traffic Safety Administration (NHTSA), "Self-driving vehicles ultimately will integrate onto US roadways by progressing through six levels of driver assistance technology advancements in the coming years."

It's an optimistic statement but it leaves many questions: How long will this journey to fully autonomous cars and trucks take? And what path will take us there? The truth is complex but the short, encouraging answer is that we're already en route.

But the road to truly independent autonomous systems will be incremental – which is why it is critical that companies begin designing around technology with the adaptability to withstand a long, gradual period of development. Fortunately, unlike the Jetsons' briefcase car, the necessary technology already exists.

Uniquely positioned for extensive adaptability and scalability, Xilinx devices provide flexible, standards-based solutions that combine software programmability, high-performance image processing tightly coupled with analytics and any-to-any connectivity, with the security and safety needed for next-generation automotive systems.

AI capabilities require high processing power combined with low latency, and Xilinx adaptive solutions offer these characteristics with as little as three microseconds of latency. Additionally, they allow for the incorporation of advanced neural networks to facilitate sophisticated machine-learning capabilities. That's why high-compute-powered, low-latency, power-efficient, and eminently flexible Xilinx FPGAs and SoCs are already in over 100 vehicle models across nearly 30 manufacturers.

Along with the versatility of Xilinx automotive solutions comes increased complexity in implementation. Fortunately, the XiLink software development kit has been developed to seamlessly integrate Xilinx into new automotive designs. Avnet incorporates these tools to leverage Xilinx solutions to help speed products to the market.

Asystom

Creating the Circular Economy

source ©: Asystom

Predictive maintenance involves using external multisensor devices to measure a machine's state of health by detecting anomalies and drifts from its normal operating footprint. These devices need to be located on the equipment to be monitored, without additional wiring or other modifications, by integrating connected, energy-efficient electronics in a non-intrusive and compact manner.

Asystom, a specialist in predictive maintenance for Industry 4.0, has introduced a turnkey, standalone system for monitoring equipment and preventing breakdowns. It is targeted at industrial sites in mining, steelworks, automotive, aeronautics, pharmaceutical laboratories, water and waste treatment, food, and energy.

The technology takes a detailed operating footprint of a machine and then monitors it in real time to give the earliest possible alert of any performance drift or malfunction. The objective being to improve the productivity and thus the profitability of production units by avoiding unscheduled shutdowns.

Using Asystom's algorithmic developments, the devices process large amounts of complex data and transfer them for processing in real time. The devices integrate multiple physical parameter sensors (up to nine parameters) to predict industrial equipment failures and to determine the causes. The measured information is encrypted and transferred safely to server-based storage via a wireless LoRa (Long Range) network to avoid any additional installation burden.

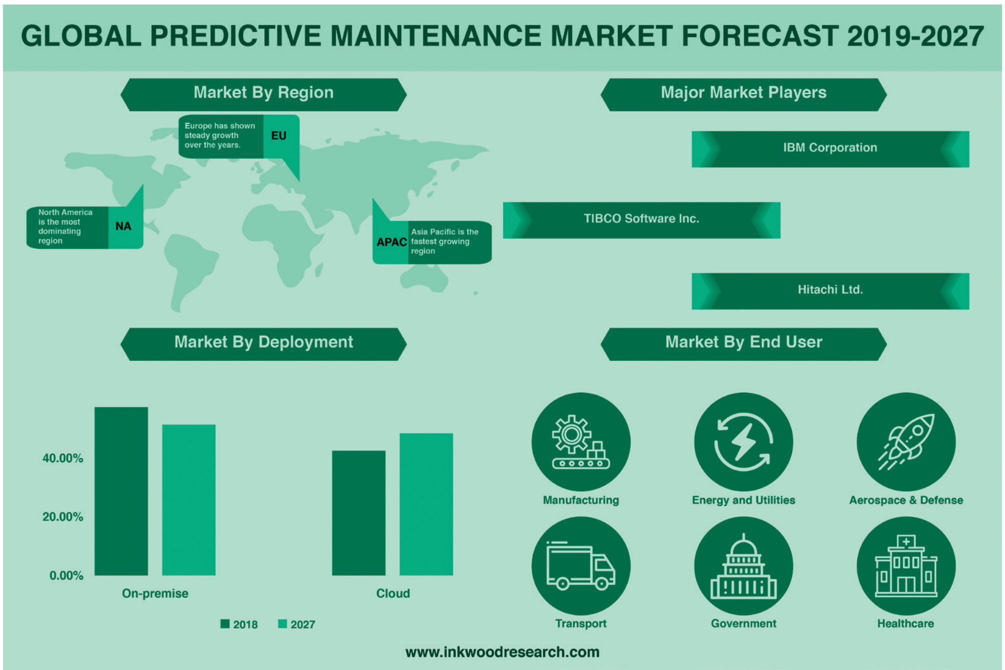
Pierre Naccache
CEO of Asystom

Operating alerts, diagnostic tools, and device setup all run on a single web-based application.

