PROCESS
TECHNOLOGY

AUTOMATION + CONTROL + INSTRUMENTATION

X2 puts you in control

Easily calibrate your entire electrical safety tester workload

The new 5322A Electrical Safety Tester Calibrator helps calibration technicians comply with new regulatory standards up to four times faster than with traditional manual, multiple-product methods.

The Fluke Calibration 5322A facilitates compliance with exacting international standards including Australia and New Zealand's AS/NZS 3000 and regulations for various electrical testers.

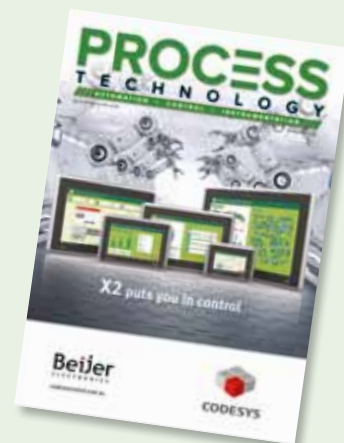**Contact Fluke Australia for more information**

⌨ au.flukecal.com   ☎ 1300 135 853   ✉ auinfo@flukecal.com

0419

PROCESS TECHNOLOGY
APRIL 2019

CONTENTS

READ ONLINE!

This issue is available
to read and download at
www.processonline.com.au/magazine

INCORPORATING CYBERSECURITY INTO WATER UTILITY MASTER PLANNING

A STRATEGIC, COST-EFFECTIVE APPROACH TO MITIGATING CONTROL SYSTEM RISK — PART 1

Umair T Masud, Manager, Consulting Services Portfolio, Rockwell Automation

Cybersecurity threats are ubiquitous and far-reaching. But the stakes are highest when the threats impact critical infrastructure, including water systems.

Yahoo. The Democratic National Committee. Ukraine's power grid. Significant cybersecurity breaches unwittingly kept each of these organisations in the headlines for weeks at a time in recent years. And after the headlines had faded, these companies faced a damaged reputation and an aftermath marked by fading consumer confidence and more than a few class action lawsuits.

While these breaches have put consumers on alert, tactical campaigns targeting industrial applications and critical infrastructure such as Stuxnet, BlackEnergy and Havex have heightened governmental attention and resulted in additional pressure to protect vital systems.

For those safeguarding and distributing the public's water supply, these massive security breaches and threats are yet another reminder of the potential vulnerability of their systems. Due to limited budgets, uptime requirements and talent shortfalls, many utilities struggle to apply even basic security measures. The latest call to strengthen system security to meet the most advanced threats has added a new level of confusion and concern.

Historically, water utilities embraced the IT landscape later than many industries. Many are just now beginning to realise significant benefits. Most have incorporated consumer online access to account information. Others have added smart metering technologies, including advanced metering infrastructures (AMIs). Still others have built SCADA systems that can potentially leverage cloud and mobile technology.

But while the benefits of new technological capabilities are readily apparent, the associated risks often remain undetected and unchecked until a major breach occurs. Recognising the catastrophic impact such a breach could have within critical infrastructure, governments and security communities around the world have stepped up research, leadership, training and guidance.

In the US, *Executive Order 13636 Improving Critical Infrastructure Cybersecurity*[1], issued in 2013, was followed by the National Institute for Standards and Technology (NIST) *Cybersecurity Framework*[2] in
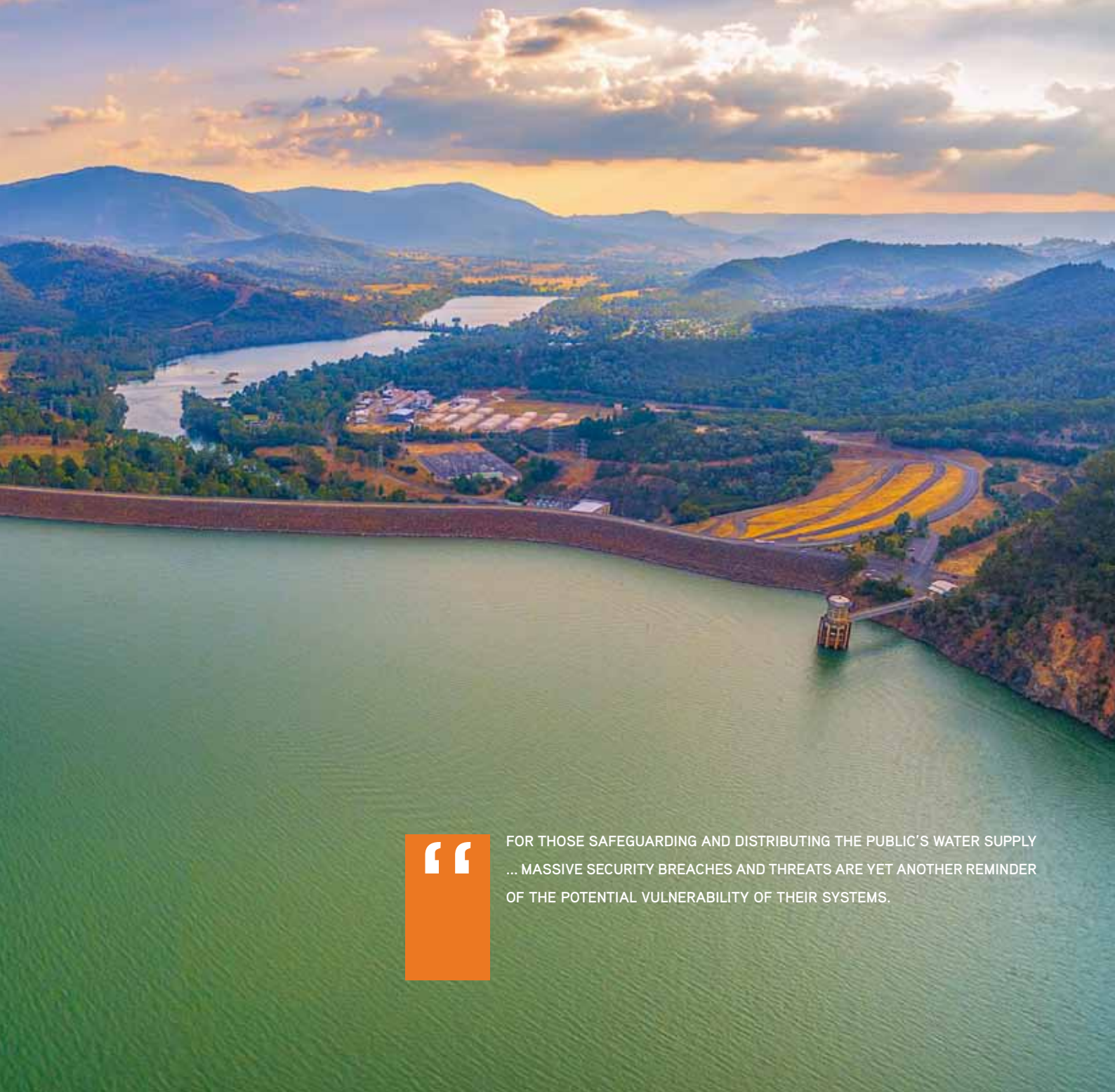
> **FOR THOSE SAFEGUARDING AND DISTRIBUTING THE PUBLIC'S WATER SUPPLY ... MASSIVE SECURITY BREACHES AND THREATS ARE YET ANOTHER REMINDER OF THE POTENTIAL VULNERABILITY OF THEIR SYSTEMS.**

2014. This voluntary framework consists of referenced standards, guidelines and practices to promote the protection of critical infrastructure. Simultaneously, the American Water Works Association (AWWA) released its own *Process Control System Security Guidance for the Water Sector*[3] to provide a sector-specific approach to adopting the NIST framework.

Simply put, there is no lack of practical guidance and tools — and independent experts and suppliers eager to help. As with any security framework, program or solution, implementation can be daunting for water system professionals, especially those in public utilities with limited IT staff and resources. This article outlines the most dangerous cyber threats to utility control systems and why an active defence strategy is often the most practical and effective response. It also includes steps utilities can take now to prepare for the inevitable day when they are faced with a new security challenge or regulatory requirement.

Unique water sector challenges: mission, infrastructure and expertise

Water utilities face unique challenges when addressing cybersecurity issues. Unlike many organisations, water utilities are usually publicly funded and accountable to the community at a very local level. Their mission is to provide a clean, uninterrupted water supply to their state, city or municipality — and to do so within budgets that are often politically charged.

Ageing distribution networks

It's no secret that the water infrastructure in many places around the world is both deteriorating and in need of expansion to match population shifts. Upgrades are costly and time-intensive.

For municipalities of all sizes, repairing and updating water mains, reservoirs and pumping stations is an imperative — and a growing, oftentimes unpredictable, expense. Given limited budgets and resources, utilities must make tough choices. And in many cases, that means devoting the majority of available funds

Water industry

" WHILE PASSIVE DEFENCES STILL HAVE A PLACE IN WARDING OFF LOW-LEVEL ATTACKS, AN AGILE AND ACTIVE DEFENCE STRATEGY IS REQUIRED TO STAY AHEAD OF THE MOST ADVANCED ADVERSARIES.

and personnel hours to maintaining the existing water distribution system.

Conversely, emerging technologies and methods are available that provide new capabilities to improve and extend the life and service level of the infrastructure. But there is often limited budget and staff available to evaluate and deploy them.

Disparate industrial control and information systems

Of course, utilities still must attend to their industrial control systems (ICS) and IT infrastructures to meet other critical industry requirements:

- Maintain and optimise increasingly complex process control and SCADA systems — and develop ways to minimise vendor and control system sprawl.
- Establish proper risk and use evaluation for new technology to minimise negative exposure and impact to future budgets.
- Improve consumer trust — and satisfy growing demand for more transparency and access to account information.
- Meet the inevitable demands of regulatory compliance.

But with internal resources committed to maintaining system availability, many utilities are forced to postpone comprehensive upgrades. More typically, utilities evolve their systems slowly — and rely increasingly on multiple service level agreements (SLAs), system integrators and contractors for control system expertise.

Outsourcing has its advantages. However, often one unintended consequence is a 'silo' approach to the ICS and IT infrastructure and disparate systems. Without appropriate oversight, this can result in a fragmented environment that, by its very nature, is more susceptible to cyber risk.

Escalating threats, increasing sophistication

Across all industries, cyber threats are escalating, both in number and sophistication.

While the private sector accounts for the majority of threats — and power generation receives most of the attention in the utility space — the water sector is equally vulnerable. Although many data breaches are the result of accidental insider activity, the source of the initial breach provides little consolation if it opens the door to malicious actions.

More sophisticated. More persistent. More dangerous.

Perhaps of even more concern than the accelerating number of cyber threats is the nature of those threats. Today, hostile entities are applying sophisticated, orchestrated methods and multiple technologies to stay one step ahead of the IT professionals who implement safeguards to foil them. Among the most dangerous attacks are those orchestrated by advanced persistent threats (APTs). Once nearly the exclusive purvey of nation states seeking data for political

or other strategic gain, evidence suggests that APTs are now being found in critical systems on which citizens depend.

Most important to the success of an APT or any sophisticated threat actor is its ability to remain undetected for as long as possible. Therefore, a successful breach does not begin with, nor may it ever culminate in, mass destruction. Instead, it relies on a covert progression of activities which can be masked by the common noise of a typical network environment.

Sophisticated malicious actors often begin innocuously enough — with information gathering or 'Google hacking' via public-facing websites and social media. While the initial activity appears benign, this passive reconnaissance phase quietly identifies possible vulnerabilities in the system.

Next, the attack moves to active reconnaissance. Now, the attacker deploys a variety of external probing and scanning activities — perhaps including phishing and social media mingling — to acquire sensitive information, such as usernames and passwords. Once inside the system, the attack exploits vulnerabilities utilising sophisticated software tools. These attack vectors take many forms and are custom tailored to the targeted environment. In some cases, these tools may identify the presence of zero-day vulnerabilities. These unknown software weaknesses enable further infiltration until detected and patched. The goal of exploitation is to establish some level of command and control. Once a beachhead is established, additional reconnaissance activity focuses on locating sensitive data within the system — and then transferring it out of the network for malicious purposes. Since the exfiltration of data can resemble normal network traffic, it's very difficult to detect. At this point, the damage is done.

Impervious to traditional countermeasures

For years, cybersecurity programs have centred on network isolation and segmentation — and passive defence activities — designed to mitigate system vulnerability.

How can cyber events affect water systems?

Cyber events can affect water system operations in a variety of ways, some with potentially significant adverse effects on public health. For example:

- Make unauthorised changes to programmed instructions to take control of water distribution or wastewater collection systems — resulting in disabled service, reduced pressure or overflow of untreated sewage.
- Block data or send false information to operators.
- Change alarm thresholds or disable them.
- Prevent access to account information.
- Interfere with treatment equipment and potentially impact all downstream who are dependent on clean water — from private citizens to industry.

