COGNITIVE TIMES

TRANSFORMING OLD INDUSTRIES WITH NEW TECHNOLOGIES

FLOWSERVE IS USING ARTIFICIAL INTELLIGENCE TO SPARK THE NEW INDUSTRIAL REVOLUTION

MARCH 2017

SPARKPREDICT®

We know that unexpected equipment failure can bring your operations to a costly standstill. SparkPredict® identifies imminent mechanical issues long before problems occur, allowing maintenance schedules to be optimized and ensuring you won't be caught off guard by asset failures.

sparkcognition™ | *Human Intelligence at Machine Scale®*

26
THE NEW INDUSTRIAL REVOLUTION
After 220 years, Flowserve is still innovating, and today uses predictive maintenance powered by artificial intelligence to produce the industry's top hardware.
by **Marla Rosner**

16
A.I. ON THE BATTLEFIELD
A FRAMEWORK FOR ETHICAL AUTONOMY
by **Amir Husain** and **General John Allen (Ret.)**

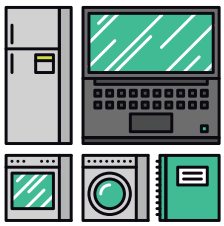
38
ASSEMBLING THE SYSTEMS
HOW TECHNOLOGY PARTNERSHIPS ARE ENABLING THE IoT
by **John King**

contents

04 **Important Dates From History & Today**

06 **IoT Security: The New Challenge for Oil & Gas**

08 **Driving Into the Future**



10 **How Secure is the Internet of Things?**

12 **Finding Threats in the Industrial Internet**

14 **Oil & Gas, A.I., and the Promise of a Better Tomorrow**

19 **The Cogniteam** Comic Strip

20 **A.I. in Social Media**

21 **A.I. for Oil & Gas: Is it Time to Invest?**

32 **2017 A.I. & IoT Landscape**

33 **Cancelling Flight Delays: Predicting the Future of Aircraft Maintenance**

36 **But What About Smart Buildings?** The Importance of IoT-Enabled Structures in Smart Cities

42 **Building the Mind of a Caddy:** How A.I. Could Revolutionize Golf

Amir Husain
Editor in Chief

John King
Executive Editor
Production Director

Jon Coyle
Art Director & Designer

Victoria Salas
Managing Producer

Milton Lopez
Producer

Kimberly Erler
Producer
Editor

Marla Rosner
Staff Writer

Contributing Writers
Caroline Lee
Philippe Herve
Keith Moore
Kimberly Erler
Jerry Schirmer

FROM THE EDITOR

by **Amir Husain**

This edition of Cognitive Times is dedicated to the Internet of Things (IoT). This is a topic that's been covered quite often in the popular press, but we hope our somewhat unique take on the subject will be received by our readers with interest.

But where did IoT—this network of embedded devices that increasingly pervades physical space—even come from? Why is it happening now? In truth, IoT adoption is a result of the miniaturization and cost reduction in electronic device fabrication. In other words, we owe the existence of the IoT to Moore's Law. While one consequence of Moore's Law is talked about quite often, i.e. the doubling of transistors in the same amount of space every two years or so, its cost corollary is more often ignored. If you don't want to build a massive, modern general purpose processor with a budget in the billions of transistors, but instead have a more modest goal in mind, you can elect to pay less, and use a smaller amount of space and power. This is precisely why, on the one hand, Moore's Law enables a processor like the Intel Xeon Broadwell-E5, with a transistor count approaching 8 billion, to cost thousands of dollars, while on the other hand, a fully functioning computer in the form of the Raspberry Pi Zero, is a mere five dollars.

The Raspberry Pi Zero and a plethora of literally hundreds of convenient, highly integrated embedded boards have the ability to run a full fledged operating system, provide support for multi-threaded TCP/IP communications (the ability to act as an Internet server or client), access anywhere from megabytes to terabytes of storage, and integrate with external devices, displays and sensors while sipping power from a battery. All this, for anywhere from five to a hundred dollars. You can buy a Happy Meal from McDonalds, or you can buy a computer. How crazy is that?

"So what?," some might ask. So what if you can buy a computer for five dollars? And the answer isn't simple to give, because it is multifaceted. First, when a computer this capable costs five dollars, you can embed it everywhere. In cheap appliances, home fixtures, industrial machines, wearables, cars, trains, planes—or, more likely, every plane seat and armrest—underneath the pavement, in manhole covers, and almost everywhere else you can imagine. We will go from one device per person—the famous Microsoft slogan "a computer on every desk," to hundreds of computers per person. This means that we can process and capture data from everywhere.

Second, inexpensive computing hardware, when combined with smart algorithms, means that we can automate more of the world around us. Not only can we process the data from the burgeoning IoT, but we can make automated decisions and actuate physical systems. The world will increasingly be controlled and run by these systems.

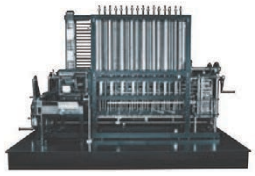
Third, with a number of software innovations, such as blockchain, the distributed storage system borrowed from cryptocurrency, IoT systems will be able to function and communicate reliably without requiring a central coordinator. This means that a world built on IoT technology will be both intelligent and autonomous in a federated fashion. It will be resilient.

Of course, this next stage of the industry's evolution does place additional responsibilities on those of us who are responsible for transforming these dreams into functioning infrastructure. The need to deliver security is one such responsibility. We cannot play fast and loose with IoT security, particularly when it comes to systems that control or actuate. The downsides would be tremendous. Equally importantly, if we are going to automate physical actuation—changes in the real world based on the output of AI algorithms—we have to ensure that we bring a level of explainability and transparency to AI decisions.

These are exactly some of the areas where SparkCognition and our partners are investing our combined intellectual and engineering capabilities. We know a world covered in intelligent devices will enable a host of opportunities for citizens, businesses and countries. We believe it is a worthy endeavor to build this new world responsibly, safely and with great care.

JANUARY

Jan **21**



Babbage's Analytical Engine Operates for the First Time

In 1822, Charles Babbage began developing the Difference Engine, considered to be the first automatic computing machine. It was capable of computing several sets of numbers and making hard copies of the results. On January 21, 1888 the analytical engine passed its first test.

Jan **8**

Stephen Hawking's Birthday

Stephen Hawking was born in 1942.

Jan **15**

Wikipedia Day

Wikipedia was formally launched on January 15, 2001 by Jimmy Wales and Larry Sanger. It's the world's 6th most popular website in terms of overall visitor traffic and has a total worldwide monthly readership of approximately 495 million.

FEBRUARY

Feb **6-9**

21st Annual ARC Industry Forum

The 21st annual ARC Industry Forum will be held in Orlando, Florida to learn more about how the digital enterprise will be realized and the benefits that this can bring. Discover what your peers are doing today and what steps they are taking in their respective journeys.

Feb **7-8**

2017 IADC Health, Safety, Environment & Training Conference & Exhibition

The International Association of Drilling Contractors is hosting a conference that examines a range of topics impacting accident prevention, environmental protection, competency, and training in the drilling industry.

Feb **12**

Charles Darwin's Birthday

Charles Darwin was born in 1809.

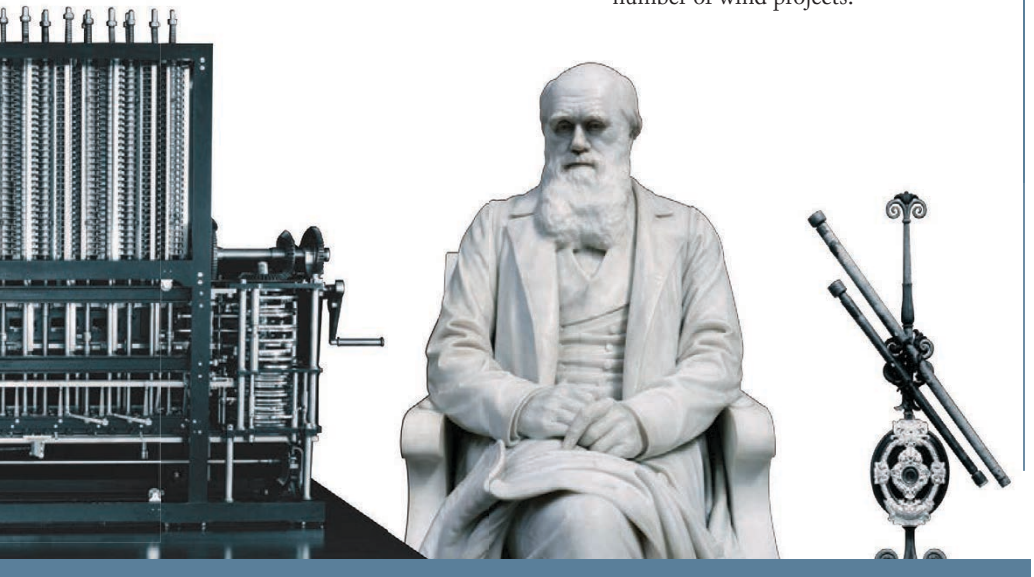
Feb **13-18**

RSA Conference 2017

Take advantage of this opportunity to learn about new approaches to info security, discover the latest technology, and interact with top security leaders and pioneers.

IMPORTANT DATES

FROM HISTORY & TODAY

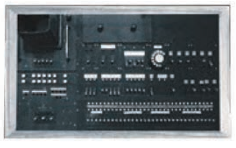


Feb
17

Former IBM CEO Thomas J. Watson's Birthday

Thomas J. Watson served as the chairman and CEO of IBM. He oversaw the company's growth into an international force from 1914 to 1956. Watson developed IBM's management style and corporate culture and turned the company into a highly effective selling organization, based largely on punched card tabulating machines.

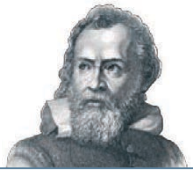
Feb
19



Alan Turing Proposal For ACE (Automatic Computing Engine)

In 1946, Turing presented the "Proposal for the Development in the Mathematics Division of an Automatic Computing Engine (ACE)."

Feb
15



Galileo's Birthday

Galileo was known as the "father of modern physics." With help from an early telescope, he helped remove Earth from the center of the universe. His contributions to astronomy include the confirmation of the phases of Venus, the discovery of Jupiter, and the observation and analysis of sunspots. Galileo was born in 1564.

Feb
28

AWEA Maintenance & Safety Conference

Success means driving operational excellence. The AWEA Operations & Maintenance and Safety Conference is where the industry comes together to recognize unique challenges and identify solutions in these areas. And as the wind energy industry continues to expand, so does the need for an evolving approach to operating the nation's growing number of wind projects.

MARCH

Mar
8

Hydraulic Institute 2017 Annual Conference & Centennial Celebration

This momentous event will recognize the critical role that pumps play in society and honor pioneers, innovations, organizations, and technical achievements that have propelled the industry for the past century.

Mar
14

Pi Day

The math holiday, Pi Day, is celebrated on March 14 (3/14) because the date resembles the ratio of a circle's circumference to its diameter 3.14159265359∞, or 3.14 for short.

Mar
28

Enterprise IoT 5G Summit 2017

Enterprise IoT 5G Summit 2017 is a practical digital transformation conference for IoT strategists, as well as IT and Operations professionals tasked with digitally transforming their enterprise leveraging IoT and 5G technologies. On March 29th, don't miss Amir Husain, SparkCognition's CEO, for his presentation, "AR and AI in the Enterprise: Staying Abreast of the Smart Technology Revolution."

IoT SECURITY: THE NEW CHALLENGE FOR OIL & GAS

by **Philippe Herve, VP of Solutions at SparkCognition**

According to a recent Accenture report, global investment in financial technology (fintech) ventures in the first quarter of 2016 reached $5.3 billion. In the days before the concept of the "digital oilfield" emerged as a result of the proliferation of the Internet-of-Things, companies struggled to find ways to centralize their operational information. It was extremely difficult to efficiently monitor all assets, provide support, and solve problems in real-time for better decision-making. Companies that have been able to do this now are staying competitive and cutting their costs, proving there's still hope for the oil and gas industry. This is great news, yet, in some cases, this transformation presents additional challenges.

Drilling rigs all over the world are powered by expensive machines with tremendously high costs of failure for events such as kickbacks or explosions. With so much at stake, monitoring these systems is a daunting task, which requires a great degree of expertise. In order to maintain and operate this critical equipment, experts are required by their organizations to be physically onsite at the rigs—whether onshore, offshore, or dispersed throughout remote areas around the world—to make critical decisions on the fly and help with asset maintenance. Even though inefficient and at-times laborious, security was rarely a problem as these drilling rigs were most frequently controlled by air-gapped systems, or systems which were not connected to external communication networks. The closed-loop systems made it extremely hard for outsiders to gain unauthorized access to their IT or OT network.

More recently, organizations have started to implement IoT solutions onto their systems. Countless hours and human resources are saved, processes are improved tremendously, and failures are minimized. All the data from almost every system available can now be accessed, measured, and managed in one place. This is a remarkable advancement, yet it is also the reason why cyber attacks are getting more dangerous than ever before. Since systems are now connected, they can be attacked and compromised, even if these controlled systems are dispersed in decentralized locations. This has become such a problem that the energy industry has been cited by the Council on Foreign Relations as the most vulnerable sector to the threat of cyber attack.

Indeed, US ICS-CERT reported that 53% of attacks within the energy industry mainly target control systems using common hacking techniques such as SQL injections, spear phishing, and watering hole attacks. These hacking methods aim to infect your systems through your database, your emails, or exploiting your organization's site browsing behaviors. According to TripWire 2016 Energy Survey, more than 80% of respondents coming from the oil and gas industry acknowledged an increase in the number of successful cyberattacks their organization has experienced the past 12 months, while 68% aren't confident in their organization's ability to detect all cyberattacks.

In September 2015, SecurityWeek Feedback Friday revealed that the systems of the United States Department of Energy was breached more than 150 times between October 2010 and October 2014. This led to significant growth in oil & gas security spending, from $26.3 billion in 2015 to a projected $33.9 billion by 2020.

To sufficiently combat the growth of threats in both number and sophistication, combined with the scarcity of security talent, the oil and gas industry needs a stronger approach to cybersecurity. Keeping this in mind, SparkCognition has developed an AI-based solution for cyber-security, SparkSecure®. The technology is designed to monitor and protect not only the IT infrastructure, but also the OT network.

SparkSecure® monitors all data communications in real time and identifies suspicious and malicious activity on a network. The software signals analysts for where to look in order to identify the exact location of a potential attack, and provides evidence as to the validity and severity of the threat.

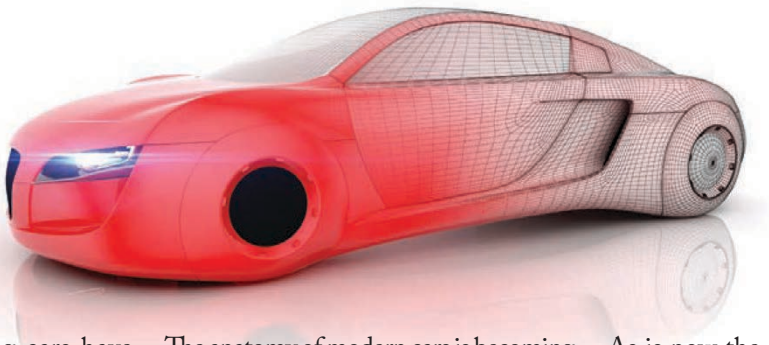
Most attacks today are new, signature-free, zero-day threats. However, with large amounts of accurate and trustworthy information acquired through automated research retained by SparkSecure®, most zero-day attacks can be identified.