Stephane Lhuisset, CTO of Asystom, says, "We are increasingly seeing the emergence of the principles of a circular and responsible economy. Industry has come to realize that it's better to optimize the use of equipment, which must be durable while remaining efficient. Industry digitalization and preventive maintenance are effective means to achieve this, as well as improving production capacity."

Asystom's analytic devices are also aligned with this concept. Customers don't need to frequently change the batteries of their wireless sensors or, worse, throw them away after two or three years because they have become obsolete.

Pierre Naccache, founding president of Asystom, adds: "We have driven technological innovation by allowing the devices to 'wake up' just when needed. Asystom devices can be configured remotely to measure in real time but, also and above all, are capable of determining when to take measurements. All data is transmitted in real time and accurately. Information and alerts are presented on an easy-to-use dashboard and, finally, these devices are all manufactured in Europe."


GLOBAL PREDICTIVE MAINTENANCE MARKET FORECAST 2019-2027

source ©: Inkwood Research

source ©: unsplash / Jonathan Lampel

Droniq

Traffic Management for Drones

Droniq is working on integrating unmanned aerial systems (UAS), commonly known as drones, into the (controlled) airspace, in a reliable, secure, and affordable way. By making drones "visible" for other aircraft and airspace control, a significant increase in operational safety can be achieved. To do this, they developed a hook-on device (HOD) called HOD4track, which can be mounted to almost any UAS on the market.

Droniq was founded as a spin-off of the "connected drones" research project, which was initiated by Deutsche Flugsicherung and Deutsche Telekom in 2016. The goal of the project is to demonstrate that drones can be safely integrated into the airspace by using existing technologies, like LTE, GNSS, and FLARM, to unleash their full economic potential. A drone safety solution is highly appreciated with millions of aircraft expected in the future.

The drone traffic management system (UTM) is an independent web platform for drone operators to perform below-line-of-sight missions, like power grid inspections. The UTM calculates a real-time airspace situation display. All drones that are signed into the system are visualized together with their flight routes. Alerts are triggered for potential collisions and airspace can be blocked on demand or when necessary. When the drone operator logs into the UTM the position is calculated by the HOD continuously and independent from the UAS flight controller. If necessary, FLARM (flight alarm) signals received from surrounding air traffic are also sent to the UTM. Additionally, the drone's position is sent via FLARM, making it visible to other aircraft nearby.

The position of the HOD is tracked by a u-blox M8 GNSS module, which supports up to three GNSS systems including GPS/Galileo together with BeiDou or GLONASS at meter accuracy. These low-cost multi-constellation GNSS receivers are affordable for start-ups at a price range of under €100. Operating at 5 V and consuming <400 mA, the whole device weighs only 35 g, which is very energy-efficient when mounted on drones. Even fully equipped with antennas and an external battery, it weighs only 149 g. The four-way antenna constellation enables LTE, GNSS, FLARM, and ADS-B signals to be processed simultaneously.

Droniq is working on a pilot project together with the German military (Wehrtechnische Dienststelle der Bundeswehr Manching), Fraunhofer IIS, and Deutsche Flugsicherung to test anti-spoofing and anti-jamming GNSS applications for civil aviation. The Galileo Public Regulated Service (PRS) has been selected to provide this service for critical navigation. The consortium has built a demonstrator, which is using Galileo PRS on the HOD. This generation of the device transmits the encrypted Galileo PRS signal to the UTM. The goal is to have a protected server environment to decrypt the code within the infrastructure at Deutsche Flugsicherung. This would allow safe operations within the DFS Data Center, together with the UTM.

Davey Bickford

Having a Blast

source ©: Emerald X

The most dangerous moment in mining is when someone lights the fuse and everybody starts running. Davey Bickford, a subsidiary of Enaex, a world leader in mining services, wants to defuse the situation with its remote control electronic detonator, dubbed DaveyTronic Edge.

The system uses a common IoT radio frequency protocol to communicate up to thousands of detonators before triggering each explosive device.

Electronic detonators have been around since the 1990s, but, says Aymeric Denuelle, of Davey Bickford, the Achilles heel were the fixed-wire networks connecting the detonators to the blasting machines, which were complex and prone to electric leakage.