Simply put, passive defences are systems that do not require human intervention. These standard countermeasures are important components of any network security program and include antivirus software, security patches, signature-based intrusion detection systems, email filters and firewalls. In recent years, water utilities have recognised the importance of installing, improving and keeping these systems up to date.

In addition, governments and the security community have supported this approach by instituting standards written to help ensure minimal levels of security in various business sectors.

As essential as these countermeasures are, they often leave systems susceptible — or even defenceless — against APTs and other sophisticated, targeted attacks. Here are a few reasons why:

• Anti-virus software only protects systems from malware signatures it recognises.

• Malicious attackers use encryption, DNS tunnelling, email and other covert techniques to avoid detection by intrusion detection systems.

• Email filters struggle to stop correspondence that in every way appears legitimate.

Given today's climate, any organisation that claims traditional countermeasures are enough to keep their systems secure is naive at best. Advanced threats are real and occurring regularly across every business sector — including water and wastewater.

Moving towards active cyber defence

While passive defences still have a place in warding off low-level attacks, an agile and active defence strategy is required to stay ahead of the most advanced adversaries. At the highest level, an active defence strategy[5] uses sophisticated forensics and intelligence sharing — across industries and governments — to identify and counter cyber threats.

> "Our current efforts, geared towards 'passive' cyber defence, are fixated on continuously monitoring and patching systems. Passive defence does not work and will never work against serious cyber threats."[4]
> — *Steven Chabinsky, Former Deputy Assistant Director, FBI Cyber Division*

Of course, not every utility faces the same level of cyber risk or requires the same type of program to achieve an appropriate level of security. For the largest utilities, transforming their ICS Security Program into a comprehensive security operations centre (SOC) may be merited. For many others, an enhanced ICS Security Program that incorporates an appropriate level of external partners is sufficient.

All utilities must perform a business impact analysis or risk assessment to establish the appropriate governance and level of security for their ICS Security Program.

Where to start

It's a process, not a project

With internal IT and ICS security expertise in finite supply — and outsourcing common — there is an understandable tendency for utilities to view any initiative related to information infrastructure, metering or process control systems as a 'project'. By definition, projects are limited in scope and have well-defined objectives, timelines and budgets.

For example, a water utility might initiate a project to change over their metering system to AMI technology. It may select an outside vendor for the project, based on an open bid process. Expenditures are relatively finite and predictable — and expected outcomes can be easily communicated to the public.

Projects are focused on completing a task. Projects begin and end — and may even co-exist at cross-purposes with other projects. But when it comes to safeguard-

ing a utility's industrial control system, a 'set-it-and-forget-it' project mentality can be dangerously limiting. To be truly effective, cybersecurity must embrace a cohesive strategy that extends through every project in parallel with all business operations throughout a utility's life cycle. A breach at any point can put the entire system at risk.

Simply put, cybersecurity is a critical business objective. As such, it must be approached as an ongoing process, albeit one where budget projections and public relations are challenging — and where success is measured by what doesn't happen, rather than what does.

In Part 2

In Part 2 of this article a foundational methodology for building a cybersecurity program will be introduced.

References

1. US Department of Homeland Security 2013, *Fact Sheet*, ⟨http://www.dhs.gov/sites/ default/files/publications/EO-13636-PPD-21-Fact-Sheet-508.pdf⟩

2. US Department of Commerce, National Institute for Standards and Technology (NIST) 2015, *Cybersecurity Framework*, ⟨http://www.nist.gov/cyberframework/⟩

3. American Water Works Association (AWWA) 2014, *Process Control System Security Guidance for the Water Sector*, ⟨http://www.awwa.org/portals/0/files/legreg/documents/ awwacybersecurityguide.pdf⟩

4. Chabinsky S 2013, Passive Cyber Defense: *The Laws of Diminishing and Negative Returns*, American Center for Democracy ⟨http://econwarfare.org/passive-cyber-defensethe- laws-of-diminishing-and-negative-returns/⟩

5. Lee R M 2015, *Threat Intelligence in an Active Cyber Defense, Part I*, Recorded Future, ⟨https://www.recordedfuture.com/active-cyber-defense-part-1/⟩

CLAMP METER

The Fluke 376 true RMS AC/DC clamp meter with iFlex offers improved solutions for a wide range of current measurement situations.

TechRentals

https://bit.ly/2FrhZLB

WIRELESS SENSOR NODE

The WISE-4471 wireless sensor node utilises Narrowband IoT (NB-IoT), an international standard defined by the 3rd Generation Partnership Project (3GPP).

Advantech Australia Pty Ltd

https://bit.ly/2HM5fB1

MASS FLOW METER FOR DOSING CONTROL

Using a low flow control system containing a Bronkhorst CORI-FLOW mass flow meter can help to manage the dosage of corrosion inhibitors more accurately.

AMS Instrumentation & Calibration Pty Ltd

https://bit.ly/2ujcubC

POWER CHAIN CONFIGURATOR

The ÖLFLEX Connect Chain configurator can be used to digitally engineer a power chain online with a few clicks of the mouse.

LAPP Australia Pty Ltd

https://bit.ly/2CvHud5

SCADA increases flexibility, lowers costs for two water utilities

When Park City Water in Utah, located east of Salt Lake City, needed a new SCADA system and HMI, it picked the same solution chosen by its neighbour, Mountain Regional Water (MRW) District. The two utilities collaborate on projects often, share some resources and even share data

Both MRW and Park City have seen significant improvements since switching from their previous SCADA systems to Ignition from Inductive Automation. MRW saves more than US$400,000 per year on energy with the greater control it has achieved by using the new system, while Park City saves the equivalent of one full-time employee by using Ignition to automate its reports to a state agency. Both utilities plan to do more with Ignition in the future, and operators are becoming more engaged with the data at both organisations, creating their own screens in Ignition.

Ignition was implemented at both utilities by system integration company SKM. Based in Bountiful, Utah, SKM operates all over the western United States. "Both utilities need to see data, track the data very closely and store large amounts of data," said Allen Rogers, a principal and project manager at SKM. "They wanted the data to help them make better decisions, run their operations more efficiently and save energy. Being able to track everything in their systems was key to all that. And both utilities are constantly expanding.

"I knew we needed a SCADA system that allowed for growth and could handle a lot of tags, without the need to go back and relicense things. Ignition was a great fit for both Mountain Regional and Park City."

Using Ignition, SKM has built several solutions for both utilities, and its unlimited licensing model is perfect for the growing utilities.

"We needed a new HMI/SCADA system primarily because the one we were using was difficult to expand," said Doug Evans, Water & Energy Manager for MRW. "Every time we wanted to add a site or expand our water system, we needed to acquire new licences. We wanted a SCADA system that could provide everything we needed in one package."

The number of SCADA tags for each utility has since jumped sharply. MRW went from 5000 tags to more than 90,000, while Park City went from 8000 to 130,000.

"We took them from looking through a peephole into their systems, to having a nice bay window," said Rogers.

"The granularity of our data collection with Ignition allows us to see things in our water system that we were never able to see before," said Nick Graue, Public Utilities Engineer for Park City Water. "The real-time data allows us to monitor our system very closely now."

Mountain Regional Water saw significant improvements after switching to Ignition for HMI/SCADA.

It's also easy to add more clients. "Prior to Ignition, we had multiple operators fighting over the mouse to control the SCADA system," said Graue. "Now we have individual terminals for each operator. Everybody has eyes on the system and nobody is getting in anyone's way."

The mountainous region requires MRW to pump plenty of water uphill, and that consumes a lot of energy.

"One of the things we really value with Ignition is that it allowed us to venture into new realms of energy and power management," said Evans. "And it saved us over $400,000 a year. That savings more than funds my entire department, as well as much of our SCADA improvements and upgrades."

For Park City, reporting has become much easier. "I really enjoy the reporting tool that SKM built for us," said Graue. "I'm able to query any parameter of any tag within our entire system, and learn anything about what was happening at a certain time.

"It also gives us the flexibility to continuously add tags of our choosing, whether it's new instrumentation or new reporting capabilities. We are constantly modifying our SCADA system."

Park City sees Ignition as a strong base for the future. "Ignition, in our minds, is a great foundation for what we see as the smart utility," said Graue. "We have various other critical business systems, such as our automated meter reading and our CMMS. We feel we can continue to capitalise on these great technology systems by integrating them with each other."

Rogers said he was very impressed with the speed and power of Ignition when he first became familiar with it. "I was really surprised at how fast and easy it was," he said. "I was able to download Ignition and install it, and within 10 minutes I was connecting to PLCs and adding tags. It was very impressive."

ESM Australia
www.esm.com.au

Cybersecurity - Automation Securely

With PFC100 and PFC200 Series Controllers

Increasing networking and advanced connection to the Internet that is already nearly standardized and now rightly propagate the trend to secure data storage and data transmission in all areas, including automation technology.

WAGO has responded to these requirements for automation components with the PFC100 and PFC200 Controllers. Linux® provides the basis that allows security mechanisms (e.g., IP tables (firewall), VPN, IEEE 802.1x and SCEP) to be implemented. An IPsec or OpenVPN connection can be implemented directly from the PLC via which data are sent encrypted.

In addition, a standard integrated firewall provides protection against unauthorized access. Users thus have the option of upgrading controllers according to the requirements stated in the BDEW (Federal Association of Energy and Water Industries) white paper and the BSI-IT (Federal Office for Information Security) security catalog.

Both the PFC100 and PFC200 Controllers support all TCP/IP family protocols for the simple connection to a network: DHCP, DNS, SNTP, FTP, Telnet, http and Modbus TCP/UDP. In order to ensure information security and integrity during Web access and data transfers, the TLS 1.2 encryption method is used as standard for establishing secure HTTPS and FTPS connections, and the SSH protocol is integrated as standard for establishing secure shell and SFTP connections.

Both controller generations can be configured via integrated Webserver (Web-Based Management) and WAGO's e!COCKPIT programming environment (based on CODESYS) according to IEC 61131-3.

Closed letter (encrypted information) and sealed letter (encrypted channel)

Information remains secure because it never leaves the factory

Open letter (information NOT encrypted)

WHY WAGO?

→ VPN directly on the controller
→ Current encryption protocols
→ SCEP for the distribution and blocking of public certificates
→ Network access protection through IEEE 802.1x

sales.anz@wago.com | (03) 8791 6300 | www.wago.com.au

ETHERNET CABLE FOR ROBOTS

The number of robots used in manufacturing is growing rapidly. According to the International Federation of Robotics (IFR), more than 3 million industrial robots will operate worldwide by 2020 just to drive automation in manufacturing. At the same time, requirements for safe communication between robots, axes, control systems and superordinate systems are also rising.

The igus CFROBOT8.PLUS cable range is designed for ethernet communication between robots, axes, control systems and superordinate systems, and supports torsion angle of up to ±360°.

Specially designed for use in energy chains, the product has been tested for torsion in three-dimensional motion for over 15 million cycles; testing is ongoing to determine the expected maximum service life. So far the result is that the electrical features of ethernet communication work faultlessly, according to the company.

Treotham Automation Pty Ltd
www.treotham.com.au

PROCESS OPTIMISATION FOR WASTEWATER

Veolia Water Technologies has launched AQUAVISTA Plant, a digital solution composed of a suite of intelligent software solutions for real-time optimisation of process performance. It provides a state-of-the-art autopilot to optimise the whole wastewater system, including sewer network and treatment plant. AQUAVISTA Plant focuses on real-time automated optimisation of the consumption of energy and chemicals, biological and hydraulic capacity enhancement, stable operation and compliance of wastewater treatment plants and sewer networks. It is suitable for small and large municipal and industrial wastewater treatment plants.
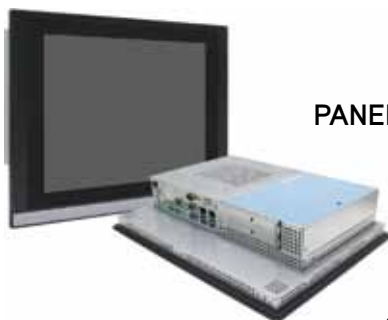
More than 50 features are available, from activated sludge, biofilter, MBBR, UASB and physical/chemical processes to anaerobic digesters, anammox processes and sewer networks. Depending on the number of installed features, AQUAVISTA Plant analyses several sensor measurements in real time and, based on a holistic analysis across all the data collected, will make optimised setpoints available in real time for all parts of the wastewater treatment plant or the sewer network. With combined optimisation, the wastewater treatment plant and the sewer network can perform as one integrated treatment system, for the maximum benefit of the environment and the treatment costs.

AQUAVISTA Plant is claimed to provide from 20% to 50% in overall OPEX savings, up to 40% more biological and up to 100% more hydraulic capacity, improved effluent quality at the wastewater treatment plant as well as a reduction of combined sewer overflows.

Veolia Australia and New Zealand
www.veolia.com.au

INTEGRATED DEVELOPMENT ENVIRONMENT

The DK IoT Studio is an integrated development environment (IDE) that aims to deliver "radical simplicity" to IoT developers and solution providers. It has an intuitive user interface along with drag-and-drop functionality. Users simply drag sensors, processors and other library elements and drop them onto the design panel. Making connections among these elements allows users to start collecting data and sending it to mobile devices or to the cloud.