Not only that, SparkSecure® algorithms can differentiate between anomalous and malicious behaviors. The ability to do this has significantly minimized the burden of resolving false positives for security teams, saving them time and resources that can be better spent dealing with real threats.

With every advancement comes a trade-off. Driving a car presents more risks compared to walking. However, without cars, we wouldn't be able to travel as efficiently as we now can. We then learn how to maneuver it to minimize the risks. It's the same case for bringing IoT to oil and gas. The energy industry only gets more and more competitive, and companies cannot afford to be left behind. However, if companies can understand the implications and challenges that come with adopting IoT, and actively "maneuver" to find the right technology and security systems, keeping systems secured is an achievable reality.

DRIVING INTO THE FUTURE

by **Kimberly Erler**



Self-driving and flying cars have been romanticized and fictionalized, almost from the time the first Model-T rolled off of the assembly line. Who hasn't longed for a car like KITT they could signal to come pick them up at the front of a packed holiday shopping mall when they had to park in the farthest lot? Certainly at one time or another we've all visualized our own boring cars as Jetson-esque "bubble" cars that would take off and allow us to fly up and away from 5pm rush hour traffic.

Fiction is now reality. And, while we're still working out all of the kinks, it won't be long until several of the cars stuck in traffic with us won't have anyone sitting behind the wheel. In fact, most of those cars won't even have steering wheels. And the first flying car completed its first solo flight in Israel in November of 2016 (but with a price tag of $14 million, civilian applications will be difficult to justify anytime soon).

I recently had the opportunity to drive a highly advanced vehicle with all of the safety features (self-braking, lane guidance, speed control) and auto-steer. While it is a completely disconcerting feeling not to be in control, it's easy to see how the benefits of self-driving cars will far outweigh the fear of not having human intervention in the driving process. But that's not to say that the fear is not legitimate.

The anatomy of modern cars is becoming much different from the cars on which we learned to drive. Where once steering wheels attached directly to a vehicle's axle and wheels, these physical tethers are phasing out. Sensors and computer chips read the direction of the wheel and send signals to the tires. So, if for some reason the electronic system controlling your steering goes haywire, or worse, gets hacked, you'll have no control over the direction of your car. But it's not just the steering—it's every system in the car, from the radio to the brakes—that's vulnerable to interference.

Just as the proliferation of computers spawned legions of people looking for ways of attacking those systems, so too is the advent of IoT technologies in cars bringing forward those seeking to find a way in. In 2015, Chrysler got a wake up call to this very issue when a pair of hackers remotely took control of a Jeep, leading to a recall of 1.4 million vehicles. Luckily, these hackers were only proving a point in a controlled setting to illustrate a critical security flaw. Had they been nefarious in their intentions, who knows the havoc they may have been able to wreak.

The good news is that cyber security and the protection of those things vulnerable to outside manipulation is growing quickly. Closed-systems are being utilized to negate outside interference, especially in the case of cars. As is now the case in Chrysler's Jeep, someone would have to be physically inside an individual car to manipulate its systems.

Weigh those risks against the multitude of benefits, however, and it's easy to see why we're speeding toward this new age in travel. Aside from the obvious road safety benefits (cars that avoid each other, eliminating the dangers of distracted driving), self-driving cars open up a whole new world of possibilities that will change the way we live.

Why buy a car when you can, at a moment's notice, summon a driverless car to take you wherever you need to go? Imagine the cost savings (no car payments, no insurance, no gas). And think about those people who are homebound or restricted to their immediate neighborhoods, because old age or some type of physical or mental disability doesn't allow them to have a driver's license. It will open a whole new world to them.

So, while we may not be able to emulate George Jetson for years to come, we can soon see cars with KITT-like capabilities (even if we'd have to imagine ourselves as David Hasselhoff). Now, if they could just find a way use rocket propulsion a la James Bond's Astin Martin, driverless cars or not, driving would get really fun!

HOW SECURE IS THE INTERNET OF THINGS?

by **Keith Moore**

The Internet of Things is changing the world. Everything is connected, and the amount of data available for consumption is growing exponentially. From a technologist's view, this is an exciting opportunity. From a network administrator's perspective, it's terrifying.

While the majority view IoT as an exciting buzzword, the network administrator understands that the connectivity required by true IoT deployments will lead to safety-critical industrial systems, previously existing behind firewalls, being inevitably exposed to potentially insecure networks. Not only that, but a huge workload will arise in ensuring that countless machines are secured in the first place. As the cherry on top, the network administrator likely understands that the existing defense paradigm already in place for network protection will no longer work.

Something needs to change. Network protection systems need to evolve. To understand how this needs to happen, it's important to look back in time at the history of security—starting long ago before cyber ever existed.

Begin by asking a simple question: how have people historically defended themselves? Prior to 7000 BC, before mass agriculture had fully developed, it was the patriarch who took on the role of defender and was responsible for the well-being of his family. He was tasked with learning how to fight and fend off invaders, regardless of circumstance (think, the movie The Croods, 2013). While it worked to some degree, it was also inefficient because everybody had to devote some of their time to doing it.

As agrarian civilization emerged, people began to live closer together, ending the patriarchal defense system. With that transition, something fantastic occurred. They built walls. Not just around houses, but around towns and villages. This let specialized "soldiers" defend a perimeter and fight for a village, letting the common people on the inside go about their daily lives without fear. This had a variety of other benefits, but most notably it changed how people would live and defend themselves for the rest of history.

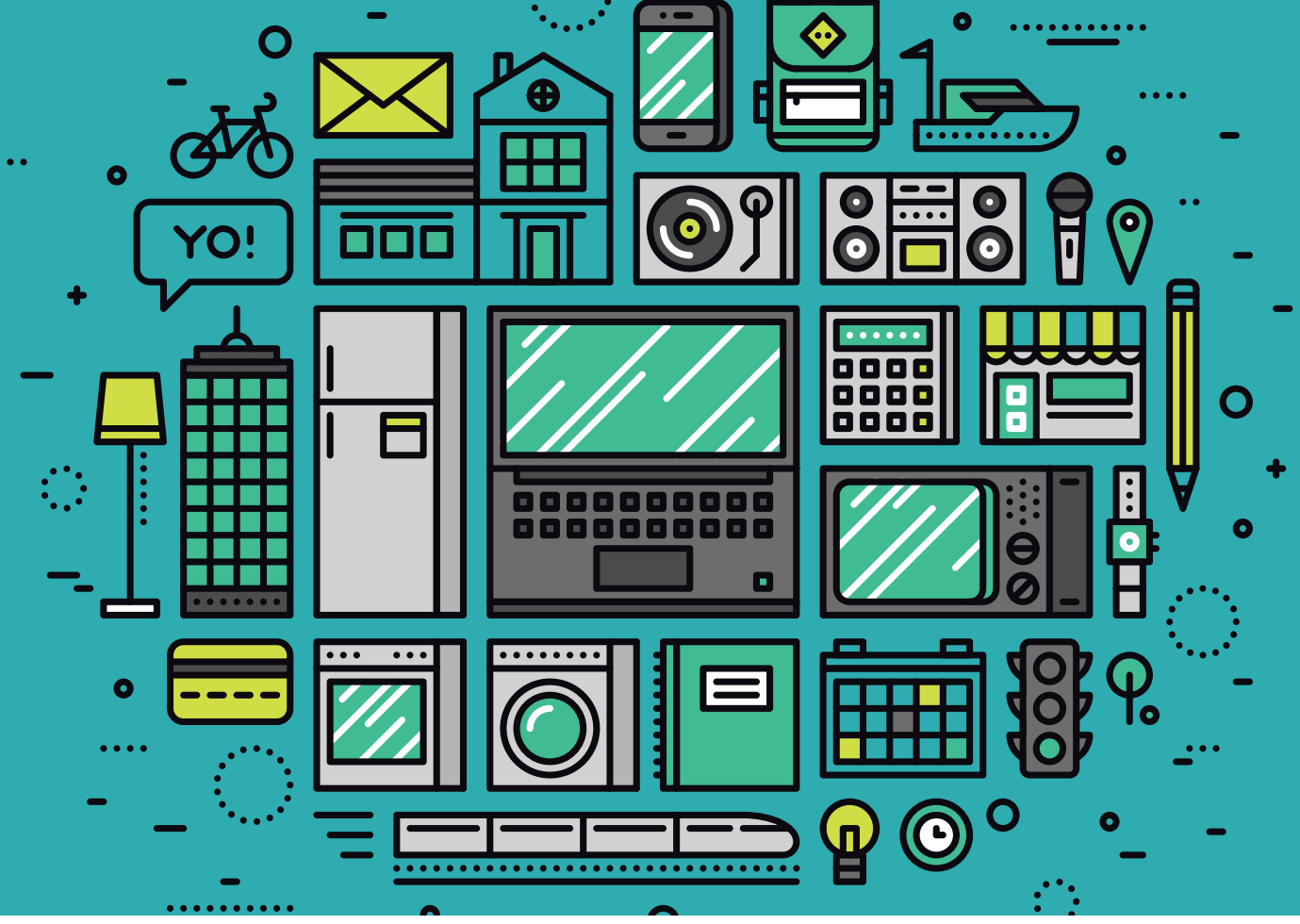
Now, think about how this applies to software, notably software deployed onto the Internet of Things. Think about how you might defend any of those endpoints today. There might be a firewall, but that is a static and slightly outdated technology. To supplement and provide personalized security, most would probably use endpoint detection systems like an antivirus software, which runs an application on the device 24/7 checking for malware. While it works to some degree at defending a system against threats, history has shown that such a solution is rarely scalable when dealing with a shifting threat landscape.

There are a few reasons why endpoint protection will not be sufficient for protecting the Internet of Things:

"THERE ARE MILLIONS OF MALICIOUS FILES CREATED EVERY DAY, AND THE FACT THAT 27% OF ALL MALWARE VARIANTS IN HISTORY WERE CREATED LAST YEAR (KOROLOV, 2016) INDICATES THE LANDSCAPE IS CHANGING AND NON-LEARNING SOLUTIONS WON'T BE ABLE TO KEEP UP WITH THE ONSLAUGHT OF ZERO-DAY ATTACKS."

1) Accuracy—Endpoint protection solutions are traditionally built on signature-based detection methods, which 78% of security professionals agree (Keane, 2015) are not effective against general attacks. Even in some of the best antivirus accuracy reports, only a very small sample size of a few hundred stale malware samples are used to benchmark the products. There are millions of malicious files created every day, and the fact that 27% of all malware variants in history were created last year (Korolov, 2016) indicates the landscape is changing and non-learning solutions won't be able to keep up with the onslaught of zero-day attacks.

2) CPU Usage—According to a report published by Hobson and Company (Casten, 2009), antivirus software can account for over 15 minutes of downtime per week on endpoint desktops and laptops. This amounts to over $300 of downtime per year



per endpoint covered, and that's on robust systems designed for intense computations. An average IoT node is barely a step up from a Raspberry Pi regarding compute capability. That 15 minutes of downtime for a laptop could translate into hours of downtime for an IoT controller. In order to get around that, the antivirus solution needs to be so lightweight that it is no longer capable of adequately detecting threats. Such a solution would be unacceptable in the IoT world, as worms are often designed to propagate between nodes (i.e. Stuxnet). If that affected node was the controller for heavy machinery like a combustion turbine, any effectual downtime would be highly significant for the lives of many.

3) IT Burden—While it has been established that endpoint security is not going to be 100% accurate, this lack of accuracy also accounts for lost economic value outside of missed threats. False positives from endpoint solutions cause companies to spend nearly $1.3M and 21,000 hours of wasted time on IT support every year (New Ponemon Report Reveals High Cost of Dealing with "False Positive" Cyber Security Alerts, 2015). These numbers cannot scale with the Internet of Things—there are not enough IT jobs to support it, and there will be too many operating systems to work across. According to a survey by the SANS institute, the lack of people and dedicated resources maintaining threat detection systems is the leading contributor to why attacks go undiscovered (Shackleford, 2015). As the number of endpoints available for attack increases, the potential for more undiscovered attacks rises, and the IT burden grows.

As history shows, the future of IoT will need a better security solution than just a firewall paired with an endpoint detection system. It will require something that is more accurate, more scalable, and less intrusive.

The solution lies in building a true perimeter detection system capable of evolving as threats change. Endpoint protection, for the time being, may be a necessary evil in some places, but new Artificial Intelligence technologies will make it possible to significantly improve perimeter security with no adverse effects to end users or nodes. These tools can patrol the perimeter of an organization and provide enhanced threat visibility, automated evidence reporting, and rapid incident response, all in a dynamic environment at machine speed.

Building firewalls was a great start, but cognitive perimeter detection tools are capable of taking security to the next level. Not only can they view externally-facing log data (i.e. firewalls, web servers, etc.) and identify threats before they root and multiply, they can also sit on the outside and look in to find insider threats, malware propagation, and malicious intranet traffic patterns.

When paired with good data sources, cognitive perimeter detection methods will provide scalable, accurate solutions behind the scenes, effectively securing the borders so that end users and IoT nodes never need to worry.

FINDING THREATS IN THE INDUSTRIAL INTRANET

Jerry M. Schirmer, Ph.D
Senior Data Scientist at SparkCognition

If you read a book on statistical modeling, often you will read about examples where the data is beautifully presented, with several independent variables each having a well-defined meaning, and then mapping onto a known dependent variable. It is then the task of the statistician to merely apply some known procedures, turn the crank, and produce the correct model. As one may assume, in practice, data rarely comes out this way. In this article, I'm going to talk about a case where we were able to take some data that had little external meaning, and extract actual information from it.

So, in this case, we were hired to investigate the intranet traffic of a large industrial facility. We were provided with a series of network addresses, timestamps of occurrance, a label giving us whether the event was blocked or not, and some information about what protocol was used. From this, we were asked to identify any evidence of threatening behavior in the network traffic. How were we able to do this?

The first step was to realize that each of these internal addresses represented a physical computer in their network, and that they all talked to each other. From there, we were able to construct a graph of how information traveled through the system. Furthermore, a deeper dive in the data showed instances where the intranet traffic touched the open internet, and some smaller cases where traffic touched blacklisted IP addresses. Combined with the known labels, we were able to identify bad action by three criteria:

1. Contact of a machine with blacklisted entity

2. Frequency with which a machine engaged in behavior blocked by the client system, per their logs

3. Statistical outlying behavior derived from the first item

4. Second-order threat risk

Items 1, 2, and 3 should be familiar enough, but what is meant by "second order threat risk?" After we've assigned threat scores from the first two items, and knowing the graph of the intranet traffic, and after some operationalization to map continuous variables as you would see in a fluid to the discrete variables that you see in a graph, we are able to apply a generalization of the diffusion equation:

$$\frac{\partial \phi}{\partial t} = C\nabla^2\phi$$

Here, $\phi(\vec{x}, t)$ represents the threat score of a particular node in the graph, x represents distance along the graph, and the "time" variable is a count of contacts along nodes. This equation is more famous for describing the rate at which, say, a drop of dye will mix with water that it is submerged in, but here, we use it to describe the traveling of a threat vector through the network. Using this algorithm, even with minimal input data, we are then able to determine threat scores for every node on the network, simply using information about exposure risk. In this case, we were then able to turn around to the customer and have them identify actual problems on their client computers from the information provided. What's better is that the underlying mathematics would apply equally to any system where you have ground truth risk that is able to propagate around a system of identical components.