Early wireless detonators were unidirectional – in other words, signals could be sent to a detonator, but no response could be received. DaveyTronic Edge not only does away with the need for surface wiring, but also controls multiple electronic detonators from a single, safe location, thereby making the blasting process less risky and more efficient.

> ” Fixed-wire networks are the Achilles heel of blasting.
>
> **Aymerk Denuelle**
> Davey Bickford Enaex

Until now, mining workers have been forced to manually check conditions before pressing the button – a process known as "priming the blast." This is costly and time-consuming, as well as risky in the event of human error. But the main worry was finding detonators that failed to go off, which required searching for hours through huge piles of debris.

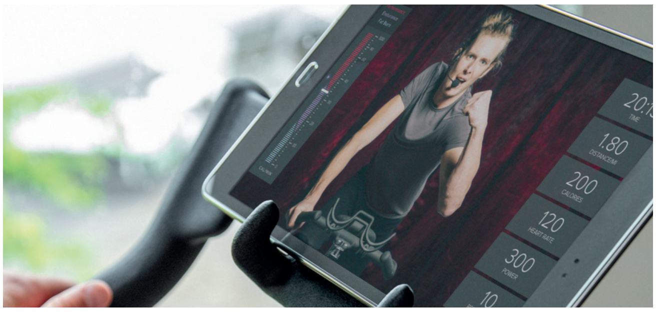
The new system has been successfully tested in a large pit mine in Chile, where it proved capable of operating safely over a distance of several kilometers.

As Aymeric Denuelle says, "Our goal is to always provide safer solutions so that our customers can trigger larger blasts from a remote firing point. Time is money in this industry and mining companies need to spend more time collecting the ore than organizing the blast."

SMART PRODUCTS

Schwinn

Smart Indoor Cycling



Many people have not been able to do their regular workout during the pandemic – with gyms closed in many countries. Riding the smart IC8 Indoor Cycling Bike from Schwinn means workouts can be done at home. The exercise bike uses Bluetooth to connect to apps including Explore the World, Zwift, Peloton, or Kinomap. Information on time taken, virtual distance traveled, calories used, and revolution speed is shown on a mounted LCD display as well as the app, and though heart-rate monitoring is enabled, it requires extra purchases. There is also a holder that can take a smartphone or a tablet. The IC8 can be adjusted for people between 1.55 meters and 1.95 meters tall. The bike weighs 50 kilograms and is available for $1,000. **www.global.schwinnfitness.com**

Klafs

A Sauna for the Smaller Home

Private saunas were once the preserve of households with sufficient space. Klafs is changing that with the foldaway Sauna S1. Fully retracted it is only 60 centimeters deep – about the size of an average closet. Pushing a button on the compact controls prompts silent motors to extend the three elements to add an extra meter to the S1, making it ready to use within 20 seconds. The back wall has a specially designed integral air channel, allowing optimal heat circulation and a healthy thermal environment in the sauna. It's so self-contained, if you move house, you can take the sauna with you just like a piece of furniture. The S1 is available in three sizes with five different exterior trims (white, white satin, Swiss pine, walnut, and oak) and four different front panels. **www.klafs.com**

Arlo

Security under the Spotlight

Arlo is updating its Wire-Free Spotlight Camera range with two models: the Pro 4 and Ultra 2 security systems. The Pro 4 delivers 2K HDR video quality and has an integrated spotlight with color night vision and 160° field of view. It connects directly to Wi-Fi, so it may be used as a stand-alone camera or as a complement to an existing Arlo ecosystem. The Ultra 2 offers the same features but upgrades the video to 4K with HDR and 180° field of view. Its improved Wi-Fi connectivity offers better performance under challenging Wi-Fi conditions. **www.arlo.com**

Brava

Making Light Work of Cooking

It has been some time since the microwave oven made its way into the home and changed the way people prepare their food. Now Brava hopes to make a similar impact with its pure light technology, an oven that uses visible and infrared light to cook many kinds of meals. The Brava oven has a built-in camera, particulate sensors, a humidity sensor, and an array of seven thermometers to assess the condition of the food, air, and cooking chamber. Six halogen lamps heat the food and can reach up to 260°C in a tenth of a second – that enables the oven to cook faster, sear quicker, and retain juiciness. Three zones of ingredients can be cooked simultaneously and algorithms control the heat and light, allowing baking, dehydrating, air-frying, and more. Wi-Fi connectivity means that new programmed recipes can be added every week and instructions, or just the camera image, can be displayed on the oven's five-inch touch screen – or on a smartphone app. Currently only shipped in North America, prices for the oven start at $1,095, which includes a two-year subscription to the Brava Plus recipe service. **www.brava.com**