All of this can be accomplished without any specialised programming skills. DK IoT Studio generates the embedded code (firmware) as well as the web and mobile application code. It makes it easy for hardware developers to go from idea to prototype in minutes without writing any code, because the tool masks the complexity of the underlying SDKs, APIs and drivers. By letting the tool do all the heavy lifting, even software developers can benefit from the quickly fine-tuned generated code.

The goal of providing a design tool like the DK IoT Studio is to provide a seamless path from the creation of an IoT solution to field deployment. The tool can also be used as a central console to monitor and manage devices, data and users. It also offers device management services, and users can also integrate their data into a third-party application, data warehouse or cloud platform.

Digi-Key Electronics
www.digikey.com

PANEL PC

Interworld Electronics has released the ViPAC-821 fanless panel PC based on the Intel Celeron N2903 processor. It features a 21″ (16:9) aspect ratio 1920x1080 LCD display with 250 nits brightness. An optional sunlight-readable 1000 nits display with auto-dimming control is also available. Touchscreen options include projected capacitive or resistive touch or no-touch anti-reflection glass.

The ViPAC-821 is housed in a full metal chassis with IP66 aluminium front panel. Optional SUS304/316 stainless steel front bezels are also available. Two memory slots support up to 8 GB of DDR3L SDRAM. A 2.5″ hard drive can be internally mounted for operating system and data storage. The base model provides a large number of I/O ports including three COM ports, four USB 3.0, two LAN ports, a HDMI port and a VGA port, as well as audio line-out and mic-in and terminals for an external speaker. Optional I/O modules include front panel USB and RFID and rear panel four USB 2.0, two COM and 8-bit GPIO.

The ViPAC-821 provides expansion capability including one full-size Mini-PCIe slot, one half-size Mini-PCIe slot and one SIM slot for 3G/4G/LTE, Wi-Fi, Bluetooth and GPS modules. Two expansion slots supporting one PCI and one PCIe card are provided for dedicated applications.

The ViPAC Series provides a wide-range 9–36 VDC power input with selectable AT/ATX mode power control. With support for Windows operating systems including Windows Embedded 7/8.1 and Windows 10 IoT 2016, the ViPAC Series is suitable for industrial applications.

Interworld Electronics and Computer Industries
www.ieci.com.au

INDUSTRIAL IoT PLATFORM

Today, the industrial automation market faces the challenge of an inflexible infrastructure that is not prepared for the rapidly changing demands of business. Nerve from TTTech is an industrial IoT platform designed to address this issue by acting as the missing link between the business and machines. Designed to help industrial automation companies such as machine builders, system integrators and plant owners to reduce costs, it also creates new value with more flexible manufacturing, smarter maintenance, higher productivity levels and shorter time to market.

The platform comprises three tightly integrated elements that build on solutions developed by TTTech alongside key technology partner and fog computing pioneer Nebbiolo Technologies. The three elements are fogNode edge computing devices, fogOS real-time operating system and middleware orchestration, and fogSM centralised system management software.

Nerve drives value for users in four key feature areas: resource virtualisation, data connectivity, open interoperability and centralised management.

Nerve operates across multiple layers of the classical automation pyramid and is capable of converging functions to the extent that old boundaries are merged or no longer apply. Through the implementation of a fog computing architecture, Nerve provides an open platform for data to be accessed, stored and processed anywhere from the edge to the cloud.

HYDAC International
www.hydac.com.au

Modelling provides asset improvement program for water network

© Stock.Adobe.com/au/pinkomelet

When the water utility for the state of Pahang, Malaysia needed a comprehensive study conducted of the water supply system for a mid-sized town in the area, it appointed Minconsult Sdn Bhd. There were nine water treatment plants (WTPs) with a total capacity of 55,470 m^3 per day, providing water to 20,186 consumers. These plants were old and in poor condition, containing antiquated and inefficient technology. As a result, the Pahang area faced water shortages and supply pressure was low and inconsistent, often taking one week to restore water supply.

Minconsult was responsible for reviewing and studying water demand in the district and making projections of the water demand up to year 2030. The project team also needed to review and analyse the existing WTPs and propose upgrading works to meet water quality standards and increase capacity to serve the projected population growth. The organisation also examined the WTPs and suggested new pipeline installation and storage reservoir refurbishment. These changes to the WTPs would improve the facility to satisfy the projected demand. Additionally, Minconsult proposed new WTPs be erected where necessary to augment the water supply system, and the project team was responsible for surveying the land at these sites. The project had a short deadline of six months.

Minconsult has provided multidisciplinary engineering and project management capabilities since 1980 and is one of the most respected firms of independent project managers and consulting engineers in Southeast Asia. Its role in the project was to provide consultancy services to carry out the comprehensive study of the existing water supply system, to identify weaknesses and shortfalls, and to propose economic solutions. The project team's study and recommendations would alleviate many of the problems with the supply system and ensure that water disruptions and shortages would not reoccur.

The deliverables and expected outcomes would include the proposed asset replacement and refurbishment and the cost plan with proposed scheduling up to 2030. However, the team faced many challenges, including a very old water network, a tight deadline of six months, and a limited core team of one team leader, one modelling specialist and two engineers. Team members also needed to schedule asset improvements and construction so that funding would be distributed without straining the financial resources.

To overcome these challenges, Minconsult leveraged Bentley's WaterCAD to develop the improvement plan. To help users consider many different situations and possible design options, the team used the application to analyse 28 various design and operation scenarios and compare them using scenario management and graphing, improving the decision-making process. What-if scenarios, criticality and isolation valve features were instrumented in the network system analysis.

One way that the Minconsult team incorporated successful modelling in the project was to ensure that the data used was accurate and up to date. This aspect was important because various groups and stakeholders needed to access the same database for information. By keeping everything in a central location, it decreased confusion and increased confidence in the data. WaterCAD allowed users to export and import data to and from CAD and spatial databases. Exchanging and updating data could occur quickly, without losing data or creating errors. Future refurbishment of water assets could easily be captured and shared across various software platforms.

The team saved resource hours because WaterCAD helped reduce the timeframe and staff input by more than half. Data import and export made it easy to share data across the team and with stakeholders, while isolation valves and criticality features helped to quickly segment models into DMA zones. Leveraging WaterCAD allowed users to automatically develop the hydraulic network from an ArcGIS spatial database and AutoCAD drawings, eliminating the need for manual work. Minconsult completed the project within the original deadline of six months, reducing costs.

By also examining water demand on the existing water pipe network and reservoirs, the projection produced more realistic results based on a more probable water growth demand and consumption. The simulation of the 28 different scenarios also resulted in a more realistic water network improvement. The water asset improvement proposal had the lowest possible cost to the company and a much smaller carbon footprint for the surrounding environment.

The project also resulted in benefits for the local community. The project provided advance-planning capabilities for CAPEX management and planning to the utility company and the state government, which manages all its water supply networks and resources. The state is now quickly aware of any issues with the existing system and able to allocate the necessary resources. Effective water assets will be built on time, reducing the amount of shortages to the people and industries within the water network. A robust and reliable water infrastructure leads to better economic and industrial growth, which benefits the local community.

Bentley Systems Pty Ltd
www.bentley.com/en-AU

We have your water quality - under control

Bürkert's Online Analysis System guarantees water quality measurement at a consistent and high level of reliability. It's compact, modular construction includes individual and application-related sensor technology.

Type 8905 gives you peace of mind when it comes to ongoing water monitoring. It offers a high degree of flexibility thanks to simple integration into existing control systems (PLC, EPC). It's efficient operation with low measurement water consumption on account of miniaturised measurement technology (MEMS – Micro-ElectroMechanical Systems) offers a unique and innovative solution to your water monitoring needs.

pH TRANSMITTER

The Model T80 pH transmitter from Electro-Chemical Devices is one part of the Model T80 Universal Transmitter product range. The T80 transmitter range also includes the capability for measuring ORP, dissolved oxygen, conductivity and resistivity, as well as being an ion selective transmitter. The transmitters are available as single- or dual-channel instruments, and digitally communicate with any ECD S80 digital sensor, automatically configuring the transmitter's menus and display screens to the measured parameter.

The Model T80 pH transmitter is available as a loop-powered (single channel only), a 24 VDC or a 100/240 VAC powered transmitter. All versions are available with the optional HART output. The line powered instruments have one 4–20 mA output per channel and also offer Modbus RTU. Available options include HART communication and an alarm relay package. The three relays can be configured as alarm (set point) relays, timer activated relays or fault relays.

The Model T80 pH Transmitter features a large, easily viewed LCD display. Loop-powered instruments have black lettering on a grey background, while 100–240 VAC and 24 VDC powered instruments have blue lettering on a white background when the LED backlight is on. The Model T80 display is easily switched between the single- and dual-channel display modes.

The Model T80 has a simple and intuitive menu structure. Navigation through the various display and information screens is accomplished using membrane switch keys tied to a soft key display detailing the membrane switch function.

AMS Instrumentation & Calibration Pty Ltd
www.ams-ic.com.au

WIRELESS ETHERNET GATEWAY

Wireless data transmission is now commonplace in machinery and equipment applications. WAGO's 758-918 wireless Ethernet gateway, which meets the IP65 degree of protection and has an internal directional antenna, is suitable for harsh industrial environments.

In addition to the standard current WLAN standards, it also allows communication via Bluetooth 4.0. Integrated access point functionality makes it possible to set up a WLAN or Bluetooth network, and the gateway can be easily configured with a button on the device or via web server.

Main features include WLAN 802.11 a/b/g/d/e/i/h and Bluetooth 4.0 with robust communication and high data throughout. The IP65 protection allows for direct on-machine use. Access point functionality makes it possible to build a network of up to seven clients. An additional version with external antenna is also available, which can be used in a control cabinet or where there is a poor radio connection.

WAGO Pty Ltd
www.wago.com.au

IT/OT CYBERSECURITY PLATFORM

Forescout Technologies has announced what it says is the industry's first unified device visibility and control platform for IT and operational technology (OT) security. Integrating recently acquired SecurityMatters technology into its core platform, Forescout offers robust visibility and control capabilities to manage cyber risk across both IT and OT domains. Additional enhancements will enable visibility for multicloud infrastructures, provide auto-classification for medical and industrial devices, automate network segmentation controls across firewalls, as well as cloud and software-defined network (SDN) environments.

Forescout's visibility into multicloud infrastructures now includes Microsoft Azure, adding to existing offerings with AWS and VMware, while integration with Cisco ACI provides visibility into SDNs for data centre environments. Integration with the full line of Belden industrial switches, along with passive monitoring of the lower layers of OT network stacks, provides deeper visibility into industrial control systems and OT devices.

Enhancements in auto-classification capabilities now allow organisations to auto-classify more devices and leverage this context for policy enforcement. Expanded coverage identifies over 500 different operating systems and over 5000 different device vendors and models.

With the growing connectivity between IT and OT networks it is important to understand the risk profile of devices in both domains. Forescout has added risk assessment capabilities, including vulnerability assessment for OT devices and industrial control systems (ICS). Additionally, rogue device detection identifies impersonators using spoofing techniques and helps organisations prevent malicious access, as well as improve audit compliance.

ForeScout Technologies Inc.
www.forescout.com

COMPACT EMBEDDED SYSTEM

The ITG-100-AL from iEi Integration is a fanless compact embedded system equipped in its basic form with standard I/O ports and supports a wide operating temperature range of -20 to 60°C with air flow.

The standard I/O ports can be expanded upon while still keeping the device's compact size with the ITG-100-AL's 'block layers' feature: additional layers with extra ports depending on the user's preferences can be added to expand the interface options and increase data storage space. These block layers include a choice of a 2.5″ SATA HDD/SSD bay, a knockout-hole layer with selectable I/O interface, or both at once.

The compact embedded system comes with a full-size PCIe Mini slot reserved for 3G/4G and an M.2 A-key slot reserved for Wi-Fi in order to provide easily accessible function expansion options.

The ITG-100-AL has palm-sized dimensions of either 137 x 102.8 x 36.2 mm or 137 x 102.8 x 56.2 mm, while providing enough basic I/O options to be applied to a variety of fields such as military applications, industrial automation, traffic control and intelligent gateway usage in smart factories.

ICP Electronics Australia Pty Ltd
www.icp-australia.com.au

THERMAL MASS FLOW METER

The ST80 Series thermal mass flow meter from Fluid Components International (FCI) offer FCI's Adaptive Sensor Technology (AST), which features a hybrid sensor system that combines both constant power (CP) and constant temperature (CT) thermal dispersion sensing technologies in the same instrument.

When operating in AST mode, the ST80 meters measure in CT during start-up and through the lower flow ranges, and will then seamlessly shift into CP mode at mid-range and higher flow rates. The result is a best-of-both technologies performance level where the ST80 meters deliver a fast response with extended measuring ranges, at low power consumption to maximise sensor reliability and reduce instrument energy expenses.