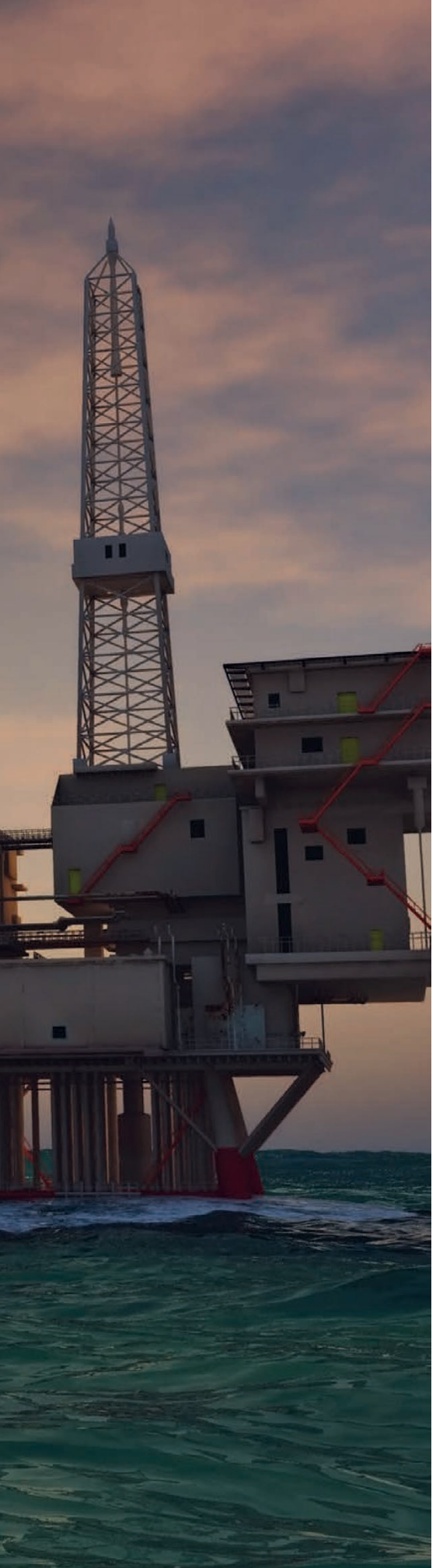
COGNITIVE TIMES March 2017 12

Momentum

WATCH LIST • 2016

OIL & GAS, A.I., AND THE PROMISE OF **A BETTER TOMORROW**

by **Keith Moore**



The price of oil has fallen over 60% since summer 2014, and anybody reading the news sees it mentioned on a daily basis. With all of the negativity portrayed in the day-to-day headlines, many forget that the oil and gas business is one of the largest, most globally-important industries in the world. All is not lost. In fact, there is much to gain.

As the Motley Fool has called out, there is a huge amount of opportunity in the oil and gas industry, notably because it has weathered times like this before.

One of the things that happens during downturns is that companies innovate. As we have seen historically, the companies that emerge the strongest during these times are the ones who adopt innovative technologies to promote growth. These companies are now embracing technologies like machine learning and artificial intelligence to optimize operations in all areas—most notably in upstream drilling and downstream production.

To delve further into how they are being used, machine learning algorithms are being fed by downhole (MWD) and surface (EDR) data systems to predict the likelihood of catastrophic or downtime-related events. For example, what if you had the ability to predict events like kicks or a blowout? This would be significant for two unique reasons.

Blowouts are catastrophic, often resulting in the loss of life. Look at how the Deepwater Horizon blowout affected BP operations. On top of the loss of life, BP had over $42.2 billion in fines, reparations, and court costs.

Identification of potential blowout conditions long before they occur, allows for control system settings to be modified for optimal production. This means that not only is the likelihood of a catastrophic event reduced, the potential for revenue is maximized. How is this done?

One of the unique capabilities that machine learning algorithms bring to the table, is the ability to identify how shifting, dynamic conditions result in different events occurring. Instead of just measuring pressure differentials between zones, machine learning algorithms can look at asset operational data, pressures, mud properties, temperature, and any other data to understand exactly what is happening downhole at that specific well. More impressively, these algorithms are able to do this without ever leveraging the physics-based equations that have been the staple of this industry for decades.

All of this data is then analyzed in an automated fashion to understand if the existing conditions could lead to a non-optimal event such as a kick, blowout, or wellhead failure. Because of the algorithm's innate understanding of what contributes to the likelihood of each event, recommendations can then be fed into the control system to not only minimize the odds of an event occurrence, but also to maximize output.

Machine learning and artificial intelligence are redefining how the oil and gas industry operates on a daily basis—helping to cut costs, optimize efficiency and, in the end, push through another downturn.

In summary, while prices will always fluctuate, by capitalizing on innovation, the oil and gas industry will continue to thrive. Machine learning and artificial intelligence are changing how daily operations are improved—helping to cut costs, optimize efficiency, and in the end, push through another downturn.

A.I. ON THE BATTLEFIELD

A FRAMEWORK FOR ETHICAL AUTONOMY

by **Amir Husain** and **General John Allen (Ret.)**

Autonomy is coming to warfare, and some would say it's already here. Weapon systems driven by artificial intelligence (AI) algorithms will soon be making potentially deadly decisions on the battlefield. This transition is not theoretical. The immense capability of large numbers of autonomous systems represents a revolution in warfare that no country can ignore. As we march towards this reality, it is important that technology leaders and military strategists begin a discussion around the moral and legal framework within which such autonomous capabilities will be enabled.

THE THIRD OFFSET

Deputy Secretary of Defense Bob Work has spent the last year describing the Department of Defense's "Third Offset Strategy," which seeks to revitalize the United States' strategic supremacy. Our "Offset Strategy" is our nation's competitive advantage for both military might and peacekeeping. However, this advantage is currently under threat as other countries improve their own forces and technologies.

These threats have eroded the advantages of our previous "Second Offset Strategy"—the United States' mastery of conventional, precise smart munitions. The best demonstration of the power of smart weaponry was the Gulf War, where a battle-hardened Iraqi Army was unable to respond to the swiftness and precision of new U.S. munitions, such as the JDAM (Joint Direct Attack Munition) and GPS-guided, terrain-following systems like the Tomahawk. But the U.S. is no longer the only country with precision weaponry. In fact, Russia, China and countries purchasing defense equipment from them now have access to these Second Offset technologies.

With sources of comparable technology growing elsewhere in the world, such as the anti-ship Brahmos hypersonic cruise missile developed by Russia and funded by India, the U.S. needs to pivot to new technologies. In this context, Deputy Secretary Work's Third Offset push, with its focus on rapid prototyping and AI, is particularly relevant.

If autonomous systems are to be a pillar of future supremacy, then now is the right time to present a framework within which autonomy can be enabled in an effective and technically viable, yet legal and moral, manner.

THE IMPORTANCE OF MORALITY IN AUTONOMOUS TECHNOLOGY

To understand how the question of morality relates to autonomous technology, one only has to read through the many articles questioning the use of weapons that decide on their own targets. The questions range from the legality of this practice to fear of a Terminator-inspired "Skynet." In truth, the discussion regarding "moral" autonomous action is not academic—it's critical.

"WITH SOURCES OF COMPARABLE TECHNOLOGY GROWING ELSEWHERE IN THE WORLD, SUCH AS THE ANTI-SHIP BRAHMOS HYPERSONIC CRUISE MISSILE DEVELOPED BY RUSSIA AND FUNDED BY INDIA, THE U.S. NEEDS TO PIVOT TO NEW TECHNOLOGIES. IN THIS CONTEXT, DEPUTY SECRETARY WORK'S THIRD OFFSET PUSH, WITH ITS FOCUS ON RAPID PROTOTYPING AND AI, IS PARTICULARLY RELEVANT."

Since the prospect of full machine autonomy—overall range of action, including deadly response—is disconcerting to many, public debate on this topic is infused with softeners. These are comforting terms like "semi-autonomous" and "human in the loop." However, these represent an easy out while also being misleading. They masquerade as answers when they don't even begin to address the question.

Effective machine functionality in a variety of situations requires full autonomy, and a wink and a nod to a "man in the loop" is actually detrimental to properly confronting and addressing this need. For example, how do we expect a swarm of autonomous undersea vehicles to act when they have a critical target in sight but realize that communications are being jammed? Do they let the threat materialize since they can't contact their human commanders? Or do they take autonomous action for our protection?

FULL AUTONOMY IS IMPORTANT, BUT NEEDS TO BE EXPLAINABLE

With all of these complications, why even go down the path of full autonomy? The answer is simple: military superiority and survivability. Autonomy grants an edge. The full potential of autonomous systems cannot be realized if there are humans in the loop for all key decisions.

The First Offset was about massive firepower delivered bluntly and coordinated over a modest window of time. The Second Offset was about modest firepower, delivered with precision and coordinated over a longer window of time. The Third Offset will be about micro firepower, delivered at unimaginable scale with immense precision on the actual target, and coordinated over a minute window of time. It will be about instantaneous, massive, surgically precise strikes. However, without full-spectrum autonomy, you lose several of these attributes. Are we sure that our competitors will compromise on these to remain in control of their own AI systems?

THE FIRST OFFSET WAS ABOUT MASSIVE FIREPOWER DELIVERED BLUNTLY AND COORDINATED OVER A MODEST WINDOW OF TIME. THE SECOND OFFSET WAS ABOUT MODEST FIREPOWER, DELIVERED WITH PRECISION AND COORDINATED OVER A LONGER WINDOW OF TIME. THE THIRD OFFSET WILL BE ABOUT MICRO FIREPOWER, DELIVERED AT UNIMAGINABLE SCALE WITH IMMENSE PRECISION ON THE ACTUAL TARGET, AND COORDINATED OVER A MINUTE WINDOW OF TIME.

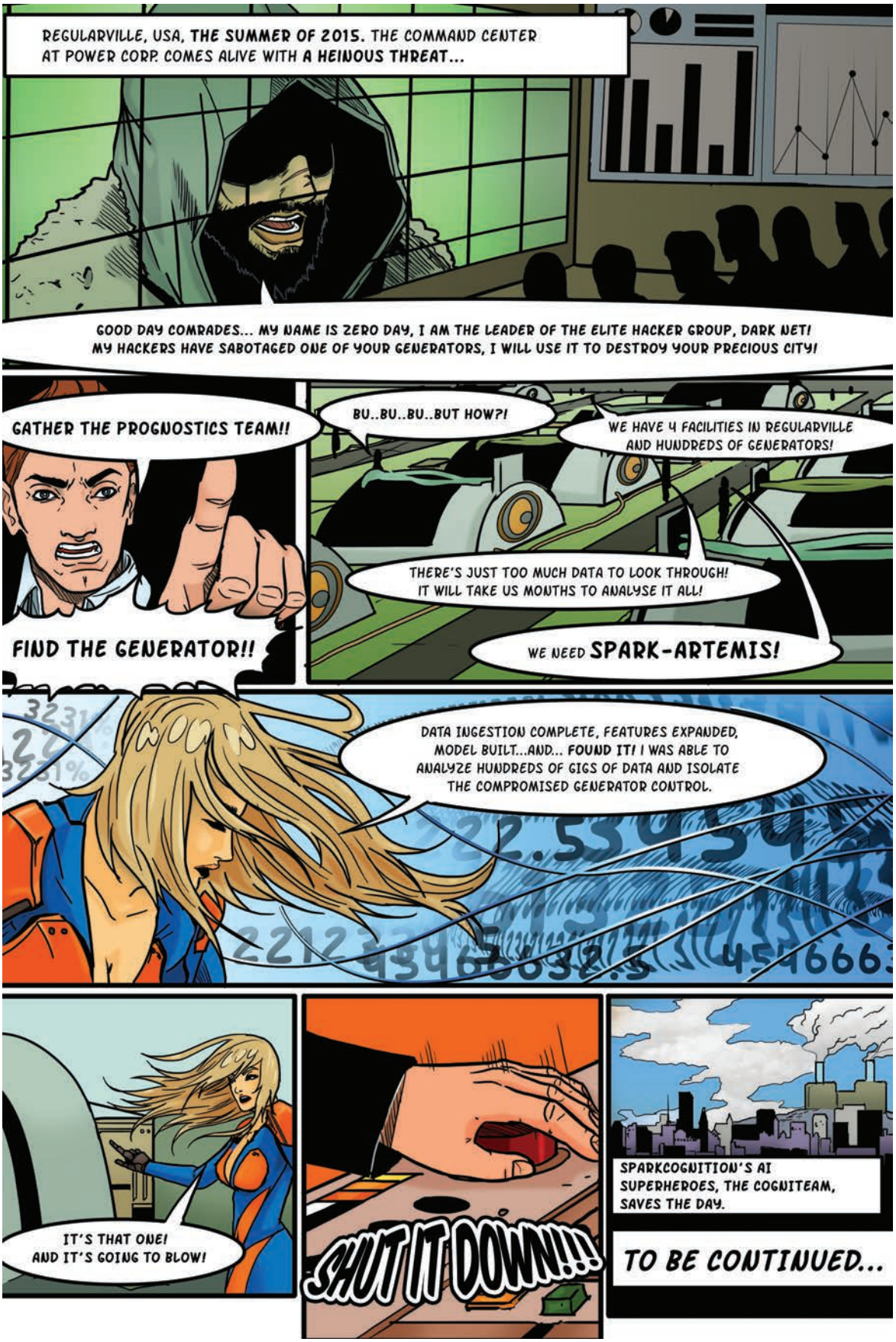
That said, it's important to make autonomous decision-making as transparent as possible, particularly in these cases. AI systems that have succeeded in today's commercial world don't make this easy. Artificial Neural Networks (ANNs), Deep Learning and other approaches that leverage vast networks of statistical weights learn patterns and behaviors that are inherently uncheckable. Much like how an autopsy on a biological brain does not reveal the memories or experiences of the individual, taking a digital "scalpel" to a neural network reveals nothing but arrays of millions of numbers, none of which have a human-interpretable label or any clue regarding what behavior or feature the numbers represent.

In order to improve behaviors, societies or systems, one must get to the root of the cause. Even ancient criminal law prescribed different outcomes for the same action given a different motivation: hang him if he killed in anger, but let him go if he killed in self-defense. Many successful AI techniques lack this level of transparency or explainability. They propose a decision, but cannot fully explain why it's the right decision or what their "motivation" was.

Policy and defense experts, such as P.W. Singer, are raising important questions about building a framework for moral use before militaries start using these systems. My own company, through natural language generation and algorithmic ensembling, is working on related explanations for why something is a threat. We, as technologists and military strategists, must understand why a system proposes to do what it does, so that we may optimize and improve it. As AI capabilities rapidly head in a direction where autonomous systems can make life and death decisions, it is time to demand explainability and accountability from the digital brains we are building.