Razer

Cool Glasses for Gaming on a Sunny Day

Razer is mainly known as a maker of computer peripherals especially aimed at gamers. Now the company has presented its first wireless communications eyewear product, Anzu Smart Glasses. Designed as sunglasses, the frames conceal open-ear audio and an omnidirectional microphone which connect to smartphones or computers via 60 ms low-latency Bluetooth. Despite the additional hardware, the glasses only weigh 48 grams and Razer claims the Bluetooth, originally developed for gaming, will make experiences more immersive. The ability to hear ambient sounds as well as transmitted audio allow the wearers to enjoy digital entertainment anywhere, while working or when outdoors. The frames are available in two designs – rectangular or round – and the lenses combine blue light filtering (35 percent protection) with UVA/UVB protective polarization (99 percent protection). For those who lack 20/20 vision, online optician Lensabl is offering a 15 percent discount on prescription lenses for buyers of the Razer Anzu. **www.razer.com**

Sony

VR to Become Reality for PS5

From launch, Sony's PlayStation 5 (PS5) has only supported virtual reality games programmed for the PS4. Among these games are *Astro Bot: Rescue Mission*, *Tetris Effect*, *Blood & Truth*, *Moss*, *Beat Saber*, and *Resident Evil 7 Biohazard*. Now, Sony has announced a next-generation VR system that is being exclusively developed for the PS5. The company claims this will bring dramatic leaps in performance and interactivity as well as enhanced resolution and field of view. The headset will be accompanied by a new VR controller that incorporates some of the features from the successful DualSense wireless controller. No images of the headset have been provided yet because it's still in development and Sony has said it will not ship before the end of 2021. Despite this, it does show that Sony is still seriously pursuing the path to a truly immersive experience for gamers. **www.playstation.com**

Blackmagicdesign

Multi-Camera Production for Everyone

The Covid pandemic has brought massive changes to the way we communicate – it seems like almost everyone has become a broadcaster, if only on Zoom, Microsoft Teams, and other free platforms. For the more ambitious, Blackmagicdesign's new series of its Atem Mini streaming boxes allows anyone to create professional, multi-camera productions for live streaming to online services, such as YouTube, Skype, or Zoom. The switches come with up to eight video camera inputs, but computer signals or smartphone displays may also be transferred to the switch. One of the built-in digital video effect generators allows picture-in-picture effects. There are five models available: the original Mini, the Mini Pro, the Mini Pro ISO, the Mini Extreme, and the Mini Extreme ISO. The latter is the top of the range and has eight HDMI inputs, four advanced chroma keyers, six independent DVEs, two media players, two downstream keyers, 16-way multiview, two USB connections, and two HDMI auxiliary outputs. It is available at $1,000, while down the range, the Atem Mini, which was introduced in late 2019, is still available for $300. **www.blackmagicdesign.com**

Dogness

Wayward Pets Collared

Chinese company Dogness, a developer and manufacturer of pet products, has released the Smart GPS Pet Tracker, a collar or harness-attached device that acts as a virtual leash. The GPS tracker has a 4G SIM card built in to show the pet's real-time location on the owner's smartphone. In addition to GPS, the device also uses Wi-Fi, high location accuracy and connection speed wireless location-based services (LBS), and Assisted Global Positioning System (A-GPS) to allow high location accuracy and connection speed. The battery will work more than a week on standby and it can be charged by cable or wirelessly with the supplied Qi pad. Pet management features in the app monitor activity and health and an alert can be sent if a pet leaves or returns to a "virtual fence" area defined by the owner. **www.dogness.com**