ST80 flow meters feature FCI's rugged no-moving-parts flow element design, which provides direct mass flow measurement with a single process penetration. They are accurate to ±1% of reading, ±0.5% of full scale and repeatability of ±0.5% of reading. The turndown ratio is factory preset to meet the requirements of the application from a minimum of 2:1 up to 100:1. This meter series operates over a wide flow range; the insertion-style configuration range is: 0.07 to 305 NMPS; the inline style configuration range is: 0.01 to 3140 NCMH.

The ST80 Series features multiple outputs to interface with control systems and/or set-up or configuration devices. The standard ST80 meter configuration includes: dual 4–20 mA, NAMUR NE43 compliant analog outputs, HART (version 7) and Modbus 485. Optionally available are Foundation Fieldbus and Profibus PA. All digital bus communications are full two-way I/O.

AMS Instrumentation & Calibration Pty Ltd
www.ams-ic.com.au

EXPANDED IO-LINK SYSTEM

Belden has expanded its Lumberg Automation LioN-Power IO-Link System to help industrial manufacturers address the fast-growing need for IIoT connectivity through simplified device automation. In addition to leveraging standardised protocols, the range features user-friendly integration and configuration tools that eliminate the need for specialised programming skills. Furthermore the LioN-Power IO-Link System makes it possible to implement predictive maintenance by transmitting diagnostic data from intelligent IO-link sensors and actuators before a failure happens.

The two LioN-Power IO-Link I/O Hubs offer 10 digital inputs, six digital outputs and 16 universal usable inputs and outputs. IO-Link devices, IO-Link masters and I/O hubs can now be easily connected to process up to 132 I/O signals per system. This offers an effective way to update from passive to active systems or to collect many digital signals in distributed environments. Moreover IO-Link devices are designed to work seamlessly with the TMG IO-Link Device Tool as well as the TE concept tool in the future.

All LioN-Power System components are designed to operate in the harsh and confined environments typical for robotics; machine and material handling; automotive and food/beverage manufacturing; transportation; and other industrial sectors.

Belden Australia Pty Ltd
www.belden.com

VIDEO INSPECTION SYSTEM

The Aqua SnakeEye is a handheld remote video inspection system. It is available to rent from TechRentals.

The lightweight and portable design combines a TFT-LCD display and 3 cm-diameter camera (including illumination) to provide the user with a clear, full-colour video of hard-to-reach areas. The modular design ensures that the camera can be easily configured for non-destructive inspections of machinery, inside walls and ceilings, vehicles and engines.

The product can function in various industrial and commercial environments. It is constructed to withstand shock and vibration and is resistant to water, dust and dirt. Additionally, it is equipped with a memory card and a rechargeable battery pack with charger.

The system comes with various adapters which allows the user to mount the camera to their hand, a 45.7 cm arm with 90° articulation, a 9 m extension cable, and a 1.6 to 3.6 m extension arm.

TechRentals
www.techrentals.com.au

2D/ 3D Laser Profile Scanner
for Welding Quality Inspection

Highest Performing Profile Scanner with respect to accuracy and measuring rate

Compact, Integrated Intelligent Controller for detection and evaluation of different surfaces

Optional **Blue Laser** technology offers higher focused, higher resolution measurement for finer details with maximum precision. Also enabling a more reliable measurement on organic, red-hot glowing and transparent objects

To find our more, please visit our website at **https://www.bestech.com.au/laser-profile-scanning-2d3d/**

OR Contact us below

MOBILE TEST BENCH ENABLES FIELD VERIFICATION IN HIGH-VOLUME GAS INSTALLATIONS

US manufacturer Big Elk Energy Systems, LLC has developed one of the world's first mobile gas flow rate test benches. This system can be used to verify gas meters that are installed in high-volume gas installations without interrupting operation. At the heart of the mobile M3 system is the ultrasonic gas flow meter FLOWSIC600-XT Quatro from SICK. The meter combines two measuring systems in a single meter body, thus offering full redundancy in a very compact enclosure.

"When it comes to measuring high volumes of gas, two things are paramount: uninterrupted operation and minimal measurement uncertainties," said Geoff Hager, CEO of Big Elk in explaining the background of the system. "To ensure the latter, gas meters are in some cases recalibrated on a regular basis. The cycles are either stipulated by law or agreed between operators. Increasingly, they are also being determined as required on the basis of equipment diagnostics. However, recalibrating the metering package system is a major hold-up for operations. Gas meters need to be removed and transported over long distances — with lots of associated risks such as transport damage. In the meantime, the system has to use redundant equipment to continue operation, often with reduced capacity. It can take weeks, and sometimes even months, until the meters can be reinstalled."

Big Elk's mobile flow test bench

In an effort to reduce this regular workload and expense, Big Elk has designed one of the world's first mobile flow test benches. The patented *Mobile. Master. Meter.* system (which is shortened to just M3) can be transported by truck to the measuring stations. Once it has arrived there, the test bench is connected to the existing pipe system and thus integrated into the gas flow. The adjustable high-pressure connection pipes of the M3 — for different run lengths, heights, angles, and positions — can be easily positioned with a crane and smoothly connected with overlapping slip joint connectors. Big Elk has thus solved a core problem that defeated earlier concepts for portable test benches.

Another special feature of the M3 is the verifiable ultrasonic gas flow meter FLOWSIC600-XT Quatro from SICK. With the aid of state-of-the-art technology, the meter combines two measuring devices in a single unit with a 4+4 path concept. This permits redundant control measurements, which are important particularly given the high demands that are placed on a test bench. Here, intelligent diagnostics ensure that even the smallest changes in the flow behaviour can be detected. At the same time, FLOWSIC600-XT Quatro is also unusually compact and can tolerate vibrations during transportation — another ideal prerequisite for a mobile test bench.

"Right from the start we wanted an ultrasonic gas flow meter for the master meter," explained Hager. "It had to be a highly reliable measuring device so that we could maintain the calibration of the master meter at a level of at least 45 m/s. As well as this, confidentiality was extremely important to us during the long R&D process. Both of these factors led us straight to the SICK team in Houston. Some of us had already been working with SICK teams for over 20 years. We value the close personal relationship, and in addition the SICK ultrasonic product line is the standard for so many of our key clients."

Deciding on the FLOWSIC600-XT Quatro

Hager explained that the decision to opt for the FLOWSIC600 XT Quatro had not been without risk to start with. "The XT, which is the successor of the popular FLOWSIC600 Classic, was new, and we weren't familiar with it yet.

"We wanted a 4+4 design — the M3 is claimed to deliver outstanding results in every application, and full redundancy is the key to this. But to start off with, we were happy with the predecessor model FLOWSIC600. It was only when we started discussing the project that several SICK team members started suggesting the XT.

"What ultimately tipped the balance was the innovative design and the new style of condition-based indicator of the XT, which enables improved control diagnostics even within a normal 4-path configuration," he continued. "With the current M3 test bench, the pressure is limited to the full ANSI 600 class. Initially, calibrations are offered for 4″ to 12″ pipe diameters. In fact though, all speeds between 30 cm/s and 45 m/s can be recorded. A second model is being planned for line sizes up to 24″ and for pressures up to the ANSI 600 class."

The M3 was launched at the start of 2018 after extensive field studies and reworking. It is initially being used in two projects, and further orders have already been acquired. "We believe that we can cover over 80% of the basic applications installed in the USA with this test bench," said Hager. "But we also have plans for additional units — in particular for a wider service range, but also to cover larger meters and higher pressure classes."

The M3 solution may still be in its infancy. But the Big Elk team thinks it is revolutionary: "We firmly believe that this is going to be a major success. It is undoubtedly just a question of time until field testing of ultrasonic gas meters becomes the default method for gas pipeline operators."

For more information: https://www.sick.com/de/en/ultrasonic-gas-flow-measuring-devices/gas-flow-meters/flowsic600-xt/c/g349351

SICK Pty Ltd
https://www.sick.com/flowsic600-xt

SICK
Sensor Intelligence.

PUSH-BUTTONS AND SIGNALLING DEVICES

APS Industrial is now offering the Siemens SIRIUS ACT range of push-buttons and signalling devices. These elegantly designed and high-performance push-buttons, indicator lights and switches offer style, intelligence and durability and a snap-on concept that makes the task of installing a unit easier.

The SIRIUS ACT range maintains its durability and reliability when dust or water under high pressure are involved. Oils, caustic solutions and extreme environmental influences cannot disrupt reliable operation.

The various communication interfacing options provided by SIRIUS ACT enable simple combinations of push-buttons and signalling devices, HMI touch screens and industrial PCs. This means that complex input stations can be set up without extensive wiring and engineering time and effort.

APS Industrial
www.apsindustrial.com.au

EXPLOSION-PROOF BEACONS

The latest additions to the D1x range of beacons from E2S Warning Signals, the D1xB2 xenon and LED explosion-proof beacons, are designed for installation in hazardous areas. They are approved by leading certification bodies and include fault diagnostics, supporting SIL2 requirements by enabling the control system to interrogate the devices' operational status.

The marine-grade LM6 aluminium enclosures D1x, BEx and D2x, the 316L stainless steel STEx range and the GRP GNEx provide a variety of mechanical protection, corrosion resistance and weight to suit different environmental requirements and applications.

The polycarbonate, UV-stable lenses are available in amber, blue, clear, green, magenta, red and yellow. While enhancing the light output, the lens filters are also field-replaceable, enabling the reassignment of beacon function to be a simple and quick process.

A particular D1x version, the D1xB2XH2, is claimed to be the brightest explosion-proof xenon strobe light/beacon available for public mode fire alarm, ADA compliant, hearing-impaired applications. The unit is UL/cUL approved for Class I Div 1, Class II Div 2 and Class I Zone 1, and suitable for both gas and dust environments.

Mechtric Pty Ltd
www.mechtric.com.au

SUEZ solves big data problem with magnetic flow meters

SUEZ operates regulated water systems in eight US states, and provides contract services to over five million people. SUEZ operates several water systems in the suburbs of New York, including SUEZ New Rochelle and SUEZ Westchester in Westchester County, New York.

SUEZ needed greater visibility into its water usage and flow so that the company could minimise water losses. The critical problems SUEZ wanted to solve were water leaks caused by line breaks in the water mains, and water theft by contractors and others. A big main break can waste millions of litres of water, since the time it takes for the leak to surface could be weeks or even months, according to Nick Curcio, manager of non-revenue water for SUEZ.

SUEZ began by closing interties between systems and routing water to locations where it could be measured more easily. "We broke the systems down into smaller zones," said Curcio. "We wanted to minimise closed valves, and made sure that no unmetered water crosses the boundaries between systems." They called these zones DMAs, or District Metered Areas. Water flow into and out of the DMAs is to be measured and uploaded to the system operating model.

The company created a big data-driven proprietary model of its water systems using historical data to determine baseline water usage in each main, in each zone, in each system. In order to compare real-time water usage to the baseline water usage the company developed from history, SUEZ needed a way to economically measure water flow and pressure at the boundaries of each zone in the systems. "These water flow meters and pressure transmitters needed to be rugged, durable and able to operate in no-power situations during storms and power outages, to continue delivering data to the model," said Keith Kolkebeck, director of technology solutions for SUEZ. "We knew we needed a battery-operated solution."

Kolkebeck and the SUEZ staff searched for devices that could meet those criteria, and determined that the Siemens Sitrans FM MAG8000 would work as the heart of the system. The Sitrans FM MAG8000 is designed for low-power applications like distribution systems and agricultural irrigation systems. It is designed to have excellent performance at very low flows, and high accuracy at the upper end of the flow range.

The transmitter can be remotely mounted. This, according to Kolkebeck, was an important feature, because of the difficulty of entering a manhole located in the street. The meter body can be mounted in the main running under the street, but it isn't usually necessary to enter the manhole. The flow transmitter, the 10-year life expectancy battery, and the cellular data logger and cellular modem are mounted on a standard back panel. Instead of being installed in a cabinet, the back panel is installed on a set of slide brackets in a footpath-mounted meter vault (the same sort of meter vault a large household water meter would be mounted in). The SUEZ technician flips open the meter vault lid and pulls the back panel up and onto the footpath for inspection, maintenance or repair.

The flow meter measures flow and the data is stored in the wireless data logger at one-minute intervals. Once a day, the data logger's cellular modem uploads the day's data to the SUEZ SQL Server enterprise database, called EOps, a proprietary program with a database that is SUEZ's meter data management system.

Curcio said the company started with 26% water losses in New Rochelle and 28% in Westchester, so it was essential that SUEZ got a handle on stopping the losses. "With the data from the flow meters, we can see water used, consumed or lost in the EOps system," said Curcio. The data has been able to pinpoint leaks that were previously thought to be simply part of the usage baseline. "A spike in usage indicates a leak, and the flow data is fed back to the model to triangulate where the leak is.

"We are finding leaks in hours, not days," Curcio continued. "Our standard time-to-fix is now less than 24 hours, where it might have taken several days before. The meter data allows us to pinpoint leaks to within a few feet. This means less time digging up the street and a faster time to repair."

The time the leak happens to the time the leak is found and then repaired has also been shortened. In some cases it is only minutes. A 30 cm main flowing at 3 m/s produces around 12,800 L/min of flow. If it takes 25 hours to find the leak, the lost water will be over 19 million litres.