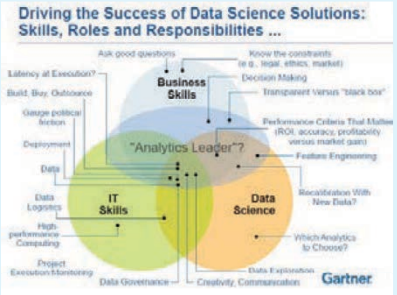
SC COMICS

THE COGNITEAM



SparkCognition 8:25 AM - 5 Jan 2017
@SparkCognition

A study of #IoT buying plans by analysts at @451Research shows robust growth ahead during 2017. http://www.computerweekly . . .



Ronald van Loon 2:03 PM—5 Jan 2017
@Ronald_vanLoon

Difference between Machine Learning, Data Science, AI, Deep Learning, and Statistics | #Data-Science #Statistics #RT http://bit.ly/2j6qBta

Nornir-insight 10:55 AM - 4 Jan 2017
@NornirInsight

40 Key Emerging Technologies to be Driving 2017 [Infographic] #AI #IoT #Robotics #Cloud #BigData #Analytics #SmartCity

Ronald van Loon 2:03 PM - 5 Jan 2017
@Ronald_vanLoon

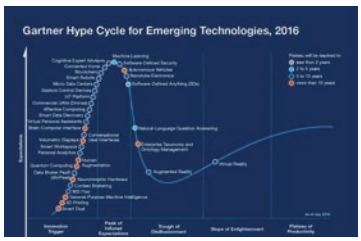
10 Emerging Technologies That Will Drive The Next Economy | #BigData #Artificialintelligence #RT http://bit.ly/2d7TyWH

BIRDonCLOUD 2:40 AM - 6 Jan 2017
@birdoncloud

Emerging Technologies Like Advanced #Analytics #MachineLearning and #IoT Help Revolutionize Public Sector Agencies

Digital McKinsey 8:41 AM - 13 Jul 2016
@DigitalMcKinsey

Looking back at: Unlocking the potential of the Internet of Things



Casino Analytics
@CCC_Analytics 10:05 PM - 27 Dec 2016

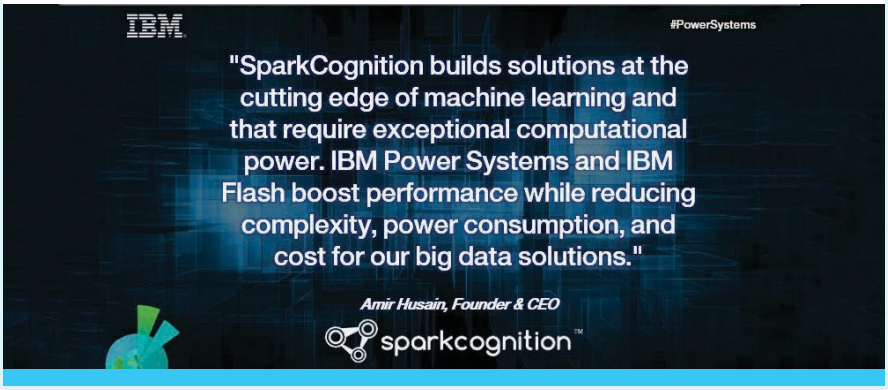
Ronald_vanLoon: RT Ronald_vanLoon: 30 Emerging Technologies You Need to Know About | #Artificialintelligence #IoT …

Evan Kirstel 7:30 AM - 6 Jan 2017
@evankirstel

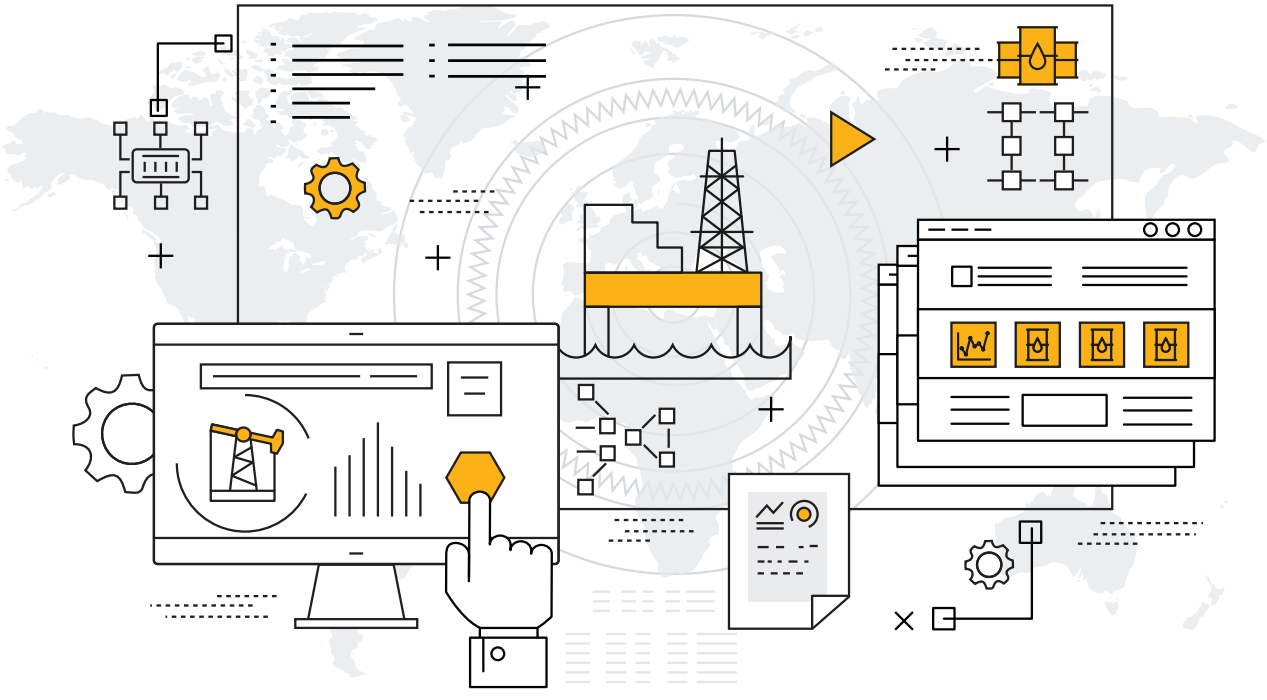
Most manufacturers will use customer-facing #VR by 2020 by @clareellenmcd http://www.computer-weekly.com/news/

IBM Systems ISVs 7:01 AM - 8 Dec 2016
@IBMSystemsISVs

#POWER8 & #IBM #FlashSystem reduces cost & complexity for @SparkCognition—read it here https://ibm.biz/Bdre47



A.I. IN SOCIAL MEDIA



A.I. FOR OIL & GAS: IS IT TIME TO INVEST?

With A.I., costly problems identified by traditional monitoring and security can be solved before they even happen.

by **Philippe Herve, VP of Solutions at SparkCognition**

When I first heard of predictive analytics, machine learning, and cognitive security, I was skeptical. I am an engineer at heart and condition-based maintenance was the only way, I thought, to effectively look at predictive maintenance. You start with the physical asset, you deploy sensors to monitor critical components, and you analyze the data. The thing is, this approach is expensive and time-consuming. Sensors need to be deployed and installed on existing equipment, software to collect, store, and process the data needs to be integrated, O&M teams need to be trained on the technology, and the software needs to be constantly updated.

With the help of complex algorithms, predictive analytics and machine learning allow decisions to be made automatically, while data analytics provide a systematic way to make sense of the large volumes of data being collected across the entire oil and gas value chain. This can help predict when an asset will fail, or ensure that resources and personnel are in place where needed. Whereas predictive analytics will ensure O&M efficiency and optimization, cognitive security is designed to monitor and protect the IT network, making a cognitive suite like that of SparkCognition a true cyber-physical solution, protecting both the IT infrastructure as well as the OT network.

With the unparalleled optimization and increased safety that predictive analytics and machine learning provide, asset monitoring and analytics have never been more important for the industry. When a top drive starts, stops, or fails, there are repercussions on the generators in the engine room. When the shale shaker's state is changing, the mud pumps are affected. Often, the entire data set on the rig is full of cross talk between the different assets. Oil and gas companies are increasingly having problems learning from data to understand the different operational states and failure modes of critical assets. The sophistication of cyberattacks in the IoT environment is making it more and more difficult for traditional security systems and teams to differentiate between natural machine failure and equipment sabotage. It is clear that the industry status quo of condition-based monitoring and traditional security solutions is outdated, and is quickly becoming more expensive and less effective.

Let's take the case of a drilling rig and assume there are performance issues in the drilling process. The O&G sector has become very susceptible to cyberattacks and the assumption that performance is a mechanical issue is no longer a given. We must now ask whether we have a problem because the rig has been compromised by a cyber threat—is the top drive under the control of hackers? Do we have a maintenance issue and the mud pump is starting to fail? Or do we have a true drilling dysfunction that needs to be mitigated with a change of the drilling set points? With predictive analytics and cognitive security, you can protect the rig from cyber attacks and be sure the equipment is operating safely and securely, per specifications.

"WITH THE HELP OF COMPLEX ALGORITHMS, PREDICTIVE ANALYTICS AND MACHINE LEARNING ALLOW DECISIONS TO BE MADE AUTOMATICALLY, WHILE DATA ANALYTICS PROVIDE A SYSTEMATIC WAY TO MAKE SENSE OF THE LARGE VOLUMES OF DATA BEING COLLECTED ACROSS THE ENTIRE OIL AND GAS VALUE CHAIN."

By leveraging patented cognitive technology and utilizing data already available, SparkCognition, a leading provider of AI-powered cognitive analytics, is able to predict failure and provide advanced warning before a critical asset incident occurs, so operators can plan for corrective actions. By providing answers to a large percentage of the questions surrounding the remaining life of each particular asset or component, cognitive technologies are equipping O&M and security teams with the means to optimize human

resources, equipment inventories, and budgets.

Today, there are vast amounts of data which are unused or incompletely used. With patented technology, we remove the clutter that exists in this data and extract the hidden value. This can only be achieved with cognitive analytics and security. Using machine learning, we are deploying implementations where our system is as good as a handful of outstanding experts in the field at predicting upcoming failure. From there on, the more you use the system, the better it gets. The future is augmented intelligence, and the future has arrived.

The London Stock Exchange is using our platform to detect fraudulent activity in finance. Flowserve, the largest manufacturer of pumps for the oil and gas industry, is using our software for predictive maintenance. The second largest U.S. utility is using our technology to improve the efficiency and reliability of their most expensive spinning assets. Generally speaking, predictive analytics is a fast-growing industry, but the oil and gas sector has been timid in adopting the approach and realizing its benefits.

The biggest barrier to the use of predictive maintenance in drilling is related to the limitations of traditional approaches. Under the constraints of machine learning, you typically need 15 failures as part of the training process of the model that will be used when the technology is deployed. In the oil and gas industry, we typically don't have this number of failures available, as we tend to perform a lot of preventive maintenance (at a very high cost) to ensure equipment does not fail. Also, when a failure does occur, we tend to replace a lot of components, sometimes without understanding which specific components failed first and why, much less understanding the failure correlation between those components. With an automated model building approach provided by our patented algorithms, we find trends in data with a very limited amount of failures. In fact, we have built reliable models in situations where we had no failures available to train the model.

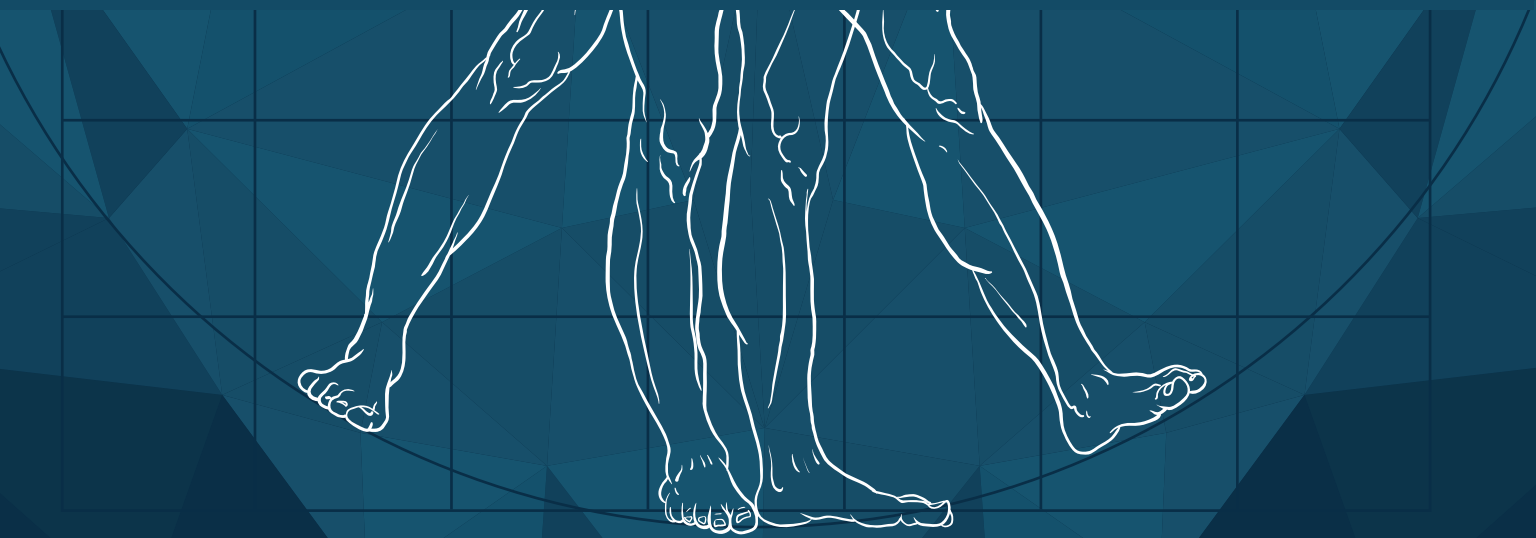
For as long as I have been in the oil and gas industry, I have heard the term "Artificial Intelligence." Twenty years ago, the most advanced Artificial Intelligence was able to state, 'six months ago, you could maybe, possibly have avoided failure with some sort of preventative maintenance.' Ten years ago, Artificial Intelligence was telling us, 'six months ago, you should have taken a specific preventative action.' Today, with the advances in Artificial Intelligence-powered software, and sensor hardware, we are now able to look at very large amounts of data and give real-time responses on the best future course of action.

Artificial Intelligence is taking the industry by storm. With predictive analytics and cognitive security, you can be sure that your equipment is operating safely and securely, per your specifications, and also receive recommendations on action to take to avoid future equipment failure or remediate a security breach.

The measurable value of predictive analytics comes from a significant reduction in the operating cost, while the biggest savings are in the increased safety brought to both personnel and equipment. Today, the use of predictive analytics is improving the operations of the O&G industry's early adopters. Using AI for drilling optimization and integration to other corporate applications and corporate knowledge is starting to be explored. With additional AI techniques, such as Natural Language Processing, one can query maintenance manuals to instantly obtain a maintenance procedure for a specific asset under question.