Insta360

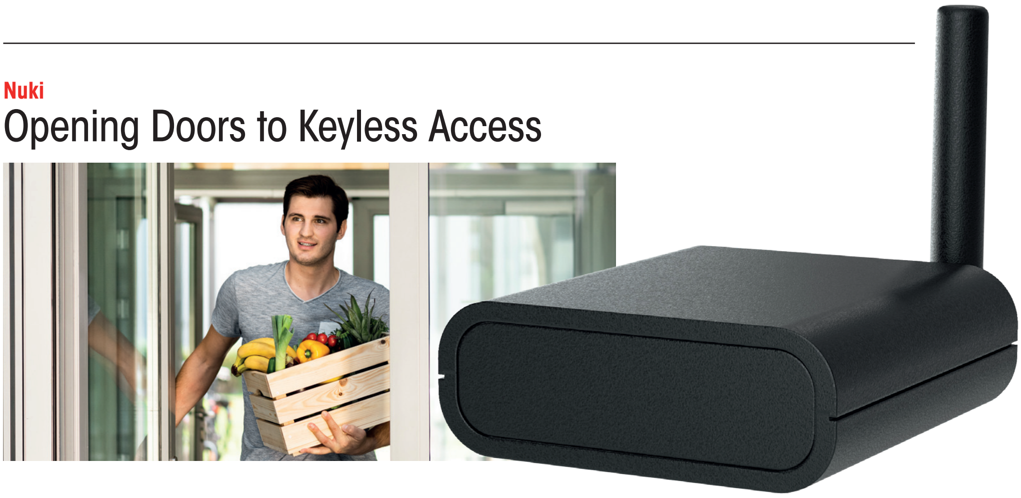
Smallest Camera for Big Action

What can you expect from a camera that weighs only 27 grams and takes up the space of two sugar cubes? The Go 2, the second version of Insta360's action camera, offers a 1/2.3-inch image sensor that captures ultra-wide-angle photos and videos which are stored internally in 1440p format. An integral magnet makes it easy to attach the camera firmly to magnetic surfaces and there is a range of accessory mounts available for other fixings. For action shots, internal sensors ensure the horizon is always level and Insta360's FlowState stabilization keeps the images and videos smooth and in focus even when the camera is attached to a mountain biker's helmet or worn by a surfboarder. It could even be fixed to a pet's neckband and the resulting shots viewed over Wi-Fi. The camera is controlled over Bluetooth from a small console in the charging case, but a smartphone app can be used to give a better idea of what is being captured. The Insta360 Go 2's integrated battery provides up to 150 minutes of shooting, and editing can be done automatically by the artificial intelligence algorithms in the FlashCut 2.0 app. The camera is available for $299.99.

www.insta360.com

Nuki

Opening Doors to Keyless Access



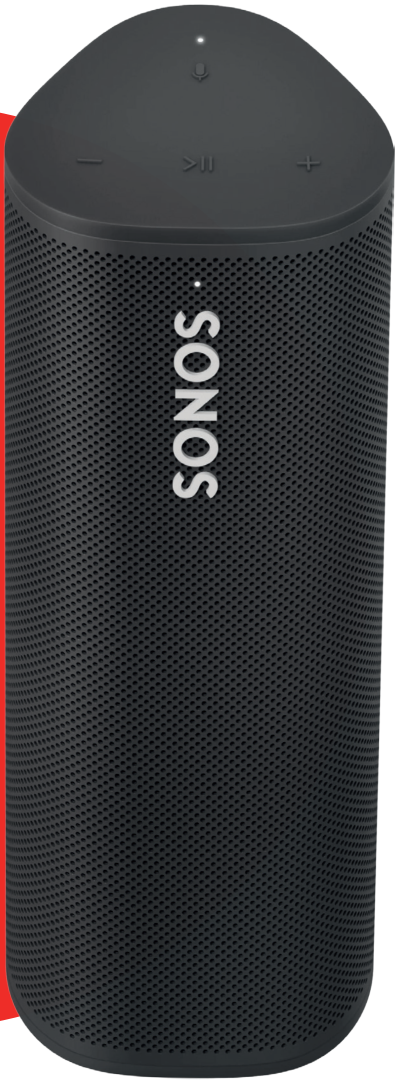
Austrian smart-lock specialist Nuki's latest product allows smart access from the street into apartment blocks for all residents. Nuki Box is installed in a building's main entrance intercom and door release system, allowing residents to open the door using a smartphone app. While the company's established solution Nuki Opener is fitted to the intercom installed within an individual flat, the new product can be used by all residents. Nuki Box is compatible with a wide range of installations and administrators can create permissions for tenants, members, service providers, and other essential visitors. This could significantly reduce the administrative burden for property owners and save them money. The owners can also enable residents to assign individual authorizations for themselves. **www.nuki.io**

Sonos

Music Wherever You Roam

The new Sonos Roam ultra-portable smart speaker can be connected to Sonos systems on Wi-Fi at home – when it is taken outside, it automatically switches to Bluetooth. Another new feature, called Sound Swap, allows users to switch the music to the nearest speaker on a system just by holding the play/pause button. Sonos claims it has made great efforts to provide powerful features and adaptability in this relatively small and light speaker, which weighs less than half a kilogram. Sonos SEO Patrick Spence said: "It's not only our smartest and most versatile speaker, it's also our most affordable. Roam provides the opportunity for millions of new customers to get started with Sonos and it is the right product at the right time as we begin to gather again with friends and family." The speaker, costing $169, is available in shadow black or lunar white. It is dustproof and waterproof, with silicone end caps to protect it against drops or bumps.