According to Curcio, a 1 million gallon (3.8 million litre) leak in New Rochelle is roughly equal to 5% of production. Finding and repairing a leak like this is critical. Curcio said that the savings in New Rochelle in previously lost water have been over a million gallons a day. Westchester's results are similar.

A longer version of this story can be found online at: https://bit.ly/2CDeGiK

Siemens Ltd
www.siemens.com.au

PoE SWITCHES

The SPIDER III range of switches by Hirschmann has expanded to include PoE options to enable fast data transfer over longer distances.

The PoE editions include PoE+ support as well as options for fibre ports in a single device. The units come with a power budget of 120 W, which includes up to eight PoE+ ports.

With jumbo frames support for CCTV applications and DIN rail mounting support, the range can be powered by 12–57 VDC and can withstand harsh environmental conditions due to its IP30 metal enclosure. The range is suitable for use across a variety of sectors and applications, especially automation environments that require reduced cabling.

Control Logic Pty Ltd
www.controllogic.com.au

MOTION CONTROL SYSTEM

The latest generation of Pilz motion control system, the PMCprimo C2, offers high cycle counts and a wide number of interfaces as well as an encoder input, digital inputs and outputs, and a USB interface for data import and export to ensure a high level of flexibility.

The product is now equipped with a 1.3 GHz processor. Users benefit from fast commissioning times due to programming via Soft PLC in accordance with IEC 61131. The upgrade to version 3.5 of Soft PLC means users now have access to all the benefits of object-oriented programming. Due to the integrated real-time task (processing time 1 ms), there is now the scope to implement high-performance applications such as path interpolations.

The system is equipped with the real-time Ethernet EtherCAT Master, and also supports master and slave communication interfaces such as Modbus/TCP, CAN or Profibus-DP-S.

The PMCprimo control systems have PLC and motion functionality, and they can manage the automation within a plant, including movement management on servo axes. Up to 32 axes can be linked flexibly to form a kind of electronic main shaft, and simple CNC tasks can be solved.

Standard functions, such as 'flying saw', 'cross cutter' or 'cam plate functions', are already stored as function blocks. Machine functions, such as tubular pouch packaging, are also available. The implementation of modern functions, such as remote maintenance, automatic parameter setting for swapped-out system components and the sharing of all I/Os, allows users to implement high-performance solutions with high availability.

Pilz Australia Industrial Automation LP
www.pilz.com.au

SECURING SCADA IN THE CLOUD

THE BEST OF BOTH WORLDS: FLEXIBLE AND SECURE

Cloud-based solutions for SCADA applications offer significant benefits in terms of efficiency, scalability, speed and cost certainty. For many industrial operators, however, the benefits are left unexplored due to fears over the risks of cybersecurity.

The benefit of SCADA in the cloud is the potential for much greater flexibility, scalability and certainty. It promises the ability to massively reduce capital expenditure, provide predictable costs, accelerate implementation and quickly accommodate changes when adding or altering assets. As a more efficient model of deployment, it significantly reduces barriers to entry across many industries.

With cloud-based SCADA, organisations don't have to set up a control centre or backup centre — they can leverage the cloud infrastructure from their service provider. Eight to 10 months for a SCADA project can be reduced to a few weeks. There is no need to buy servers, and organisations can start with fewer assets, being able to add them and delete them when needed. Software versions are always kept current.

Security issues are key to the design

SCADA in the cloud can offer a reliable and a secure solution. On-site resources and expertise can be supplemented by remote support, continual monitoring and automatic updates provided by the service provider. In many ways the design of communications is similar to topics considered in earlier SCADA systems; however, now it is more important to have a solid cybersecure design.

The issue of cybersecurity is, of course, key in such systems, especially at a time of growing threats to industrial control systems. The move to digitisation in industrial control systems has plainly increased the cyber risks. Manually operated equipment has one upside: it can't be hacked. As control functions are automated, the range of potential targets for an attack increases. Increasing connectivity, with more and more devices and systems networked in the Industrial Internet of Things (IIoT), has brought many benefits, but it has also brought cybersecurity concerns.

It is not just the 'attack surface' or number of the vulnerabilities that has grown, but also the potential consequences of a cybersecurity breach. Increased regulatory expectations mean that businesses risk serious reputational damage and costs (in terms of regulatory penalties) even without a successful breach. Those that are successful, meanwhile, have demonstrated that the risks are far from theoretical:

- The Sandworm hackers caused blackouts for more than half a million people in the Ukraine in 2016 — after targeting the US.

In addressing these risks, businesses are hampered by a number of factors. The first is general skills shortages as a result of a rapidly retiring workforce, and specifically a lack of cyber skills. Petroplan's Talent Insight Index 2017 found more than one in five in the oil, gas and energy sectors saying industry lacked the right talent for growth, and more than a third said they needed greater IT skills as the reliance on digitisation and big data grew.

Within businesses, meanwhile, operational silos persist — between sites, between businesses within groups and, perhaps most significantly, between IT and operational technology (OT) staff — despite the technological convergence.

The result is that ownership of and responsibility for these risks is unclear. This is particularly significant since the traditional approaches of IT and OT are very different. Specifically, availability in the operational space is a greater priority, being essential in many cases to safety. Appropriately, security solutions for IT and OT therefore differ substantially. Notwithstanding this, there is, in any case, still a significant lack of clarity over what is appropriate. With little in the way of consistent cybersecurity standards, we don't yet have agreement on what 'good' looks like.

A challenge, not a deal-breaker

There are, in fact, two key dangers in terms of cybersecurity when it comes to SCADA in the cloud.

The first is that they are ignored or inadequately addressed. Unsecured connections through satellite or radio communication provide hackers with an opportunity to target the remote site and hack into the cloud or SCADA system. Every unsecured valve site, for example, becomes a significant source of vulnerability.

The second danger, however, is that the risks are overstated to the extent that businesses are put off from cloud deployment. That would not only mean they miss out on the benefits SCADA in the cloud can bring in terms of efficiency, which would have a potentially bigger cumulative impact on the industry over the long term than any of the cyber attacks we've actually seen.

That's clear when you look at attack vectors — how breaches occur, and malware or hackers actually get in. In some cases, it's the result of unsecured points of connectivity to the ICS environment, with multiple equipment and system vendors given access. Elsewhere, it's the result of either external or business network security being compromised. Often, however, it's employees and contractors bringing in the threat, whether through falling victim to phishing or spear phishing attacks or through their laptops, phones, smart watches, IoT devices or removable media. The last remains a pernicious and pervasive source of vulnerability.

An issue of access

It is worth reminding ourselves that SCADA is used to monitor and sometimes control geographically distributed assets. Many of the SCADA systems being designed today are focused on collecting performance and diagnostics data for analytics to achieve an always up-to-date visualisation of the company's performance
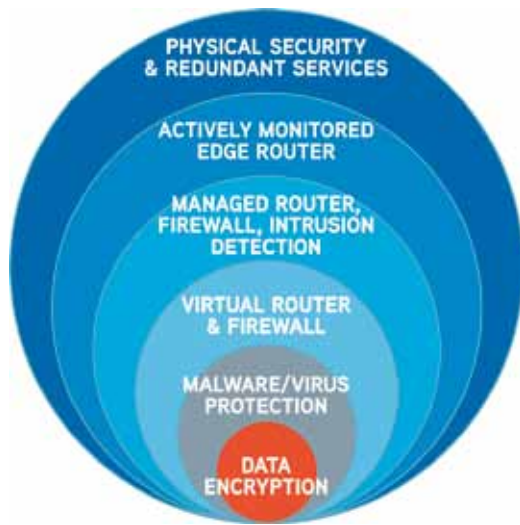
- The Shamoon virus crippled tens of thousands of computers at Middle Eastern energy companies in 2012, and resurfaced four years later.
- The WannaCry ransomware spread across the globe last year, and affected more than a third of the UK's NHS trusts — and not just hospital computer systems, but medical equipment such as MRI scanners and blood testing devices as well.

These are just some of the most high-profile examples. More widely, more than half of industrial facilities have experienced some form of cybersecurity incident, according to a Honeywell survey last year, and three-quarters expect an attack on their industrial control system, according to Kaspersky Lab.

A pressing concern

Both the number and range of attacks is growing as the threat evolves. Among the most worrying developments is the specific targeting of safety systems. In December 2017, hackers invaded the safety system of a critical infrastructure facility — described as a "watershed" moment in industrial cybersecurity. However, it actually followed an attack on the safety systems at a Middle Eastern petroleum company.

SCADA cybersecurity

Figure 1: Defence-in-depth security.

> AS CONTROL FUNCTIONS ARE AUTOMATED, THE RANGE OF POTENTIAL TARGETS FOR AN ATTACK INCREASES.

metrics while giving a much smaller group of people the ability to see leading indicators of future problems and take action now to avoid shutdowns later.

The first level of cybersecurity is simply to limit write access (control), through the application's configuration, to those who need control functionality and only with appropriate authentication. Whether the system is on the customer's site or within a data centre, this simple role-based criteria should be used to significantly improve cybersecurity. This is strengthened by the use of multifactor authentication where the most common approach is to provide a code to the user's phone (text or dedicated app) to provide a second level and one-time-use code. This nearly eliminates the use of someone else's password to gain access. Security is important when looking at SCADA in the cloud, but it is far from being an insurmountable challenge. Most of these concerns are an issue regardless of where the software is running.

The central problem to overcome for securing off-site SCADA solutions is the lack of centralisation. Businesses are left trying to secure multiple access points used by remote employees, contractors, customers and the vendors of control systems and third-party equipment and software (where they are given remote connectivity for the purposes of upgrades, patching, monitoring or support).

The numbers of these access points and the lack of central oversight and control lead to a variety of problems:
- Only partial data is available on assets and events.
- There is no proper hardening.
- There is no proper monitoring, nor governance.
- There is no proper planning and accountability around cybersecurity.

Businesses are left to simply trust that each of those making and managing the connection through these access points is doing so in a secure way. That's an unwise assumption.

This problem is only going to become more pronounced as the number of connected IIoT devices grows.

A proposed solution

SCADA is by definition data acquisition from dispersed assets. It makes sense to centralise your processing and data storage in the centre of the assets (from a communications time stand-

point) to minimise delays and communications costs. If you're monitoring assets within a single facility, you'll get your best performance at the Ethernet switch shared by most or all of the devices.

If you have many sites with great distances between them, you'll want to take a closer look at where the network centre is located. In most cases, you'll find communications are using IP technologies with very fast connections to large data centres. Today's data centres are the communications hubs of our society and already provide the physical security, IT services and cybersecurity required by today's internet applications.
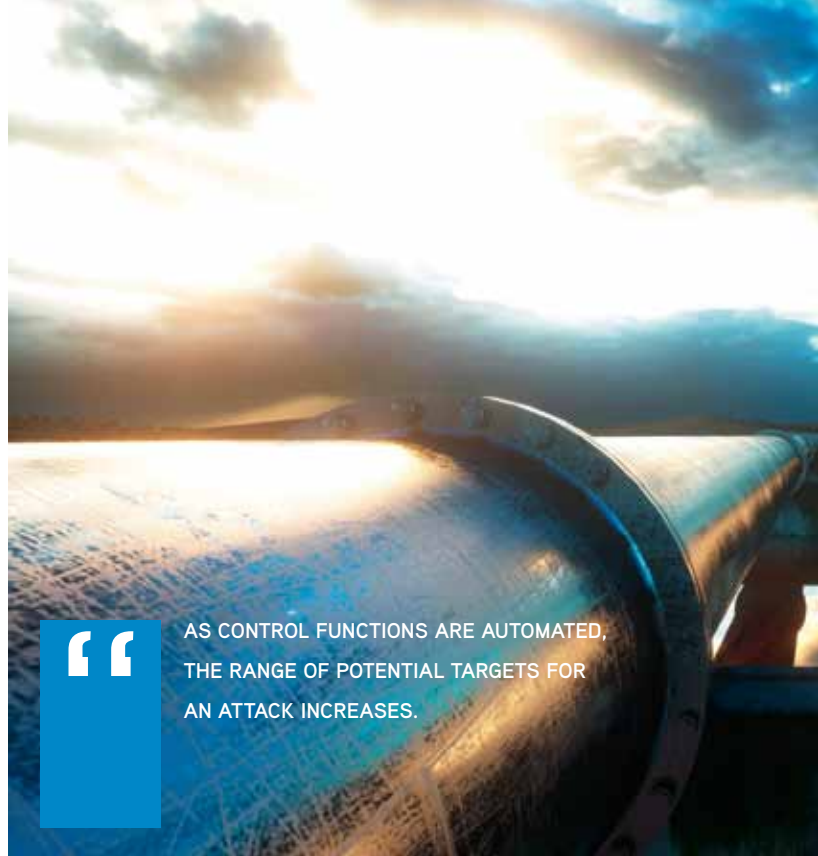
A centralised approach

The key to SCADA in the cloud is security in the cloud — centralising security through a cloud-based security centre and communication server.