The promise of AI is already starting to be realized in the O&G industry. Early adopters are taking advantage of their position on the technological adoption curve to get a head start on the competition and to keep their assets safe. The industry has always leveraged technology to adapt to change, and the early adopters have always benefitted the most. As the oil and gas industry continues to be more and more competitive, companies cannot afford to be left behind. However, if companies can understand the opportunities inherent in adopting cognitive technologies, their future surely looks bright.

HUMAN INTELLIGENCE @ MACHINE SCALE



sparkcognition™

www.sparkcognition.com

@SparkCognition

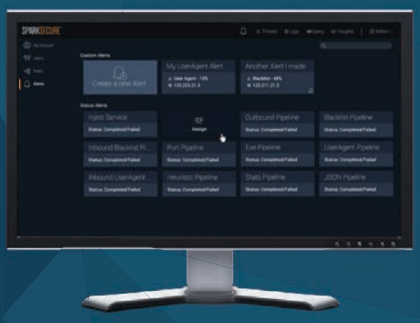
SPARKPREDICT®

Physical Asset Failure Detection/Prediction

- Builds asset models automatically
- IDs anomalies and predicts impending failures
- Incorporates domain expert input for supervised learning (optional)
- Delivers advanced data cleansing and verification
- Applies IBM Watson to deliver in-context advisory

SPARKSECURE®

Cloud Security Threat Intel & Advisory



- Identifies threats and anomalies
- Automatically develops signatures to block threats
- Aggregates knowledge in a Graph Database
- Uses dynamic NLP for automated threat research
- Applies IBM Watson to deliver in-context advisory

DEEPARMOR®

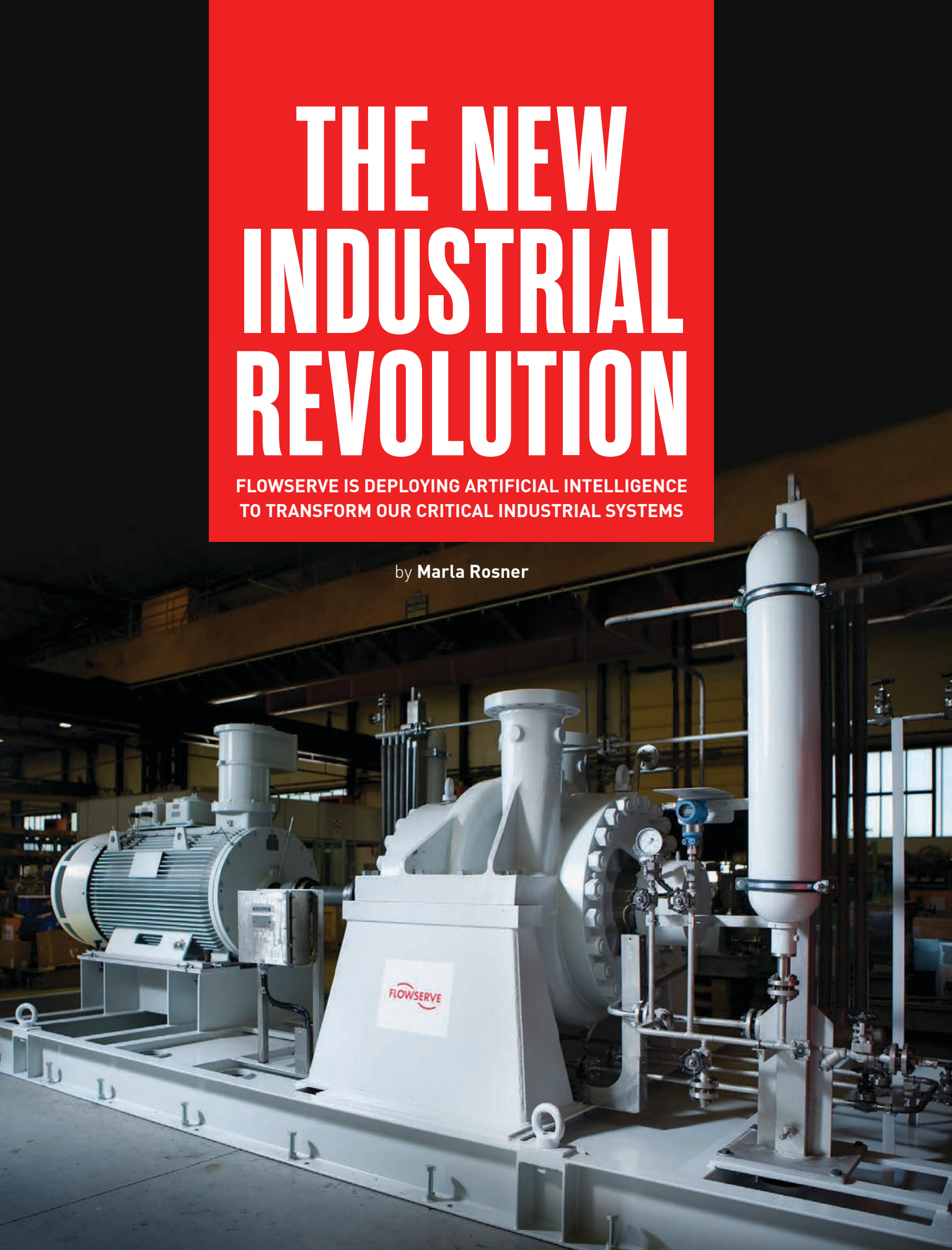
Cloud Security Threat Intel & Advisory

- Analyzes the DNA of files to ID threats
- Sub-second malware detection
- Signature-free security
- Self-learns and retains knowledge
- Combines structured and unstructured data (including NLP) to research threats
- Reduces false alerts

THE NEW INDUSTRIAL REVOLUTION

FLOWSERVE IS DEPLOYING ARTIFICIAL INTELLIGENCE TO TRANSFORM OUR CRITICAL INDUSTRIAL SYSTEMS

by **Marla Rosner**



George Washington gave the very first State of the Union address in 1790. That same year, as a nation was being born, Thomas Simpson, a civil engineer living an ocean away in London, founded a pump and steam engine workshop and named it Simpson & Thompson. While most of what we know from 1790 is relegated to history books, museum exhibits, and plaster replicas, Simpson & Thompson can today be found in its latest incarnation as Flowserve.

Flowserve has certainly had a long life, and it's done so by a tradition of constant innovation and reinvention. Throughout their exceptionally long past, Flowserve's products have always been "things of the future." We often associate innovation with tools such as the printing press, the factory line, the Internet, mobile devices, and wearable technology. But pumps? What could possibly be so exciting and innovative about pumps? The truth is, pumps are what keeps the lights on and the water flowing. The type of machinery that Flowserve manufactures is the central organ—the heart if you will—of society's most critical civil services. From energy production to water utilities, Flowserve's equipment keeps our most vital societal functions operating. And the manufacturing of this critical machinery started over 220 years ago.

Just a few years before founding his company, Simpson invented the first bell and spigot joint, a new method for making the relatively new iron water pipes watertight at socket joints. This may not seem like a big deal, but it was this type of technology that enabled modern plumbing. The bell and spigot joint would remain the primary pipe joint used across the world for 170 years, all the way until 1956. Simpson & Thompson also pioneered the use of air vessels in water towers, marking a shift from pumping water from cisterns at the top of water towers to the more efficient models we use today. In 1828, they built the first slow sand filter bed, a method of water purification that gave rise to the first treated public water supply in the world. In the 1840s, they invented the double-acting beam rotative compound engine, a more efficient and powerful steam engine that helped drive further modernization in the Industrial Age.

Most of these technologies are no longer in use today, and mean little to nothing to the modern reader. But they were critical innovations that formed the building blocks of modern society and all of its trappings we rely on, from clean water to powerful motors. They and many other such inventions allowed the company Simpson founded to grow and flourish, spreading its influence further with international mergers that eventually resulted in the Texas-based Flowserve, almost 230 years later. That tradition of pioneering at the technological cutting edge has shown no sign of stopping.

In addition to building the industry's top hardware, today Flowserve's innovation is found in the intelligence of the software running their equipment—predictive maintenance powered by artificial intelligence.

THE PROBLEM OF PREDICTIVE MAINTENANCE

Flowserve's bread and butter is designing, developing, manufacturing, and repairing precision-engineered flow control equipment for their customers' critical processes. This includes pumps, valves, seals, and support systems, mostly intended for use by some of the world's largest companies in oil and gas, power, chemical, water, and other critical industries. Even now, they're continuing to explore ways to push the industry and its technology forward.

No one is more aware of this than Eric van Gemeren. As Vice President of Flowserve's Product Management and R&D, van Gemeren is responsible for generating new growth opportunities and driving innovative practices across the product portfolio, new product introduction, product cost reduction, and has overall accountability for managing Flowserve's global portfolio of investments in emerging technologies.

van Gemeren is no stranger to any of these roles. A registered professional engineer with a Bachelor's degree in Mechanical Engineering and a Master's in Systems Engineering, van Gemeren has been developing and leading high-performance teams in high-tech organizations for more than 25 years. He has held positions ranging from military service and management consulting, to executive leadership in a multi-national organization. Throughout all this, he says, his passion has always been in driving growth through product and service innovation, helping to transform old-economy business models. In this respect, Flowserve is a standout.

"What's amazing to me is the creativity with which our customers and engineers are thinking about new ways to apply technology to better understand and continuously improve their operations," he says. "I've seen instances where some of our latest solutions can combine vibration, pressure, fluid, and thermal signatures to understand more of what's happening inside the pump or the flow system—and provide that data to a user in almost real time so they can take action quickly."

The latest frontier for van Gemeren and Flowserve is to expand even further on these aftermarket services—specifically, by selling assets that are packaged with intelligent software, such as machine learning solutions, to determine asset health and predict impending failures.

Predictive maintenance is something Flowserve has been working on for a very long time. The ability to predict asset failures before they occur is invaluable in the industries

THE GOAL IS ALWAYS TO LOWER OPERATING COSTS, REDUCE UNPLANNED DOWNTIME, AND IMPROVE RELIABILITY AND SAFETY—AND FLOWSERVE'S CUSTOMER BASE SEES TECHNOLOGY AS THE WAY TO ACHIEVE THIS.

Flowserve serves, as it can massively reduce operating and maintenance costs as well as unscheduled asset downtime. This translates to more operational efficiency.

van Gemeren sees this as a crucial part of Flowserve's evolving business model. "Flowserve is unique in that we not only are a long-standing OEM and service provider of leading edge flow control technology, but we also now have the ability to detect, diagnose, and then of course repair or even upgrade our customers' flow equipment," he says. "We've been providing solutions for remotely monitoring and diagnosing pumps, valves, seals, and actuators in our industry for many years—and we are continuing to invest in this space." Having a broad services capability—Flowserve maintains over 200 service centers globally—is a critical element in the equation.

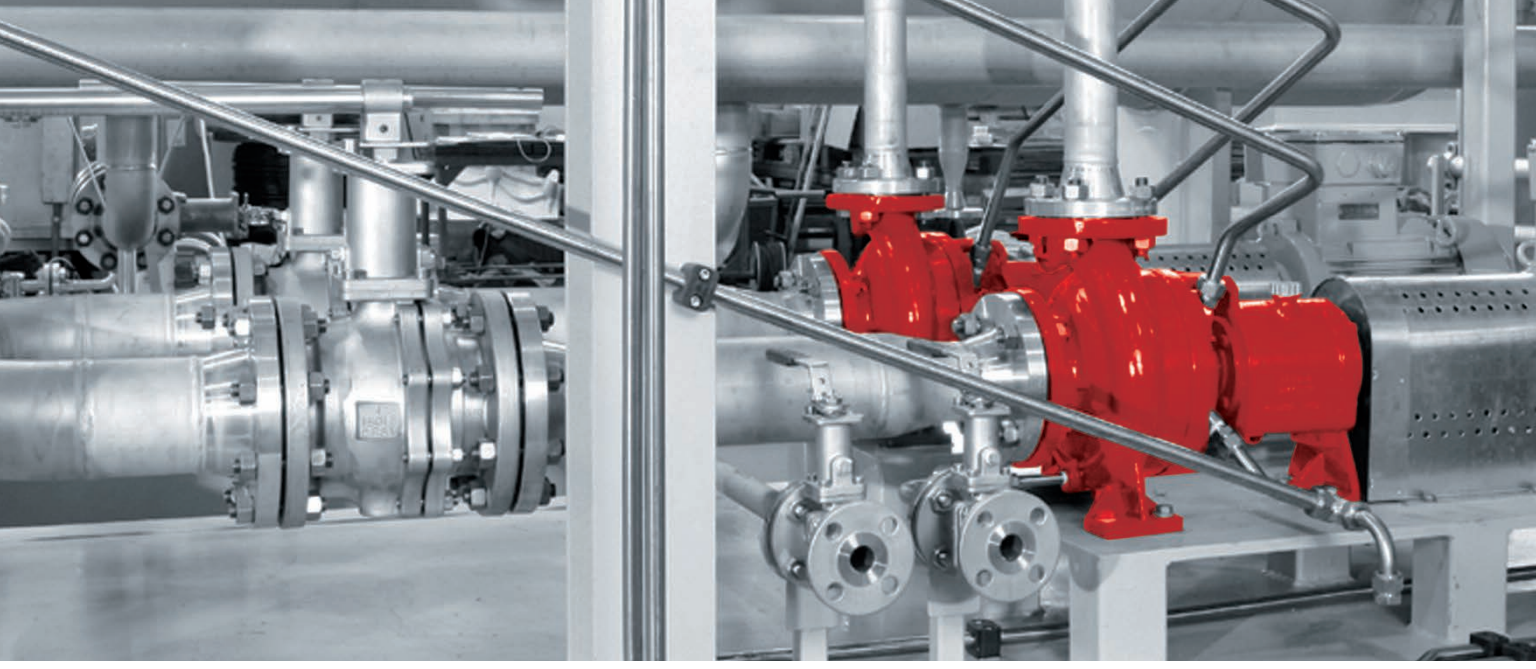
Generally speaking, predictive maintenance is approached by using models. A model is best thought of as a mathematical function, such as f(x)=y. The input for the model, or the x in the function, is sensor data from various assets, such as temperature and pressure. The output of the model—the y value—then creates the desired insights on how the assets are operating or if they're close to failure.

In the past, Flowserve and other similar companies have approached this challenge with physics-based modeling. This kind of pump monitoring involved measuring predetermined thresholds of vibration and temperature and sending alerts whenever these measurements exceeded a specified level. This methodology has worked well for years, and provides operators with immediate condition-based information. However, it stops somewhat short in that the information is generally minimal or incomplete. This pump is running hotter than expected, or this asset is vibrating beyond its specified limits. But it couldn't tell the operator why this might be happening.

"Individuating" a root cause is what Flowserve is working on, and is what will tell the plant engineer the root cause of the pending failure. Perhaps the shaft is no longer aligned, or the bearings are wearing out, or there is blockage in the line somewhere upstream of the pump. This is extremely valuable to know, and will tell the operations team where to look, and when they might expect an asset to fail in these conditions.

It was clear that a better solution would be needed. According to van Gemeren, Flowserve's customers wanted to augment better information with what their engineering, operations, and maintenance teams already do, so they could optimize operations. The goal is always to lower operating costs, reduce unplanned downtime, and improve reliability and safety—and Flowserve's customer base sees technology as the way to achieve this.