www.sonos.com



Garmin

A Smart Watch for Smart Women

Garmin claims the Lily to be “the small and fashionable smartwatch women have been waiting for” and it features menstrual cycle and pregnancy tracking to emphasize the point. Indicators may be logged alongside other health and wellness data in Garmin Connect, which can also give exercise and nutrition advice. The watch can also monitor respiration, pulse oximetry, stress, hydration, advanced sleep, and heart rate (users may configure alerts for high or low readings). In addition, specific monitoring shows the body’s current energy level – this can help with scheduling workouts, rest times, and sleep. Sports apps for yoga, Pilates, cardio, treadmill, and more are also available. Outdoor activities may be tracked if the watch is connected to a compatible smartphone. An assistance feature can also send location details to emergency contacts. The Garmin Lily is available in two styles: the classic model costs $249.99 and a sports model is $50 less. www.garmin.com

Nanit

Comprehensive Smart Baby Monitor

The Nanit Pro not only monitors sleeping babies, it also tracks their sleep quality, breathing motion, and growth. Its 1080p FHD color video and digital zoom camera can also capture precious memories – and the system provides parents with personalized guidance to help their baby sleep better. A Smart Sheet allows parents to measure a baby’s height and track growth through the camera app. Internal speakers deliver higher quality sound and audio for features like two-way talk, playing nature sounds, and real-time sound notifications. www.nanit.com

Coulisse

Easy Roller Blind Automation with HomeKit

Coulisse, in collaboration with smart-home specialist Eve Systems, has launched a range of motors incorporating Apple HomeKit technology. The modules include wireless motors for roller blinds, venetian blinds, cellular shades and curtains. Together, the companies want to make motorized blinds a mass-market product by simplifying their installation and programming. The blinds connect to a smartphone app via Bluetooth, so no gateway or bridge is needed and setup is achieved by simply scanning a QR code. All data is stored locally on the motor for security – data exchanged in the home stays in the home. The blinds also interact with other HomeKit certified accessories, like light bulbs, thermostats and movement detectors. www.coulisse.com

Yeelight

Lighting Up Google Seamless Setup

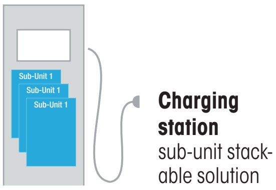
In partnership with Silicon Labs, Yeelight has developed a smart LED light bulb that supports Seamless Setup in the Google Home system. The multicolor Smart LED Bulb M2 works with Silicon Labs’ Wireless Gecko Bluetooth BG21 system-on-a-chip (SoC), which enables users to connect and control smart home devices in Google Home without the need to install other apps. Both companies say they are seeing increasing consumer demand for sophisticated, user-friendly smart home products with simplified setup requirements and Google Assistant voice control. Yeelight’s Bulb M2 is one of the first to deliver smart lighting integration with Seamless Setup. The bulb can display multicolored effects, adjustable color temperature, and its brightness goes up to 1,000 lumen. A Google Nest device may act as a hub to connect smart home devices to the web. www.yeelight.com

Power Electronics

SOLUTION FOR DC FAST CHARGERS STATIONS

STPOWER STM32

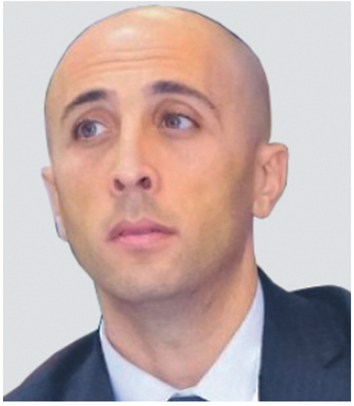
The global Electric Vehicle (EV) charging station market size is projected to reach over 30 thousand units by 2027 growing at an average rate of close to 50%. DC fast charging is expected to grow fastest since it provides charging of EVs within 30 minutes. DC fast chargers work in a power range of 30-150kW and generally are implemented with a modular approach. This is based on 15-30 kW sub-units, which are stacked to create the higher power system. This approach provides a flexible, safe, and affordable solution.ST offers efficient, smart products and solutions for the key stages of each sub-unit - Power Factor Correction (PFC), DC-DC and Control unit & driving.