This security centre can handle the authentication of connections, ensuring these are valid before allowing access to the communication server. All communications from these sites pass through a secure tunnel using Transport Layer Security (TLS) encryption, and a single firewall rule can be enforced for all remote connections. This provides a distributed architecture with secure tunnels from operations to remote sites.

Traffic from the plants or sites is all channelled through the secure tunnel, while the communication server is protected by a firewall. If it is necessary to push down a patch or update, however, the secure connection can also be used to give access to technicians remotely.

This centralised approach to security provides operations with the ability to define, automate and monitor security policies across the SCADA environment, providing increased visibility, reliability and compliance. The business can centrally define plant-wide policies, confidently deploy them and automate their execution and monitoring. It ensures security of all remote field assets from a single operations centre.

Any serious application needing real security will start there, but then add additional layers of security, commonly referred to as defence-in-depth methodology (Figure 1). These layers are meant to slow down attacks to give intrusion detection software time to identify the threat and trace it back to its source.

FRAMEWORK CORE	
Functions	Categories, Subcategories, Informative References
Identify	• Automated asset discovery and inventory • Policy management
Protect	• Automated path + AM delivery • Secure remote access and data transfer
Detect	• Monitor and log collection • Scan ports and services against whitelists/blacklists • Compliance reporting
Respond	• Secure remote access by cybersecurity experts
Recover	• Multi-site file transfer infrastructure for backup/restore

Table 1: Compliance with the NIST Cybersecurity Framework.

From the edge to the centre

The next step is to secure communications between edge devices to the data centre. This all starts with the edge device. This is usually an RTU, PLC or, in some cases, a computer. Ideally, you start with an edge device certified to ISA Secure Level 2 which generally includes secure boot, authentication and data encryption. Compliance with the standard is overseen by the ISASecure program, run by industry consortium ISA Security Compliance Institute (ISCI). An easy-to-use control software using programming languages like IEC 61131- can be used to sift through all the data and determine what's important enough to send to 'HQ'. One simple example is that you may be reading all the diagnostics data for all your local devices but only send data for devices which are outside of normal operational parameters.

Reliability can be enhanced using local data storage, so nothing gets lost if your communications link is lost. This is extremely important when using cellular, radio or satellite communications.

Secure communications can be accomplished with VPN technology and today's more secure protocols like DNP3, IEC 61850 and OPC UA, which is the latest and appears to offer the most security and functionality of the group. AMQP and MQTT are transport-focused technologies and can be added to these protocols to go from point-to-point communications to a publish-subscription (pub-sub) model, where one stream of data can be made available to multiple users.

Most solutions today will use point-to-point communications to load all the data into a large database where it can be organised and provide highly efficient historical trends or views of data originating from multiple locations. This centralised approach would then have data mirroring and automated backup processes to secure the data — usually across multiple sites with disaster recovery functionality.

Securely disseminating actionable information

Once you get your data into the cloud, you want applications that turn the raw data into something you can use to improve your business. This typically means the flexibility and power to graphically bring your attention to abnormal trends or events.

Security is not only about keeping external threats out of your business, it is about making sure the information can be trusted while empowering the authorised users to improve company performance. The next step therefore is to secure the more valuable information flowing between the data centre and those end users who may be driving between sites, managing operations of multiple sites from a remote operations centre, working from their office or even from home using their phone or tablet to assess the current situation. This is typically done with encrypted tunnels or VPN connectivity.

As mentioned earlier, control or write functionality can be limited to specific users who have been trained to understand what their actions on the keyboard can do at a site thousands of miles away. It's a great productivity tool to greatly reduce travel to distant sites. It enables collaboration with expert users to fully understand unusual situations. The system protects us from ourselves by requiring user authentication. A user name and password may be enough for low-level, read-only access but multifactor authentication may be required for write control of remote sites or sensitive financial data.

Summary

Combined with a top-down security management platform the architecture described above can be used to deliver robust ICS security following the NIST Cybersecurity Framework. This voluntary framework defines industry standards and best practices to help organisations manage cybersecurity risks. Combining centralised control with the security management platform gives businesses the ability to consistently meet these standards across sites (Table 1).

Existing manual security processes such as patching do not scale well; SCADA in the cloud can centralise and automate these, while bringing consistency, visibility and control to cybersecurity across the enterprise.

SCADA in the cloud offers significant benefits, but concerns over security could stop these from being realised. They shouldn't. With a suitable architecture and security, businesses can enjoy the benefits of cloud deployment while not just maintaining their security, but actually enhancing it.

Honeywell Process Solutions
www.honeywellprocess.com

SWITCH SOFTWARE UPDATE FOR TSN

Belden has released version 7.3 of its Hirschmann Operating System (HiOS). The software update enables Time-Sensitive Networking (TSN) support with an 802.1Qbv time-aware scheduler. Now, users can achieve predictable latency and greater reliability by allowing dedicated time slots to be available for real-time data on every device in the Ethernet network.

Key benefits from the upgraded HiOS 7.3 software are said to include reduced operating costs because separate networks for time-sensitive and non-time-sensitive data are not required; enhanced network efficiency since new TSN protocols can be added to the system over time; and optimal network performance given both time-critical and non-time-critical devices can hook up to the same network without latency concerns.

Hirschmann's HiOS system is designed to be suitable for any industrial setting that uses time-sensitive data and requires immediate, reliable communication between devices, especially for machine-to-machine communication and motion control applications. The software's comprehensive security features also make it suitable for use in high-risk industries, such as power transmission and distribution, oil and gas, general manufacturing, automotive, transportation and mass transit, rail-rolling stock and aerospace markets.

The TSN-enabled software is available for download through the Belden website or help desk system for existing users of RSPE 35/37 or OCTOPUS switches with a field-programmable gate array (FPGA).

Belden Australia Pty Ltd
www.belden.com

NETWORK MANAGEMENT SOFTWARE

Hirschmann has released an updated edition of its HiVision software to manage networks. Now available from Control Logic for new customers and through its annual maintenance program for existing users, Industrial HiVision 8.0 adds more capabilities. In addition to bug fixes and security enhancements, HiVision 8.0 includes a tool to configure Time-Sensitive Networking (TSN) technology, which combines the large bandwidth capabilities of Ethernet based on IEEE 802.x standards with the determinism of a real-time fieldbus.

Users are able to visualise TSN schedules and monitor TSN operations. The upgraded software improves the functionality of the MultiConfig tool, providing the ability to configure multiple devices at once inside industrial networks.

Industrial HiVision is suitable for any organisation that requires simple and comprehensive visualisation for fast fault finding and device replacement, management of network assets utilising SNMP or EtherNet/IP, or centralised configuration and firmware deployment.

Control Logic Pty Ltd
www.controllogic.com.au

VIBRATORY CROSS FEEDER

Greater production demands within the packaging industry has led to the efficiency of the multi head weigher increasing. Due to this as well as the demand to handle a wider range of product types, the flow of product to the weigh head is critical. A greater emphasis is also being placed on the hygienic aspect of equipment coupled with reliability and ease of maintenance.

Enmin's Vibratory Cross Feeder bridges the gap. Vibratory equipment within the food and allied industries is recognised as a desirable approach to convey and meter products. The cross feeder employs standard Enmin LD electromagnetic vibratory drives to convey product and accurately control feed rates.

As the LD electromagnetic drives are electronically controlled, a variety of controllers are available to ensure flexibility and the ability to achieve the optimal conveying output required.

Hygiene, minimal maintenance and reliability are high on the list for food processors, with hygiene naturally critical when processing food products. The vibratory cross feeder delivers in all three of these areas.

Investment costs are also ever present so the company ensures a close working relationship through the design, approval, manufacturing and installation process in order to guarantee the correct solution is delivered.

The company ensures its equipment is able to be easily integrated into any production line without operational glitches.

Enmin Pty Ltd
www.enmin.com.au

DRONE-BASED GAS LEAK DETECTION

The ABB Ability mobile gas leak detection system benefits from drone deployment as it is said to enable faster identification of leaks, require less man-hours to implement and cover wide, hard-to-reach areas. To avoid false readings, it can distinguish between biogenic methane, the source of which is ruminant animals, manure and shallow coal and oil deposits, from thermogenic methane from natural gas.

The solution uses cavity-enhanced absorption spectroscopy to detect methane and ethane with a sensitivity more than 1000 times higher than conventional leak detection tools. Off-axis integrated cavity output spectroscopy (OA-ICOS) has extreme sensitivity that allows ABB to quickly identify potential methane emissions at a greater distance while flying, which is not possible with other sensors.

ABB's analysis software automatically processes the collected methane, ethane, GPS and wind data to create a simple, easy-to-use report in either GIS compatible or PDF formats. These reports can be used to quickly identify areas in the pipeline network that potentially have leaks.

Additionally, the software features, such as the ABB Ability cloud storage tools, allow quick and efficient distribution of data and reports to all stakeholders anywhere in the world. Authorised users can view the progress of flights in real time as well as review and act on processed leak reports.

The mobile gas leak detection system is also used in urban distribution vehicles and handheld inspection devices, meaning that all three methods of gas detection can be deployed in conjunction with one another.

ABB Australia Pty Ltd
www.abbaustralia.com.au

ETHERCAT SLAVE I/O MODULE

A member of the ECAT-2000 series of modules, the ECAT-2011H from ICP DAS comes equipped with the EtherCAT protocol and can be installed in daisy-chain connections, allowing flexible device installation and reducing infrastructure and operation costs. All ECAT-2000 modules can be deployed in network topologies such as star, line or ring. Further, the isolated input and output design of the ECAT-2000 series protects these modules from harmful interference and environmental disruptions.

The ECAT-2011H has eight isolated differential input channels or 16 single-ended input channels built in, which can be selected via software. Users can obtain the status of the input through the ECAT-2011H's process data. Finally, the ECAT-2011H has passed the EtherCAT conformance test tool for protocol compliance, ensuring an eligible EtherCAT master or configurator can operate it and implement various applications with ease.

ICP Electronics Australia Pty Ltd
www.icp-australia.com.au

PLASTIC HOUSINGS

The Heavycon EVO M1 plastic housings from Phoenix Contact accommodate a modular contact insert and are smaller than a B6 interface.

The single-module housings also feature a swivel cable gland with bayonet locking. This reduces warehousing by 70% and increases flexibility.

In combination with two EVO cable glands, four housing variants can be created from one sleeve. The cable outlet direction only needs to be defined when the cable gland is snapped on. The panel mounting base and sleeve housing are interlocked via a single locking latch.

The housings are suitable for all standard single modules. Data, signals or power can be transmitted conveniently via a single compact interface. The plastic housings meet IP66 degree of protection and are shockproof up to IK09.

Phoenix Contact Pty Ltd
www.phoenixcontact.com.au

3-IN-1 BIOGAS MEASUREMENT INSTRUMENT

Vaisala has introduced an in situ 3-in-1 biogas measurement instrument, the Vaisala MGP261, for measuring methane, carbon dioxide and humidity in demanding environments. The compact measurement instrument is Ex certified up to Zone 0, which enables inline installation in explosive atmospheres.

The MGP261 is based on Vaisala's CARBOCAP infrared gas measurement technology and is optimised for biogas production processes, such as anaerobic digestion of waste from agriculture, industries and municipalities, and the utilisation of landfill gas.

The instrument offers real-time gas composition without sample extraction or treatment. Due to its stable methane measurement, the compact instrument helps biogas plant operators gain comprehensive control over their process and optimise their combined heat and power (CHP) engine performance. The instrument also enables operators to control humidity in order to reduce wear in the CHP engines and process components.

The product is easy to use and install, and it can be fitted to any existing system. The in situ installation of the instrument makes sample treatment unnecessary, enabling measurements without any sampling lines, pumps or moisture removal traps.

The instrument design is resistant to chemicals and the robust metal body is IP66 rated. Furthermore, the operating principles of the instrument mean that no calibration gases are needed in routine operation and Vaisala's background auto-calibration function reduces expensive calibration work.

Vaisala Oyj

www.vaisala.com/en/

IoT WIRELESS GATEWAY

Turck's TCG20 Series universal IoT wireless gateway is specially tailored for the requirements of industrial automation.

Three wireless variants are available: with UMTS, dual-band Wi-Fi as well as simultaneous UMTS and Wi-Fi. On the wired network side, the TCG20 Series offers a serial RS232/RS485 port, a CAN port and up to five Ethernet ports. Besides CANopen, the devices also support Modbus TCP as well as Modbus RTU as master and slave, OPC UA as a client and server as well as Codesys network variables.

The integrated web server enables the gateways to be configured online using clearly designed graphical menus and also without any programming knowledge. An EDGE-PLC Editor manages simple controller tasks and also the preprocessing of data for cyclical or event-driven data transmission. Mobile phone network costs in UMTS operation are thus kept within reasonable limits.

Turck Australia Pty Ltd

www.turck.com.au

PLANT DEVICE MANAGEMENT

Many plants struggle to manage thousands of devices in complex and often out-of-date plant device structures (hierarchies) — often using long, disorganised lists that make it hard to find and identify critical devices.