As for what van Gemeren himself wants? "I tend to think about this more from the standpoint of expanding the envelope of information readily available to the customer to improve performance and to make better decisions. Today, that window is pretty small for some equipment or systems, and it may not be all that clear. We are working to push the



boundaries of that envelope, and make it more transparent, so that the customer can truly see what is happening in near-real time to his equipment—and then act upon it. First is knowing, then taking action with that data."

The best way to accomplish all this has been years in the making. Building on known methods, using increased data collection and cloud computing, Flowserve is now adding more advanced modeling and machine learning to the mix.

With the same nose for cutting-edge innovation that has carried them through for centuries, Flowserve had been keeping an eye on machine learning as a possible solution for almost two decades. In the 1990s, machine learning was experiencing a new renaissance, as scientists shifted their focus from previous rules-and knowledge-based approaches to a more flexible data-driven approach, feeding programs large amounts of data to permit those programs to learn from the data in an organic fashion. This meant that machine learning could feasibly be applied to a model for predictive maintenance. It could be fed sensor data as the input, analyze that data, and produce maintenance information as the output—in theory. In practice, the growing technology just wasn't ready for such an application, since it was too expensive and difficult to implement.

This has all finally changed in the past few years, however, as advances both in data science and in raw computing power have finally allowed machine learning to start to reach its full potential. van Gemeren also cites the drop in hardware costs and computing costs as having allowed businesses to deploy broader and deeper computing solutions than ever before at a lower cost profile to their customers. "No longer is this a thing of the future," he says. "The tools are now becoming much more usable by engineers and practitioners who don't necessarily need a PhD in science to fully interpret the results. We are making it easier to know more about what is happening with the asset, act upon that information, optimize the system, and even predict what might happen next."

In response, the technology landscape has been undergoing massive shifts, as the newly augmented machine learning takes its place exactly where businesses like Flowserve long believed it would eventually be—poised at the forefront of a technological revolution.

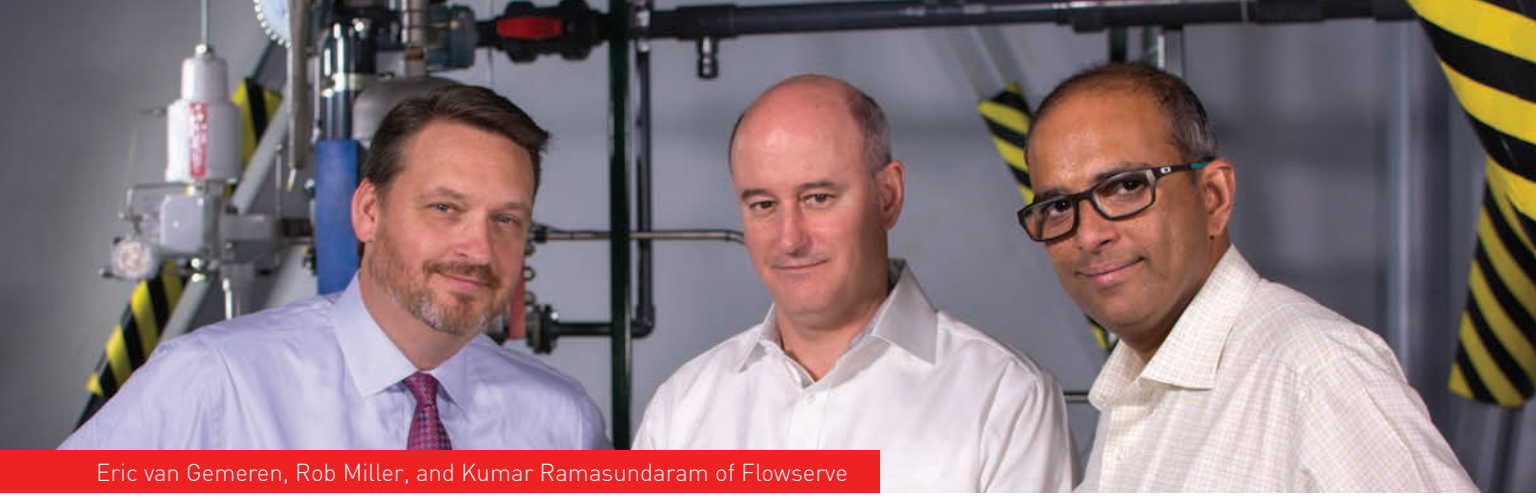
Flowserve wanted to take better advantage of these growing capabilities, and found part of their solution in SparkCognition's artificial intelligence technologies. In this sense, Flowserve did not have to hire their own data scientists or build a large support team, but could move quickly into this space with confidence.

INTEGRATING A.I.

It was in 2014 that Flowserve first partnered with SparkCognition, an Austin-based A.I. company.

Providing deep analytics and actionable insight via machine learning was the logical next step for Flowserve. "But we cannot do it alone," van Gemeren says in explaining how the partnership with SparkCognition came to be. "Great partners are fast, flexible, and bring a unique capability to the final solution. SparkCognition is great at drawing conclusions using disparate data sources, and is ideal for layering on top of other more traditional analytics capabilities that we have and continue to develop. Partners can also bring a different perspective, and SparkCognition has been great at bringing new ideas and technology, like natural language processing, to the forefront of what is possible. This capability, added to Flowserve expertise in pumps, flow equipment, and service looks to be a potent combination of talent.

Unlike the rules-based models Flowserve had previously employed, the machine learning models that SparkCognition developed for Flowserve rely on hypothesis generation based on near-real time data streams and trained on historical sensor data. By leveraging data in this way, machine learning can combine human insight and experience with a machine's speed, scalability, and lack of bias, to create models of unprecedented accuracy and sophistication.



Eric van Gemeren, Rob Miller, and Kumar Ramasundaram of Flowserve

The results are perhaps the best way to illustrate this point: SparkCognition's machine learning model allowed Flowserve to give their clients significant forewarning before a failure, an increase of as much twenty times in early testing. Models are also showing false positive rates of less than two percent in early testing, meaning that the models accurately tell the user exactly what will happen 98% of the time, helping the customers individuate true root causes, beyond traditional sensor capabilities. The next step is testing this methodology with several pilots now being deployed in the field.

"And partnerships work both ways, of course. We think partners mutually support each other, and Flowserve can bring a long history of over 200 years in an industry that brings both credibility and deep intellectual property to the relationship."

SparkCognition has also worked with Flowserve on projects that can detect the current operating state of a pump based on a relatively small number of sensor inputs, such as pressure or vibration. Using this cognitive solution, Flowserve is able to effectively identify whether a pump is operating in the right state, if there's a problem with the pump, what kind of problem there may be with the pump, and if it is a problem that has been encountered before. This is a wide range of highly valuable data, and being able to output all of it based on such a constrained data set is not only a technological achievement, but also is part of what makes this model both efficient and scalable. The scalability of this machine learning solution means these analyses can be performed not just at the pump unit level, but at the fleet level as well. This allows Flowserve to monitor large numbers of pumps as well as helping their customers gauge the efficiency of an entire operation.

All in all, Flowserve now has the ability to create dynamic models of pumps under a wide variety of operating conditions, while using multi-dimensional analysis to provide early asset failure warnings. Not only that, but Flowserve is now able to identify the factors responsible for a failure, making it easier to repair assets and avoid future failures.

van Gemeren is excited about these results, and what they mean for the future of Flowserve. He believes that this is a significant expansion in both the depth and breadth of diagnostics Flowserve can perform on running machinery, and one that also improves the predictive power of those analytics. "Together, these advances increase the return on investment our customers get from these solutions," he says. He doesn't plan on stopping there, either. His next goal is working to make internal use of SparkCognition's natural language processing (NLP) capabilities. NLP is software that can learn written and spoken language in much the same way as a human. With this capability, SparkCognition has developed solutions to understand, analyze, and use what is known as "unstructured data"—data in a format such as natural language that would normally be impossible for a machine to understand. Flowserve's next project with SparkCognition is to feed this NLP technology a corpus of technical documentation—data sheets, troubleshooting guides, electrical diagrams, and so on—in order to create a database in which their technicians can quickly and easily find relevant documentation for whatever they're working on.

Even this, van Gemeren believes, is only the beginning. "Today, we are working more closely than ever with our customers to continuously evaluate and evolve our technology to remain at the forefront of what's happening in this space," he says. "In the longer term, we see a more connected, more predictive operating environment for our customers where the combination of rapidly advancing AI technology, coupled with the reduced cost of gathering and analyzing data, allows plant owners and operators to instrument not only the 'critical few,' but also the 'important many' pieces of equipment that are key to their day-to-day operations.

"There will always be new challenges and new technologies to apply to help improve reliability and performance," he adds. It's a perfect summation, it seems, of both van Gemeren and Flowserve's approach to just about anything they do.

Flowserve may not look or sound much like the workshop of Simpson & Thompson from 1790, but the world at large doesn't look much like it did in 1790, either. The ability to change, grow, and invent along with the world around them is what has allowed Flowserve to survive for almost two and a half centuries, and it's what will keep them going in the years to come. No matter how much technology changes, there will always be a need for companies that innovate. The only way not to become a thing of the past is to always keep an eye on the future.

THE AI 100

2017

A global leader and highly awarded cognitive computing analytics company, SparkCognition is successfully deploying cutting-edge Machine Learning and AI algorithms to provide intelligence to uncover trends, anomalies, and cyber-physical threats while automatically investigating and proposing solutions in IoT and network environments.

CBINSIGHTS

2017 A.I. & IoT LANDSCAPE

DATA SCIENCE

- sparkcognition
- CONTINUUM ANALYTICS
- Alpine DATA LABS
- ALGORITHMIA
- dataiku
- DataRobot
- context relevant
- DOMINO
- ŷhat
- bigml

MACHINE LEARNING

- sparkcognition
- H_2O.ai
- skymind
- context relevant
- AYASDI
- SCALED INFERENCE
- rapidminer
- deepsense.io BIG DATA SCIENCE
- narralogics
- Windows Azure

ANALYTICS

- sparkcognition
- IBM Watson™
- PREDIX
- UPTAKE
- KONUX
- C3 IoT
- Alation
- MOTIVA
- thingworx
- ARIMO

AUTONOMOUS SYSTEMS

- Google
- TESLA
- UBER
- MOBILEYE
- SKYCATCH
- SKYDIO
- JAYBRIDGE ROBOTICS
- DroneDeploy
- OSARO
- fetch robotics

IOT INFRASTRUCTURE & HARDWARE

- nervana SYSTEMS
- NVIDIA
- QUALCOMM
- Movidius
- Cirrascale
- tensilica
- SILICON LABS
- GainSpan
- TEXAS INSTRUMENTS
- SEMTECH

NATURAL LANGUAGE PROCESSING

- sparkcognition
- semanticmachines
- agolo
- LUMINOSO
- AYLIEN
- Cycorp
- LEXALYTICS
- spaCy
- loop ai Labs
- narralogics

CANCELLING FLIGHT DELAYS: PREDICTING THE FUTURE OF AIRCRAFT MAINTENANCE

by **Caroline Lee**

Not long ago, on a Sunday night like any other, I found myself waiting in a terminal at the Charlotte airport for a connecting flight. As most 21st century travelers have come to expect, the boarding process didn't begin on time—but as most of us dreaded—our momentarily postponed boarding queue turned into two hours of maintenance on an unspecified piece of equipment. We finally took off as midnight rolled us over into the next day, and arrived at our final destination safe, but exhausted.

At face value, maintenance seems to be the most forgivable reason for a delay. FAA regulations mandate that even the simplest repairs must be made before a plane leaves the ground: if a latch on an overhead bin were to remain broken for the next flight, the airline could potentially be responsible for a serious injury to a flyer from an airborne piece of luggage. However, as forgiving as flyers may choose to be when faced with maintenance delays, the fact remains that delays make no one's day. Unfortunately, maintenance can prove quite an extensive endeavor: in fact, data from MasFlight indicates that about one-third of flight delays and cancellations are maintenance-related .

But what specifically happens during maintenance to prolong the process so much? According to one helicopter pilot and former flight quality assurance specialist, a "maintenance delay" can look like this:

1. *A problem is identified by a pilot or line maintenance crew doing a pre- or post- flight inspection, or was identified during the flight.*

2. *The maintenance procedure manual is referenced for a solution to the problem.*

3. *The maintenance technician collects all the tools and equipment needed to fix the problem, which are listed in the procedure. Lots of special tools, diagnostic equipment, and parts are needed for aircraft maintenance. They are often expensive, and sometimes hard to find.*

4. *The technician fixes the problem.*

5. *The technician accounts for all tools.*

6. *The technician records the completed procedure in the aircraft's maintenance logbook.*

7. *The technician locates the quality assurance specialist.*

8. *The quality assurance (QA) specialist checks the technician's work. The FAA requires this check.*

9. *When certain components are replaced, they require checks to be completed by the maintenance technician or pilot to ensure the new component is installed and working properly. These checks are discerned and completed as needed.*

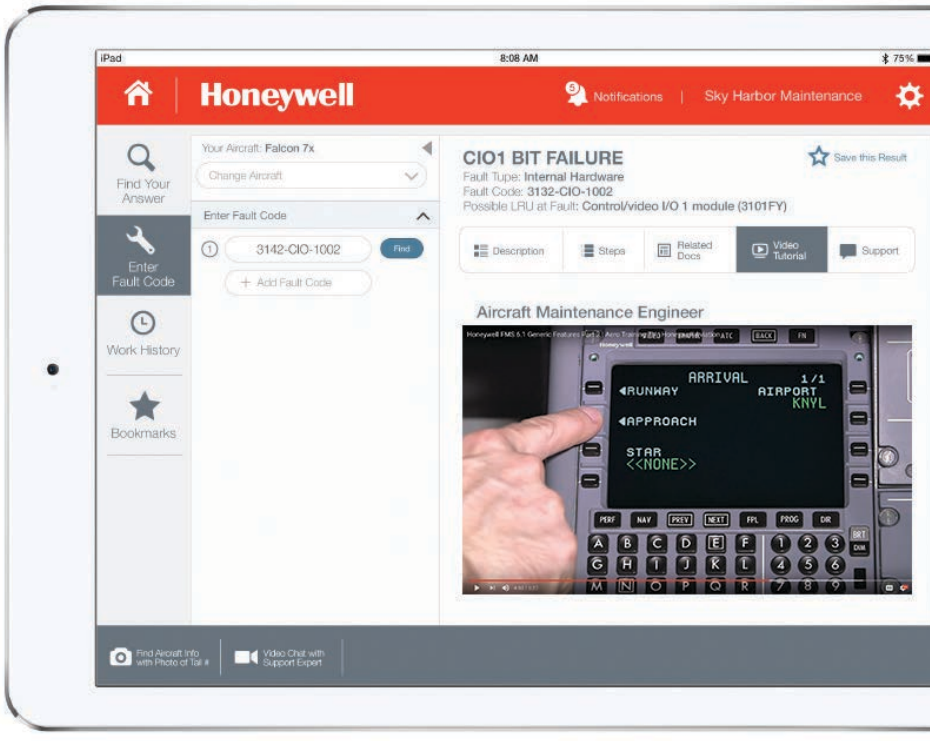
10. *After these checks are completed and the aircraft is deemed ready, the QA specialist indicates completion in the aircraft logbook.*

One of the earliest steps in this process may appear the most unassuming. Checking a procedure manual, to an average passenger, ostensibly seems like it would take the least time and effort. However, locating a specific solution to repair a given part can prove an arduous process. Before aircraft maintenance manuals were digitized in 2000, printed binders were extremely difficult to sift through. A telling example involves the Boeing 777; according to the Boeing website, the printed version of the primary Aircraft Maintenance Manual for the 777 "takes up 24 binders and requires 10 feet of shelf space." Since digitizing all manuals, this process has been expedited to an extent, but still remains complicated.