Charging station sub-unit stackable solution

The **power factor correction (PFC) stage** can be implemented through different configurations (e.g. 3 phase Vienna topologies) and ST offers a wide variety of devices based on customer needs:

- 650V Gen 2 Silicon Carbide (SiC) MOSFET (SCT*N65G2) featuring very low Rdson per area and excellent switching performance to enable efficient and compact designs.
- 650V HB2 series IGBTs (STGW*H65DFB2) ensuring higher efficiency in medium to high-frequency applications.
- 650V MDMesh™ M5 Series Power MOSFETs series (STW*N65M5) with high VDSS rating, outstanding RDSon x area, and excellent switching performance.
- The new 650/1200V series SiC Diodes (STPSC*H65 and STPSC*H12) combine the lowest forward voltage with high forward surge current robustness



For input rectification, we offer the following devices:

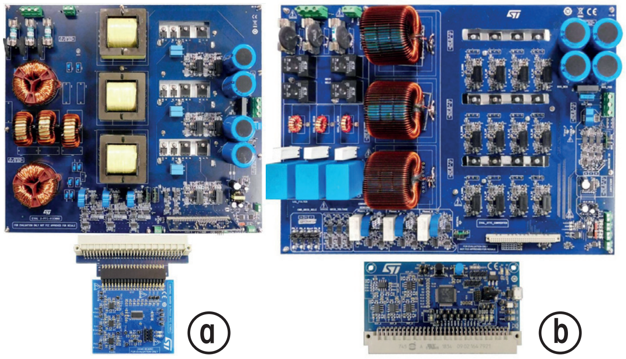
- SCR Thyristors such as the TN*50H-12WY offer 1200V blocking capability with optimized power density and surge current capability.
- Rectifiers such as the STBR*12 1200 V family with its low forward voltage drop, improves the efficiency of the input bridges.

In the **DC/DC conversion stage,** a full bridge resonant topology is often preferred due to its efficiency combined with galvanic isolation. Examples of the products ST proposes here are the SiC MOSFETs Gen 2 1200V series (STPSC*H12) and the SiC Diodes 1200V Series.

> ST solutions help customers to address the challenges of power management and control.
>
> **Luigi Galioto**
> Technical marketing engineer

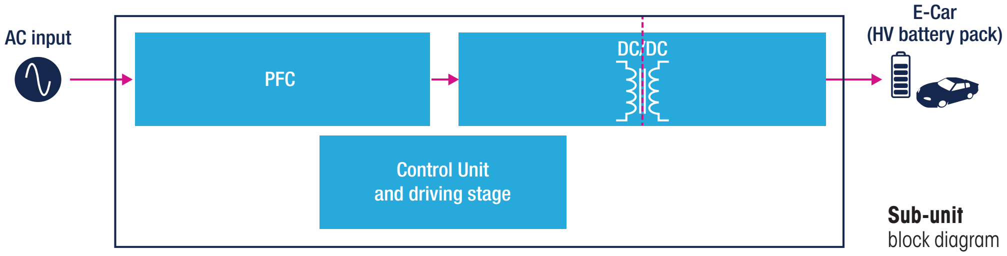
For the **control unit** ST offers two STM32 microcontrollers designed for power management applications- the STM32G474 (STM32G4 family) and the STM32F334 (STM32F3 family) The STM32G4 builds on the STM32F3 series and offers an ARM® Cortex®-M4+ core running at 170 MHz with three different hardware accelerators and a rich set of advanced analog peripherals. ST also offers digital controllers such as the STNRG388A which can independently pilot six configurable PWM clocks.

For the **Driving stage** ST offers innovative products such as the STGAP-2SICS - a 6kV galvanic isolated single gate driver designed to drive SiC MOSFETs.



Evaluation Boards

ST offers system evaluation boards enabling developers to test products directly in the final system. For DC Charging station our offer includes: The STDES-VIENNARECT (fig. a) with a 15 kW, Vienna rectifier with mixed-signal control for the PFC stage, and the STDES-PFCBIDIR (fig.b) with a 15 kW, three-phase, three-level Active Front End (AFE) bidirectional converter for PFC stage.



Sub-unit block diagram

SCIENCE FICTION OR SCIENCE FACT?

Gerd Leonhard
is the founder of
The Futures Agency (TFA)
and author
of the bestseller
Technology vs Humanity.
He is based in Zurich.

Two major forces are at work in the realm of exponential technologies: artificial intelligence (AI) and human genome engineering. AI can be simply defined as creating machines (software or robots) that are intelligent and capable of self-learning and therefore more like thinking machines.

The companion game changer to AI involves altering human DNA to put an end to some, if not all, diseases, reprogram our bodies, and possibly put an end to death. AI, of course, would be a critical enabler of such reprogramming. The power of AI is widely projected to grow twice as fast as all other technologies, exceeding Moore's Law and the growth of computing power in general.