The latest release of Emerson's AMS Device Manager is designed to provide better organised data for the management of field devices. Embedded tools allow project and operations teams to customise plant device hierarchies, project tracking and device alerts.

AMS Device Manager's bulk transfer functionality provides the tools to configure whole systems automatically — including set-up of device alert monitoring and plant hierarchies. Users can export a tag list and open it in a spreadsheet application to enter a location and alert group for each device. Then, using bulk transfer, users can set up the system with a properly populated hierarchy and alert monitor. With a correctly defined plant hierarchy, maintenance teams can visualise device data in targeted views.

With the updated AMS Device View — the browser-based interface for AMS Device Manager — maintenance can assign devices to specific projects and track them on separate project dashboards, avoiding the distraction of alerts flooding the operations dashboard.

The latest version of AMS Device Manager also offers system-wide automated locking of devices. Organisations can protect against unauthorised changes to devices without relying on physically adding or removing jumpers. Customisable software-based locks can be enabled for select personnel for specific amounts of time, after which the system will automatically relock the devices to ensure that device configurations are protected.

Emerson Automation Solutions

www.emerson.com/au/automation

SELECTING A PROCESS MANUFACTURING ANALYTICS SOLUTION

FIVE QUESTIONS TO ASK

The large gap between data and insight in process manufacturing will only start closing when data analytics vendors start putting the process engineer first.

Process manufacturing organisations run on data — from a manufacturing, operations and business perspective.

The data generation and collection strategies at the centre of manufacturing processes have evolved dramatically, especially in recent years. Process manufacturers now collect and store huge volumes of data throughout their operations, both on and off premise, across multiple geographic locations, in an increasing number of separate data silos.

These advances have coincided with the proliferation of connected sensors and increasingly inexpensive storage, leading to an Industrial Internet of Things (IIoT) projected to generate more than 4 trillion gigabytes of data per year by 2020, according to IDC Research.

Data analytics solutions have a huge positive impact on the growing volumes of data in many sectors, from retail to finance. So why aren't these solutions widely leveraged in process manufacturing? With so much data and the promise of so many new technologies, why is it so difficult to apply these technologies to process manufacturing and gain the same benefits as other sectors?

Why do process manufacturing organisations still feel like they have too much data and too little insight?

This gap — between the data process manufacturing organisations have and the insights achieved — exists because some data analytics solutions fail to completely grasp the unique challenges and opportunities presented by process manufacturing. Aggregating data from different sources (eg, process historians, sensors) is especially challenging for analytics solutions that were not developed specifically for process manufacturing.

When we talk about data analytics solutions, we mean any software enabling process engineers or scientists to:

- create a cleansed, focused data set for analysis through assembling, aggregating or wrangling data from various sources, including data historians, offline data, manufacturing systems and relational databases;
- investigate operations data using 'self-service' tools to rapidly analyse alarm, process or asset data for ad hoc or regular reporting;
- publish or share insights and reports across the organisation to enable data-driven action or enable predictive analytics on incoming data.

Many data analytics solutions claim to offer some or all of these things — with the goal of finally closing the gap between data and insight. But are they successful, and what are the criteria that determine success?

In this article are five questions every process manufacturing buyer should ask when evaluating a data analytics solution.

Finally, process manufacturing data is hard to navigate. Sensors have timestamps that need to be aligned and aggregated across specific ranges in time. It is difficult to get answers to even the simplest of questions and overcome hurdles that transaction data doesn't have.

What is needed

Many analytics, reporting and industrial control systems can present data, but process manufacturers have far fewer options for solutions that can coordinate and aggregate data in helpful ways. In your evaluation, you should consider how easily the analytics solution makes it for users to select an appropriate time series for analysis and synchronise input from various control systems, sensors and other sources (which may report at different intervals) to present an accurate view of activity within the specified time window.

An analytics solution should do the heavy lifting of synchronising time-series data from different sources so your specialists have a clear, accurate data set to work from. The solution should not require them to download data from different systems (control systems, databases, sensors, spreadsheets etc) and coordinate it by hand in spreadsheets before any meaningful analysis can begin. It should also support the most useful analysis and output formats for time series data, such as pattern search, value search and scatterplot charts.

2. Does the analytics solution rely on your experts or its experts?

Why it matters

Beware of experts bearing correlations. Many data analytics vendors know their own technology extremely well, but don't know much about process manufacturing. For example, an analytics solution might tell an oilfield operator that production is diminishing at a specific well, but would not point the operator to check a specific asset, which an industry-focused solution could do. Lack of process or vertical expertise can lead to a focus on the analytics themselves rather than the implications of any findings — and, in turn, an emphasis on correlations over outcomes.

The key to positive business outcomes for process manufacturers is empowering subject-matter expert employees. A typical process manufacturing organisation has a great deal of expertise at its disposal, spread out across different roles including skilled process engineers, analysts, architects, team leads and other technical specialists.

These experienced frontline users often have decades of experience, detailed knowledge of the company's processes and history, situational awareness of its operations and fluency in plant assets, sensors and tags. They have the advanced technical education and experience to ask smart, productive questions.

Unfortunately, these employees are often limited by an ageing suite of software tools, most of which were originally created in the mid- to late-1990s. They know the right questions to ask — but using existing data analytics tools to answer those question can be difficult and time-consuming, approaching impossible in many cases.

1. Is the solution designed specifically for process manufacturing, and can it handle time-series data and solve intricate process manufacturing problems?

Why it matters

Anyone who works with process manufacturing data knows it isn't like other data. No matter the industry — from pharmaceutical to mining to oil and gas — the data produced and the assets involved present a tangle of convoluted relationships and contextual challenges.

Whether you're looking at a refinery, a production line or a wind turbine farm, there are historians collecting data across many different protocols used by multiple vendors across a disparate array of equipment, all of varying ages and implementations.

These systems are typically producing data at speeds and volumes that other industries would find dizzying, and at uneven intervals that can confound conventional analytics solutions. All this data also needs to be cleansed to be useful.

To make matters worse, all these events and signals lack the associated context to make them meaningful on their own — a problem that is further compounded when assembling data from multiple sources which requires the addition of these key relationships.

" ANALYTICS SOLUTIONS FOR PROCESS MANUFACTURING SHOULD PUT POWER INTO THE HANDS OF THE PEOPLE WHO CAN MOST EFFICIENTLY CREATE THE MOST POSITIVE OUTCOMES.

What is needed

Packaged analytics solutions won't know more than the process engineers and quality specialists that focus on your operations every day, and they shouldn't pretend to. Instead, data analytics solutions should make it easy for your specialists to access and work with the data they need so they can apply their particular expertise.

Process engineers excel at solving problems and driving incremental improvements by studying how slight changes impact performance. Solutions that save time by helping engineers isolate variables will return tremendous value because users can focus on making changes and modelling results, instead of collecting, coordinating and preparing data.

Analytics solutions for process manufacturing should put power into the hands of the people who can most efficiently create the most positive outcomes by providing productivity tools and features to help them assemble, cleanse, search, visualise, contextualise, investigate and share insights from process data — all without involving IT experts.

If you give the right tools to the right people, you can immediately see positive results.

3. Is the analytics vendor more focused on the problems being solved or the technologies involved?

Why it matters

We're in the midst of an overwhelming wave of innovation that includes software innovation with big data, hardware innovation highlighted by highly scalable, on-demand computing architectures and cognitive computing innovation marked by ongoing advances in machine learning. These rapid advancements have led to two big problems for anyone trying to compare analytics solutions for process manufacturing organisations.

First, emerging technologies — big data, predictive analytics, machine learning, cloud computing and others — have eclipsed the narrative of benefit and impact. The capabilities of these technologies have surpassed our understanding of the best way to get value from them. Rather than discussing why we should adopt a particular innovation, the conversation focuses too often on what technology to use, often with more enthusiasm for the technology than the actual benefits.

Second, the sheer pace of recent innovation means there has been too little focus on fitting new offerings into existing environments. Technology generations used to last decades, now it feels like months. Many companies get lost in the fog of technology discussions instead of focusing on end results and engineers don't necessarily want technologies, they want insight and solutions. Technology is just one resource (an important one) that gives engineers the insight they need to make improvements.

What is needed

The world of big data, predictive analytics, machine learning and cloud computing needs to be turned inside out — from a technology-centric revolutionary approach to a user-focused, problem-solving evolutionary approach.

Engineers can't just start by 'grabbing a bunch of sensor data' — it isn't a trivial task. It's also often the start of a longer process that involves cleansing, adding context and performing calculations — a process that needs to leverage the hard-won insights and institutional knowledge of engineers.

Analytics solutions for process manufacturers should fit into existing information system infrastructures and enhance them rather than forcing the enterprise to continually catch up to adapt the latest technology. Process control systems, historical production records, ERP systems and specialised applications and processes are at the heart of your business. Process manufacturers need analytics solutions that can easily fit into these environments through interfaces to their existing systems and enhance their value by extending their functionality and allowing the data they collect and produce to be easily used and shared in new ways. It is better to leverage existing investments than to continuously make new ones.

4. Does the analytics solution require you to move, duplicate or transform your data?

Why it matters

Contextualisation has always been difficult with process data, often requiring manual effort and painstaking work in Microsoft Excel to define relationships between relevant data. Historians have come a long way in terms of trend viewing and investigation, but 'Export to Excel' is still every historian's most important feature for doing the 'real work' of data aggregation, context and modelling.

For example, a pharmaceutical engineer might have several hypotheses to explain a bad batch outcome, ranging from an error by a particular operator to a bioreactor maintenance event to a specific raw material variation. The data exists to validate these hypotheses, but it requires bringing together disparate databases, often across multiple data silos, and then creating context to evaluate the data.

This contextualisation process goes by many names — including data wrangling, data harmonisation and data blending — but for many analytics solutions, these tasks still require manual data transformation and duplication. Duplication adds hidden cost to the environment by increasing storage requirements and bandwidth consumption.

What is needed

Users achieve meaningful results when they can focus on data analysis instead of data collection and processing. Analytics solutions for process manufacturers should easily aggregate data from disparate sources and perform the complex calculations needed to synchronise data points that were collected at different intervals. It should also allow engineers to contextualise data without getting IT or other experts involved, without duplicating or transforming the data and without creating additional data lakes.

5. Can the solution help your engineers work as fast as they can think?

Why it matters

Engineers typically look at data for a specific reason. For example, because an alarm went off in a system, or someone has asked a question or they need to generate a report. Traditional analysis tools often require specialised skills or syntax, so these tasks can be difficult and time-consuming — and the tools are typically only mastered by a few people within an organisation.

Beyond the struggles of individual users, few tools are built around collaboration and organisational knowledge capture. When one user cleanses data for a project or creates context and relationships among data sources, that analysis and information is often lost, with no way for other users to discover or leverage it.

What is needed

Data analytics solutions should be flexible enough to support both real-time collaboration and existing workflows. Engineers should be able to interact with tools spontaneously, as quickly as they can create tasks or devise hypotheses. The user interface should allow Google-like searches instead of requiring users to learn a new environment.

Insight gains value when it is shared. For example, one person might know a certain set of process data really well, and they know how to clean and transform that data, while another person might know the ERP system really well, and another might be an expert with maintenance systems. Analytics solutions should make it easy for engineers to distribute their work and provide a central place where employees can work together to leverage each other's expertise and information.
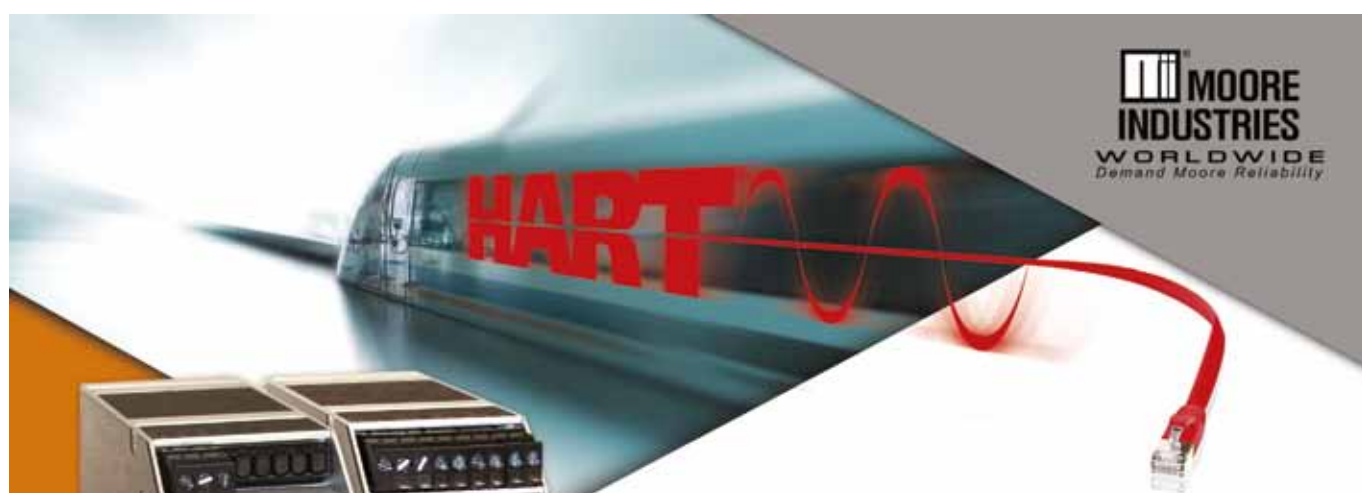
Conclusion

Presumably, the goal of any analytics solution is to improve outcomes in yields, margins, quality and safety. So, any data analytics solution should be drawing from all of these recent technology advancements to accomplish those outcomes — without your organisation having to enlist expert assistance or know exactly how these underlying technologies work.