"Last year alone, Boeing distributed enough maintenance documents to create a stack of paper more than 24 miles (38 km) high and a stack of microfilm cartridges more than 14 miles (22 km) high."

Furthermore, as planes in an airline's fleet age, the likelihood and urgency of repairs increases accordingly. Pilots know better than anyone that aircraft parts must be replaced rather predictably after a certain number of flight hours or by a certain date. But this does not account for parts expiring or wearing out before their documented date, which occurs sporadically. The issue of maintenance delays thus exists as a dilemma of both inconvenient categorization and an incapacity to predict the future. In each case, what's a maintenance engineer to

SPARKCOGNITION HAS PARTNERED WITH HONEYWELL TO DEVELOP AN IBM WATSON-POWERED "ADVISORY" APPLICATION FOR AEROSPACE MAINTENANCE. THE GOAL OF THIS PARTNERSHIP IS TO DELIVER AN ARTIFICIALLY INTELLIGENT APPROACH TO FLIGHT MAINTENANCE IN ORDER TO OPTIMIZE WORKFLOW AND DELIVER RELEVANT DOCUMENTATION FOR FASTER REPAIR TURNAROUND.



do when faced with an unplanned part replacement or a complicated repair?

Enter artificial intelligence, a resident expert at quickly identifying problems and directing users to a viable solution at a speed far exceeding that of the most experienced human expert. With predictive analytics, the ten or more steps within aircraft maintenance could be reduced down to the repair itself and corresponding QA check. Delays could be mitigated altogether, as fleets could perform maintenance on predicted failures while the aircraft is off the clock. In fact, an endeavor to structure a seasoned aerospace engineer from an artificially intelligent learning environment could suspend a large portion of existing delays and cancellations, if applied effectively. Rather than acting alone, predictive maintenance could implement sensors to accurately track performance statistics per part, in tandem with existing part schedules and catalogues, as well as identifying problems far in advance. AI could perform the following systematic maintenance augmentations:

- Ask questions that would otherwise would have involved Aviation Technical Service (ATS) reps
- Provide context to ATS reps automatically when they join the conversation
- Track path to resolution
- Track complex presentation of problems; for example, fault codes that show up together
- Add an interface to knowledge base (aircraft maintenance manuals)
- Encourage collaboration by providing a seamless interface to exchange data

Leading AI companies today are deploying such systems. For example, SparkCognition has partnered with Honeywell to develop an IBM Watson-powered "advisory" application for aerospace maintenance. The goal of this partnership is to deliver an artificially intelligent approach to flight maintenance in order to optimize workflow and deliver relevant documentation for faster repair turnaround.

Such AI-powered systems can monitor the health of aircraft with health prognostics and deliver predictive maintenance insights while providing an in-context advisory that can go as far as to align job assignments to match technician experience and expertise. The results are optimized schedules, minimized maintenance costs, maximized safety, and most importantly, avoidance of flight delays.

By closing the gap between a digital repository of maintenance knowledge and a human engineer executing relevant repairs, predictive maintenance with AI advisory can transform the current shortcomings of the aerospace industry and get passengers home sooner.

This author will confess that thinking about the gleaming, futuristic implications of AI-driven engineers on airline maintenance is certainly most hoped-for while on a flight delayed by maintenance. But if underlying (and oft unspoken) need truly drives the best innovation, then predictive maintenance will be the chance to transform an industry for the better.

BUT WHAT ABOUT SMART BUILDINGS?

THE IMPORTANCE OF IOT-ENABLED STRUCTURES IN SMART CITIES

by **Amir Husain**

People have always sought to make sense of the environment and utilize resources to enhance their safety, comfort, and well-being. It is no different in the growing world of IoT and the evolution of how brick-and-mortar buildings are moving from solely providing shelter to having increasingly complex "intelligent" systems, which allow them to evaluate their own surroundings for the ultimate comfort and safety of their inhabitants.

We are all familiar with current systems installed in many buildings—automated doors, thermostats, smoke detectors, security motion sensors, and the like. These conveniences make our surroundings more comfortable, but that is where their usefulness ends. Increasingly sophisticated systems will enable buildings to "think" for themselves by inferring outcomes and insights from the collected data of these technologies and not only predict, but diagnose issues.

The fact is that we live in physical spaces that have a great impact on our safety, productivity, effectiveness and security. Sensors of a variety of types serve to augment human perception and bring to light forces and phenomena that we would otherwise remain unaware of.

The availability of inexpensive sensors means that many types of measurements can now be made over large areas, while maintaining precision from multiple readings. These sensors enable us to measure all sorts of "fields" in areas where we live, work and play. And knowing more about the environment in this way—gleaning information on fields and how they interact with each other, looking at phenomena or measurements that pertain to our safety, or to the efficient functioning of our environmental systems, for example, can provide us with useful insights to drive action.

The sensors are all sources to tap in order to generate deep and meaningful insights about what is going on inside a facility from maintenance, power management, security, and utilization perspectives. All of this data can be fused together to furnish significant insights. Depending on the purpose and security profile of the building, advanced big data analysis and Machine Learning/ Artificial Intelligence techniques can be used to create an invisible digital shield around zones in the building or the facility as a whole.

At Austin-based AI company SparkCognition, we have pioneered Automated Model Building algorithms and have applied these capabilities with great success to several large-scale plant and equipment use cases. For example, FlowServe Corporation, one of the largest manufacturers of pumps, valves and other types of oil & gas facilities equipment, uses these algorithms to extend the failure forewarning window on their products from 2-3 hours using conventional data science techniques, to up to five days. But most interestingly, as the equipment encounters real-world loads and differences in maintenance and usage patterns, the algorithms self-adapt and optimize their predictions to the specific pump or valve they are monitoring. They don't need to apply a single hand-built machine learning model to all instances of the same pump, even though the equipment has "drifted" significantly over time and is no longer like it was when it first rolled off the factory floor.

Building design is poised at a fascinating juncture where, for the first time, structures will not only serve as passive dwellings, but will become proactive participants in enabling security, comfort and productivity for their inhabitants. The means to achieve this leap in capability will be the combination of 1) advanced sensors and IoT technology, which will allow the building to gauge its environment, learn about its users and monitor itself, 2) artificial intelligence based cognitive capabilities that will form the core of a smart building's 'mind,' enabling pattern identification, anomaly detection, state recognition, continuous learning, speech and language understanding, planning and more, and 3) actuation systems that will allow decisions informed by sensors and made by AI algorithms to actually be acted upon and implemented in a physical sense.

While it is possible to retrofit older structures with this type of capability, as with all significant refits, costs will be high and the entire spectrum of capability will not be available as 'upgrades.' Therefore, it is the right time for architects, engineers, owners and planners to start thinking about how they can create smart spaces from the ground up. Future buildings will be as much about AI, IoT, and advanced automation as they will be about steel, concrete and glass. And perhaps their most distinguishing characteristics will emerge from their intellect, and not just their looks!

ASSEMBLING THE SYSTEMS

HOW TECHNOLOGY PARTNERSHIPS ARE ENABLING THE IoT

by **John King**

Finding the connective tissue between otherwise unconnected ideas, is where the seeds of innovation can lie—a value sewn into Dr. Tom Bradicich at a young age by his parents. Dr. Bradicich's father, in particular, taught him to always strive for excellence in everything he does, and as the vice president and general manager of Servers and Internet Systems at Hewlett Packard Enterprise (HPE), Bradicich continues to seek out greatness in the form of innovative technologies.

Bradicich started his college career as a music major and bounced to physics and psychology before settling on the more lucrative engineering field to support his young family and charitable endeavors. He was drawn to the constant innovation required by the field, and chose to continue on to a PhD for the challenge of contributing to the human knowledge base. A pioneering dissertation on telemedicine led to appointments as an IBM fellow and then a fellow at National Instruments. Coupled with his business and product general management experience, those high-tech connections opened his eyes to "the most innovative domain today": the IoT.

In the past, the internet represented an interconnected network of users finding new ways to connect with each other online. In today's world, the internet extends beyond computers and users. Billions of devices and "things" (the "T" in IoT) are connected to the internet and soon, hundreds of billions of devices. The internet transcends the computer, the device, and even the user itself with its ability to connect two seemingly unlike parties and inanimate objects with one another to achieve a given effort together, collaboratively. The IoT represents new insights derived from objects, the environment, and other parts of the physical world. It offers new ways to engage with each other and exchange meaningful information with or without human intervention.

"The IoT is where so much cutting-edge technology converges," says Bradicich. "When you break it down, IoT and its successes come from the joining together of multiple partnerships

from different technical and business domains and industry verticals," something that Dr. Bradicich believes is a key component to innovation within the IoT.

"When addressing the IoT challenge, we've portioned the solution into four stages: there's the sensors that touch the things, then it moves to a stage of data acquisition and control systems and actuation, and then it'll move to a stage of edge IT such as switches and storage and compute at the edge, and then it may move to a data center or cloud," explains Bradicich. "So just by looking at that simplistic architecture, one can conclude many players are required to have an end-to-end solution and not one single player does it all."

Knowing that partnerships are what lead to innovations, and therefore solutions, Dr. Bradicich and his team have monetized what it means to stay connected in an ever-changing technological world through the development of the Edgeline Converged Edge Systems, where "unprecedented high performance compute, control systems, data acquisition, and HPE iLO systems management is converged in a single enclosure and hardened for IoT edge environments." This type of innovative thinking lends itself to problem solving—something both HPE and SparkCognition have teamed up to conquer.

Where data exists, there's analytical value; where there's analytical value, there are solutions and preventative measures. The goal of the partnership between SparkCognition and HPE is to deliver an unprecedented level of interoperability among operational technology (OT) and informational technology (IT). Machine learning is an invaluable tool in understanding a complete system that is comprised of users, devices, and sensors. As raw data is collected, this partnership encourages the derivation of insight within the system to improve operations, equipment, processes, and security. The implications in terms of user cost-savings are a key outcome, as well as AI-driven prognostics. These provide asset and network protection by detecting problems—whether physical or cyber—before they occur, as well as helping to understand root-cause analysis and remediation of any real or potential problems.

Dr. Tom Bradicich, PhD

VP and General Manager of Servers and Internet Systems at Hewlett Packard Enterprise

Combining resources can create results that would be otherwise unfathomable, and that's what HPE and SparkCognition have teamed up to do. With SparkCognition's knowledge and know-how in the world of AI-powered predictive analytics and cyber security, and HPE's philosophy to lead innovation through the convergence of IT and OT, the IoT will now be protected from unknown mayhem and security breaches.

A key component of an efficient and effective IoT system is the way that system collects, stores, transmits, and analyzes data. SparkCognition creates technology to ingest and analyze data in a variety of environments. That is, the company can process data at the edge of a network, such as through an embedded computer located within a physical asset; or they can process data in a cloud or a central data warehouse. There are several examples where it's advantageous to do one over the other.

HPE's Edgeline System, as the name implies, is created to process data at the edge of a network. For example, in industrial Internet of Things applications such as power production, smart traffic lights, or manufacturing, the edge devices capture streaming data that can be used to prevent a part from failing, reroute traffic, optimize production, prevent product defects, or detect an external

cyber threat to the system. When data analysis is done at the edge of a network, it is known as "edge analytics."

Edge computing does not completely replace cloud computing, however. For example, an analytic model might be created in a cloud then pushed out to edge devices. However, edge computing does provide certain advantages over cloud computing in specific instances, and IoT applications are one area making breakthroughs in edge computing. The mountain of data uprooted by IoT has to be processed and responded to in a short amount of time. On a global scale, the cloud is an indispensable part of that process. Unfortunately, as the distance between the cloud and users grows, so does the transmission latency—the delay before a transfer of data begins following an instruction for its transfer.

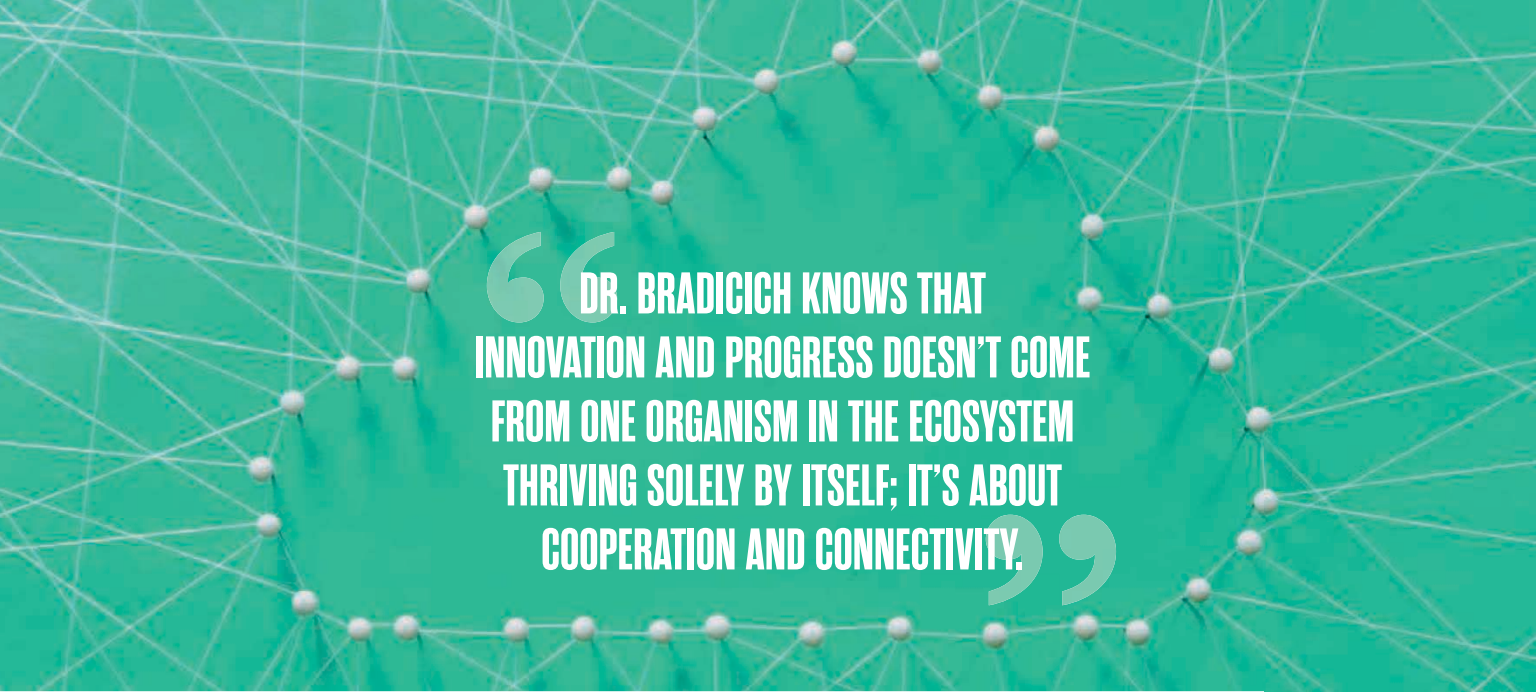
Edge computing shortens the distance between the cloud and users by placing a small edge server between them. This takes some of the workload off the shoulders of the cloud and onto the server, which speeds up applications that demand a low latency response like self-driving cars, robots, and drones.