These two game changers and their scientific neighbors, such as machine learning and genomic medicine, will have a huge impact on what humans can, and will, be in less than 20 years. Machines will do things that were once the sole domain of human workers, blue collar and white collar alike, such as understanding languages, complex image recognition, or enabling us to use our bodies in highly flexible and adaptive ways. No doubt, by then we will be utterly dependent on machines in every aspect of our lives.

We are also likely to see a rapid merging of humans and machines through new types of interfaces such as augmented reality (AR), virtual reality (VR), holograms, implants, and brain–computer interfaces (BCI), plus body parts engineered with nanotechnology and synthetic biology.

> ”
> By far the greatest danger of artificial intelligence is that people conclude too early that they understand it.
>
> **Eliezer Yudkowsky**

If and when things such as nanobots in our bloodstream or communications implants in our brains become possible, who will decide what is human? I argue that technology does not, and probably should not, have ethics, but what will happen with our norms, social contracts, values, and morals when machines run everything for us?

For the foreseeable future, despite the claims of AI evangelists, I believe machine intelligence will not include emotional intelligence or ethical concerns because machines are not sentient – they are duplicators and simulators. Yet, eventually, machines will be able to read, analyze, and possibly understand our value systems, social contracts, ethics, and beliefs, but they will never be able to exist in, or be a part of, the world as we are (what German philosophers like to call "Dasein").

But, regardless, will we live in a world where data and algorithms triumph over what I call "androrithms" – all that stuff that makes us human? We often see the humble beginnings of a huge opportunity or threat and then, in an instant, it will either be gone and forgotten, or here and now, and much bigger than imagined. Think of solar energy, autonomous vehicles, digital currencies, and the blockchain. All took a long time to play out but suddenly they are here and they are roaring. History tells us that those who adapt too slowly or fail to foresee the pivot points will suffer the consequences. Wait-and-see is very likely going to mean waiting to become irrelevant, or simply to be ignored. We will need a new strategy for defining and retaining what makes us human in this rapidly digitizing world.

WE TALK IOT, THE SMART INDUSTRY PODCAST

Welcome to We talk IoT, a regular series of podcasts from the editors of Smart Industry – the IoT Business Magazine. Our podcast keeps you up to date on the most important developments in the world of IoT, IIoT, Artificial Intelligence and Cognitive Computing. Listen to leading industry experts, business professionals and experienced journalists as they discuss some of today's hottest tech topics and how they can help boost your bottom line.

You can listen to the first episode right here on smart-industry.net. Or you can follow We talk IoT, the Smart Industry podcast on the following streaming providers to always get the latest episodes:

- Go to Spotify
- Go to Apple Music
- Go to Soundcloud

This podcast is brought to you by Avnet Silica in cooperation with Microsoft.

powered by AVNET SILICA

Leading-edge Solutions for Fast Charging Stations

life.augmented

Complete solutions for high-efficiency designs

Power Factor Correction & DC/DC

Silicon Carbide MOSFETS
650 /1200 V series

IGBTs
650 V HB2 series

Power MOSFETs
650 V MDMesh M5 Series

Silicon Carbide Diodes
650/1200 V series

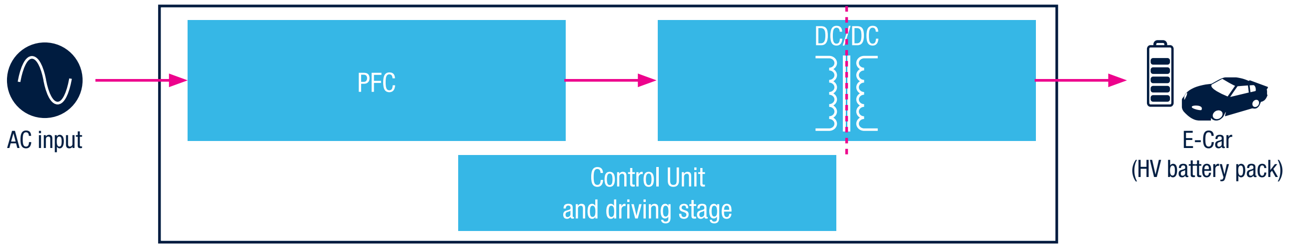
Input Rectification

SCR Thyristors
1200 V TN*50 H - 12 WY series

Rectifiers
1200 V STBR*12 series

Driving Stage

Isolated Gate Driver
STGAP2SICS - 6 kV isolated driver



Control Unit

32-bit Microcontrollers
STM32G4 Series

Digital Controller
STNRG388A for power conversion

Evaluation Boards

15 kW Vienna Rectifier Board
STDES-VIENNARECT

15 kW three-level Active Front End
STDES-PFCBIDIR

For more information visit www.st.com/ev-charging