As for the role of the cloud, Dr. Bradicich does not imply that the cloud should be replaced. He's looking instead to build an ecosystem full of partners from various aspects of the industry to delve deeper into the IoT landscape of possibilities. What emerges will be the result not of technological muscle alone, but of the ability of stakeholders and partners to continually experiment and push the boundaries around how innovation occurs. It is likely that the greatest technological innovations of the near future will be the result of collaboration, and cooperation in designing the partner ecosystem itself.

"I'm not saying that the cloud is in any way, shape, or form going to do anything but get better," said Bradicich. This notion of computing getting more distributed as well as connected is what I see as the innovative frontier, and I'm moving my company in that direction. So it's being the first mover to add an alternative to cloud connectivity, which is simply computing and converged OT at the edge. We want to give our customers choice, and avoid cloud lock-in when compute at the edge is the answer."

Some industry analysts posit that the future of IoT will likely hinge on edge computing (the "things" of the IoT) doing the heavy lifting of analysis rather than running data through the cloud. As for Bradicich, he offers seven reasons that edge computing is growing: bandwidth (the amount of data is growing faster than the bandwidth to send it to the cloud), latency (time lag to send to cloud), security (sending data to a server hosted elsewhere is less secure), corruption/reliability (data may be mis-sent), duplication (since the collection phase occurs at the sensor then again at the cloud), data policy (some data can't be housed elsewhere), and cost (cloud hosting is obviously not free).

While some believe edge computing will make cloud computing obsolete, Bradicich has a different idea: "I call it 'distributed IT centralization.' It's not forsaking the cloud, it's being the first mover to add something to the cloud connectivity, which is simply edge computing and OT convergence at the edge." Much in the way that smartphones have become so much more than phones, Bradicich foresees enterprise class data center technology being taken to edge computing and converging data acquisition, control systems, and industrial networks, all in the same box. That's exactly what HPE's new Edgeline Converged Edges Systems family does.



This is not to say every aspect of this process is handled by one company, but rather, an ecosystem of partners comes together to best serve the customer. "For example at HPE, we offer a new product category called Converged Edge Systems that we've invented," explains Dr. Bradicich. "One of the most important issues with edge computing is security: more sensors mean more vulnerability points and more people engaging. It is common to consider security as an afterthought, after one puts the solution together then to impute security on that," says Dr. Bradicich. "However, at HPE we build that in from the beginning. We work with partners such as SparkCognition who have a forte and a set of experiences along the line of being able to predict and analyze, not only physical failures, but also threats."

While there are many fruits to be reaped from IoT, its success it not guaranteed. There are three major risks that hinder any innovation from flourishing, according to Bradicich. These include the market risk (whether the market is ready for IoT), the technical risk (whether the device can be built), and the company risk (whether companies are willing to invest in the novelty). Touching on company risk, Bradicich purported that many companies are wary of innovation because they have nothing to compare it with. "When it's new, there's no history and we as humans like precedence as, it makes us feel comfortable. Because it was done before, I saw it before. But with innovation you have to sometimes suspend your disbelief. You also have to look at the fact that it's possible that everything is temporary."

Addressing the market risk, Bradicich noted how the market is hungry for IoT. "We have many customers and partners evaluating Edgeline Systems, and others in deployment. So, I think early signs look very good as far as the first 'technical' risk." Expounding on the technical and company risks, he said, "We're using proven technologies. We have combined with innovation such as the AI-powered technology developed by SparkCognition. And therefore, all systems are good as far as we can manufacture it and have it perform as designed. Now, concerning the 'company risk', what's needed is an ecosystem of other partners. This helps each company lower its inhibition. Innovation is not just about helping people overcome a specific problem. It's also about helping people overcome their reluctances. That's really powerful."

Without doubt, IoT has its share of risks. Given the innovations at stake, however, the biggest risk, in the words of Bradicich, is to take no risks at all. Just as innovation is propelled by a strong, diverse ecosystem of interrelated technologies, a key component of minimizing risk is to find great partners to work with.

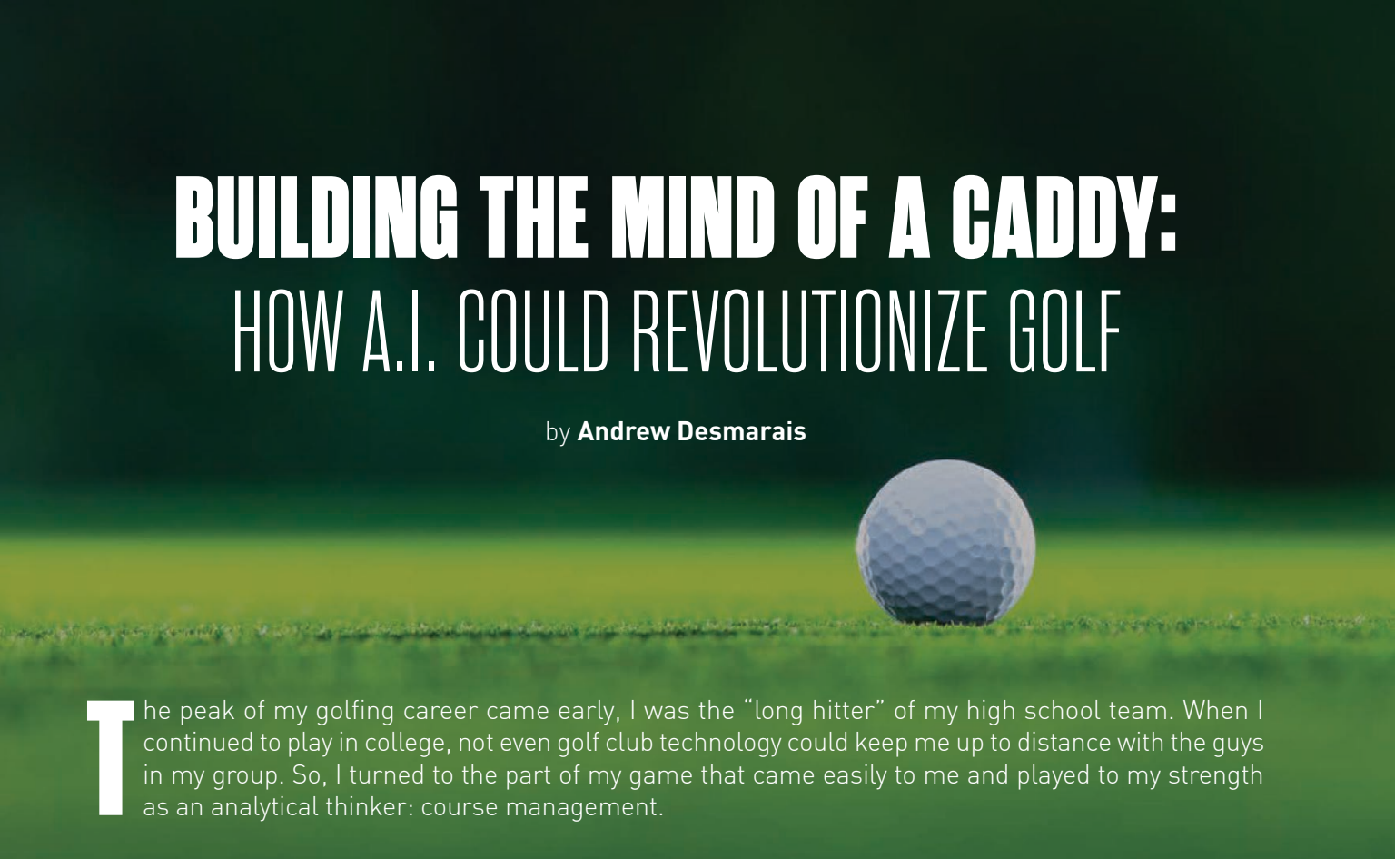
Whether in the cloud or at the edge, technological innovation is all about creating systems and networks that are more than the sum of their parts. Life never emerges separately from its environment. It needs an ecosystem. The Internet of Things is a technological ecosystem waiting to come to life, and innovation in IoT is an ecosystem design story. "A partner ecosystem is absolutely crucial simply because the solution is end to end, and IoT is a solution," said Dr. Bradicich.

The Internet is no longer solely about connecting people—it's about connecting things, systems, and networks. With the surge of devices connected to the Internet, IoT has many advantages for businesses, consumers, the environment, and society as a whole. Dr. Bradicich knows that innovation and progress doesn't come from one organism in the ecosystem thriving solely by itself; it's about cooperation and connectivity. An ecosystem cannot thrive without the other moving pieces, or in this case, strong partnerships.

"I've always told my teams", Bradicich says, "a good company aggressively follows the trends, but a great company sets the trends. And we must set the trends so our customers can be trend-setters themselves."

BUILDING THE MIND OF A CADDY: HOW A.I. COULD REVOLUTIONIZE GOLF

by **Andrew Desmarais**



The peak of my golfing career came early, I was the "long hitter" of my high school team. When I continued to play in college, not even golf club technology could keep me up to distance with the guys in my group. So, I turned to the part of my game that came easily to me and played to my strength as an analytical thinker: course management.

I didn't know that's what it was called at the time, but years later I was praised by my Division-I NCAA golf coach who said it was the strongest part of my game. Course management is the process surrounding a golfer's decisions in choosing the best shot to hit in any given situation.

Course management and Artificial Intelligence (AI) have a lot in common. After attending the 2016 BMW Championship, I recognized how similar a golf caddy is to an AI application in business. Although best known for carrying the bag for a golfer, a caddy's most valuable asset is their ability to help the golfer gather information to make an ideal golf shot. In business, the AI's job is to do the same—to resolve problems and make predictions to help the human in charge make the best decisions.

In the end, the golfer raises the trophy because of their ability to leverage their experience, combined with their judgement on various course conditions, to execute the golf shot. The relationship between AI and businesses is very similar: AI enables businesses to create deeper, more meaningful insights with data that was less valuable before.

TECHNOLOGY

Consider the traditional approach to analytics. In a variety of tools and processes, analysts collect multiple variables around existing or real time events, create a model, deliver the insights for change, and record the results.

Most businesses applying AI, leverage the capabilities similar to the caddy-golfer relationship: enabling the user to create more accurate and predictive insights. The purpose of AI is to build a machine-like software that replicates the human brain.

Humans are best at cognitive abilities like reasoning, language-related analysis, and decisions with no known context. Organizations today are finding the most value with a combination of human activity and cognitive analytics capability. Together, they extract meaning from volumes of untouched data.

AN A.I. VS. HUMAN COMPETITION

Imagine you're the caddy for your daughter's first chance at winning the junior club championship. Not only will she clinch her first tournament victory, you know that this could be her ticket to the varsity team at the top local high school. She's well-prepared. Hours of practice at the driving range fueling her confidence. One opponent stands in her way. A well-recognized player in the city with dozens of rounds recorded this season.

But, this is 2017, and AI is moving beyond the R&D departments of your office and onto the mobile devices of every person. While your daughter is relying on your personal skills and experience in golf, her opponent is guided by an AI-enabled caddy.

WHAT WOULD IT BE LIKE TO COMPETE AGAINST AN A.I. CADDY ON THE GOLF COURSE?

You spent hours playing the course alongside your daughter. You know her game as well as your own game. You think you have the AI caddy beat. But, an AI-enabled caddy could replicate the "feeling" a human gets for making decisions. Based on combining the various advances in AI, it knows when to suggest a risky shot, or play it conservative with a shot to the middle of the green.

While you're frantically flipping through your notes from last years' junior club championship, the opponent's AI caddy is letting machine learning algorithms calculate the most strategic shot in milliseconds. A subset of AI is machine learning, and this caddy is well-trained. A strength of machine learning is the ability to process large amounts of data, recognize and classify patterns, and continuously learn from the real time data to make the best predictions.

Your daughter typically plays best on the first nine holes and you know that words of encouragement during this time are crucial to keep her momentum going through the back-nine. But, you're still not ahead of the AI caddy. The AI caddy knows how and when to communicate in the crucial moments as well. It uses natural language processing (NLP) to digest post-shot comments to decide the best method for encouragement, saying: "Put it behind you; you got this!" if it's early in the round, and staying quiet after a bad shot when it's late in the round.

WHAT IF IT'S AN UNKNOWN SITUATION?

Here you all stand on the 18th tee box, tied with the opponent. You are acutely aware of the mental strain that each player is dealing with. The opponent's golf club is visibly shaking from her nerves. You're secretly hopeful the AI caddy misses this obvious cue. There's no training data for this situation. You think you have the AI caddy beat.

But, a strength of AI is to rationalize through an unknown situation. The opponent communicates her concern with the nerves, explaining: "I'm afraid my nerves might make me hit it shorter." NLP analyzes her tone, correlates it to a situation where she was nervous before, and makes the recommendation to hit slightly more club.

Altogether, the difficulty and complexity of replacing the caddy makes it an excellent illustration for the power of AI. No shot in golf is the same. Either the lie is different than before, the direction of the wind is changing, or most likely: the swing is not feeling as consistent as it did two days ago when practicing.

You and your daughter win—this time. She got lucky since the AI caddy's battery fails, leaving her opponent with no advice on the putt to tie the tournament. After all, progress in AI seems to be outpacing extended battery life.

And for next year's tournament, there's no hesitation for investing in the AI caddy.


OTC2017
OFFSHORE TECHNOLOGY CONFERENCE 2017
1–4 May 2017 \\ Houston, Texas, USA \\ NRG Park
2017.otcnet.org
sparkcognition™
Join SparkCognition™ for a panel session entitled “Big Data,” featuring CEO/Founder Amir Husain.
WEDNESDAY, MAY 3RD, 2017 FROM 2–4:30PM AT THE NRG CENTER IN HOUSTON, TX

DEEPARMOR®

The world's first fully cognitive anti-malware system leverages machine learning, natural language processing and A.I. algorithms to analyze files and provide signature-free security

ANALYZES THE DNA OF FILES TO IDENTIFY THREATS

SUB-SECOND MALWARE DETECTION

SIGNATURE-FREE SECURITY

SELF-LEARNS AND RETAINS KNOWLEDGE

COMBINES STRUCTURED + UNSTRUCTURED DATA (INCLUDING NATURAL LANGUAGE) TO RESEARCH THREATS

REDUCES FALSE ALERTS

Welcome to the Intelligent Edge

We live in a world where everything is connected. Data created from these connections, drive faster insights when acted upon at their source—at the IT edge.

To bring intelligence to the edge, Hewlett Packard Enterprise has integrated enterprise-class IT, data capture and control within Edgeline Converged Edge Systems. Now you can gain real-time insights to better control your industrial IoT environments.

Learn how you can command the intelligent edge at **hpe.com/info/edgeline**

Accelerating next

Hewlett Packard Enterprise