The large and growing gap between data and insight in process manufacturing organisations will only start closing when data analytics vendors start putting the process engineer and analyst, by whatever title, at the centre of the picture. These engineers have the expertise, ability and incentive to ask the right questions and take advantage of insights generated by the answers. Analytics solutions need to unlock process engineering knowledge in a way that is convenient for users.

Seeq Corporation
www.seeq.com

STAINLESS STEEL PANEL PCs

APLEX Technology's FABS-9XXA series of food-safety-grade stainless steel HMIs aims to improve the safety and productivity of the food and beverage processing industry.

The FABS-9XXA series of HMIs features panel PCs powered by 6th/7th Generation Intel Core i3/i5/i7 processors and is available in sizes ranging from 12.1 to 21.5″. The FABS-9XXA is compliant with EN-1672-2, constructed with a default SUS304 or optional SUS316 stainless steel front panel, and rated for IP66/IP69K water protection. The front panel has a special edge design that is formulated to allow water flow through the charmed edge while preventing water seepage into the inner structure of the panel PC for easy and comprehensive cleaning. The adhesive materials used for edge lamination and the HMI's sealing sponge meet FDA 21 CFR 177.2600 for food safety assurance and the touch glass is tested by the SGS group.

Due to its simple installation and panel-mountability, the FABS-9XXA series of HMIs is versatile and can be installed in facilities or equipment with ease. The HMIs are also equipped with strong communication networks and I/O expansion capabilities, capable of conforming to specific requirements while providing flexible connectivity and integration.

The series offers a choice of resistive-touch or projected-capacitive touchscreens with anti-reflection coatings and has a wide-range 9–36 VDC supply input.

Backplane Systems Technology Pty Ltd
www.backplane.com.au

DCS UPGRADE

ABB Ability System 800xA 6.1 provides significant innovations to the entire DCS architecture and introduces technologies that are said to shorten timescales for project execution, reduce the impact of late changes and enhance the scalability of the system, bringing value to capital projects. This is achieved by the introduction of Ethernet I/O solutions, additional High Integrity controllers and a series of engineering tools such as an Ethernet I/O Field Kit, an Ethernet I/O Wizard for field commissioning and the possibility to engineer with signals in the Control Builder.

The Select I/O is an Ethernet-based single-channel I/O that uses xStream engineering to reduce project delivery schedules. Independent teams can work in parallel and then bind together later. This reduces the impact of changes during the project, particularly late changes, and effectively reduces the commissioning time. Pre-tested, standardised cabinets can be wired directly to field devices and eliminate the needs for physical marshalling cabinets, reducing drawings, equipment and labour. Testing efforts and the hardware footprint are reduced as well.

Version 6.1 supports IEC 61850 Ed 2, which means that it is ready for modern digital solutions such as digital substations. System 800xA's hardware is said to be equally effective for small hybrid systems as it is for large, high-availability, integrated automation applications. The modularity of the subsystem results in high return on assets by providing the flexibility to choose the specific functions necessary to meet actual requirements.

ABB Australia Pty Ltd
www.abbaustralia.com.au

HYBRID DRIVE CABLES

For motors from SEW-Eurodrive and Siemens, igus has developed the CF280.UL.H, a hybrid cable specifically for use in the energy chain.

In order to drive motors, many engineers increasingly come face-to-face with hybrid cables. This eliminates the need for cabling with a separate measuring system cable for the encoder. The CF280.UL.H is suitable for applications up to a bend radius of 10x diameters across all industrial sectors. The cable offers a wide operating temperature range of -25 up to +80°C. Depending on the manufacturer's specification, the cable has a black or orange oil-resistant PUR outer jacket, and is coolant-resistant and flame-retardant.

A braided shield with high coverage ensures good EMC protection of the cable over a long service life. The cable series also has American UL approval, as well as the EAC and CTP certificate for the Russian market.

On customer request, igus harnesses all its cables with the appropriate connector in-house.

Treotham Automation Pty Ltd
www.treotham.com.au

MAGNETO-INDUCTIVE DISPLACEMENT SENSOR

Bestech Australia has announced the industry-standard version of its magneto-inductive sensors, MDS45. Combining features of both inductive and magnetic sensors, these sensors provide linear output signal with high temperature stability. The sensors are capable of measuring displacement between 20 and 50 mm. The ranges can be easily adjusted by changing the magnet.

MDS45 sensors have their own robust M12/M18/M30 stainless steel housings with IP69K protection, which makes them suitable for displacement measurement in demanding environments, such as in the food industry. The MDS45 is also available in a flat plastic housing option with compact and flat design for measurement in a restricted area. As the sensors and the magnet can be installed separately, measurements through objects and non-ferromagnetic materials are possible.

The MDS45 is also suitable for dynamic applications with a fast measuring rate of maximum of 3 kHz. It is designed with high-temperature and pressure-resistant materials for measurement in harsh environments. One example of a relevant application is accurately measuring the dosage when filling drink cartons in the factory. The sensor is capable of measuring the valve lift of the filling line which translates to the dosage transferred.

The sensor also provides analog outputs in 4–20 mA or 2–10 V which can be interfaced with an industrial data acquisition system with minimum signal conditioning.

Bestech Australia Pty Ltd
www.bestech.com.au

ROBOTIC SORTATION SYSTEM

Robotics and warehouse automation company GreyOrange has launched its latest modular sortation system, designed for modern distribution and logistics centres serving retail, courier and express companies.

The Flexo modular robotic sortation system is designed to fit well in most warehouses due to its fluidic layouts, requiring minimal additional infrastructure. The AI-enabled robotics system can be scaled to meet evolving business needs to handle large peaks, and reduced during non-peak hours to minimise operating costs.

The system utilises GreyMatter, the company's AI-enabled warehouse execution platform. Capacity can be increased easily with the addition of more autonomous mobile robots (AMRs) as the business grows.

The system's fleet of AMRs carries parcels from inducts — where parcels arrive — to their sort destination, using the most efficient path determined by AI and machine learning algorithms. The robots perform high-speed sortation, similar to a fixed conveyor sorter in conventional sorting systems, with added advantages such as the ability to add sorting capacity during peak periods, faster deployment, easier layout updates, and modular components that can be individually turned off when not in use.

Designed with no single point of failure, Flexo can handle up to 12,000 parcels per hour, including common post and courier items up to 15 kg, sorting up to hundreds of destinations.

Advanced Warehouse Solutions
www.advancedws.com.au

COMMS *2019*
CONNECT

Events for critical communications users and industry

SYDNEY

ROSEHILL GARDENS | **12-13 JUNE 2019**

Public Safety | Transportation | Utilities | Government | Enterprise

SPEAKERS INCLUDE

TONY GRAY
Chief Executive
TCCA

EDWARD PARKINSON
Acting CEO
**First Responder
Network Authority**

**STATION OFFICER
GRAHAM TAIT AFSM**
Operational Communications
Systems Officer
Fire & Rescue NSW

MARY EGAN
National PMO Lead
Public Safety Mobile
Broadband
NSW Telco Authority

PLUS

**500+ users and industry experts | 40+ exhibitors | 30+ speakers | 3 training workshops
2 conference streams | Finnish Critical Communications stream**

TRAINING WORKSHOPS
included in conference package

— **Sensors, smart cities and the implications for critical control rooms**

— **Critical communications standards supporting a multi-vendor and interoperable environment for all mission- and business-critical sectors**

— **ARCIA Professional Development Training workshop — multicoupling**

IN CONJUNCTION WITH
**ARCIA INDUSTRY
NETWORKING DINNER
12 JUNE 2019**
Book with your
conference package or
visit arcia.org.au

Networking
Drinks Sponsor

Wireless Innovation

Media Partner

critical comms

Association Partner

ARCIA

Supporting associations and media organisations

TCCA

THE **CRITICAL
COMMUNICATIONS** REVIEW

IWCE
INTERNATIONAL WIRELESS
COMMUNICATIONS EXPO

IoTA
IoT Alliance Australia

RadioResource
INTERNATIONAL

For more information or to register visit www.sydney.comms-connect.com.au

AS I SEE IT

IO-LINK ENABLES INDUSTRY 4.0 AND REDUCES COSTS

Motivations for flexible manufacturing, efficient production and visibility require that we have more diagnostics and data available for analysis and monitoring. Flexible manufacturing requires that sensors and field devices be able to adapt to a rapidly changing set of requirements. With the parameterisation feature of IO-Link slave devices, we can now send new parameters for production to the sensor, on a part-by-part basis if required.

For example, you could change a colour sensor's settings from red to green to orange to grey and back to red if necessary, allowing for significantly more flexible production. With efficient production, IO-Link slaves provide detailed diagnostics and condition monitoring information, allowing for trending of data and prediction of failure modes, thus eliminating most downtime, as we can act on the predictive data in a controlled and planned way.

Trending of information, like the current output of a power supply, can provide new insights into changes in the machine over time or provide visibility into why a failure has occurred. For example, if a power supply reported a 2 A jump in output three weeks ago, we can now ask, "what changed in our equipment three weeks ago that caused that?" This level of visibility can help management make better decisions about equipment health and production requirements.

In the last year IO-Link has become widely accepted. We have seen installations in almost every industry segment: automotive OEMs, automotive tier suppliers, food and dairy machinery, primary packaging machinery, secondary packaging machinery, conveying systems, automated welding equipment, robot dress packs, on end-effectors of robots, automated assembly stations, palletised assembly lines, steel mills, wood mills and more.

The biggest roadblock to IO-Link becoming even further utilised is a lack of skillset to support automation in the factory, or a wariness of IO-Link as 'being yet another industrial network'.

One of the biggest trends in the development of IO-Link technology is the reduction of analog devices on the machine. With analog signals there are many 'gotchas' that can ruin a good sensor application: electrical noise on the line, poor grounding design, more wiring, expensive analog input cards and extra integration work. Analog signals also introduce the need for unnecessary calculations: for example, a linear position measurement sensor is 205 mm long with a 4–20 mA output tied into a 16-bit input card. How many bits are there per mm? A controls engineer needs to do a lot of mental gymnastics to integrate this into their machine. With IO-Link and a standard sensor cable, the wiring and grounding issues are typically eliminated and, since IO-Link sensors report their measurements in the engineering units of the device, the mathematics are also eliminated. In our example, the 205 mm-long linear position sensor reports 205 mm in the PLC: simpler, faster to integrate and usually a much better overall application cost.

There is no doubt that IO-Link is a major enabling force for Industry 4.0 and smart manufacturing. Major automation players are engaged, promoting and, most importantly, building an installed base of functional IO-Link applications that are well worth a look.

Will Healy III is enthusiastic about smart manufacturing and STEM education. Will has a degree from Purdue University in mechanical engineering and loves sharing his passion for automation. He is published, works as an industrial adviser, and has widely presented on the value that sensors and the IIoT bring to manufacturing.

FREE

to industry and business professionals

IF YOU CAN'T MEASURE IT, YOU CAN'T CONTROL IT
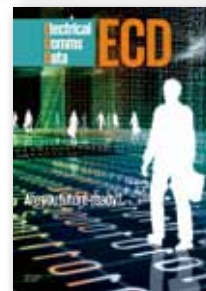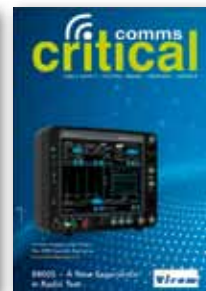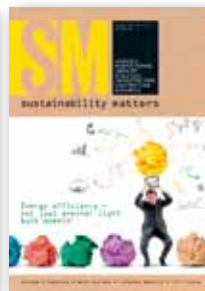
CERLIC SLUDGE BLANKET PROFILE SENSORS

Cerlic
ELETTA GROUP
WASTEWATER SYSTEMS

See the sludge level...

PROVEN NEAR INFRARED (NIR) TECHNOLOGY
- Directly measures total suspended solids concentration (mg/L, ppm or %TSS)
- Choice of 2% or up to 5% TSS (e.g. primary or thickened sludge) models
- Not an indirect, compensated ultrasonic echo or turbidity sensor

FULLY AUTOMATIC (MOTORISED) CBX
- Measure Sludge Blanket & Fluff (unsettled or rising solids) when triggered by rake, SCADA or timer
- Real-time TSS concentration vs depth for full sludge profile
- Continuous 4-20mA or Profibus DP (including temperature)
- Tilt switch for tangle prevention & self-cleaning (cable + sensor) for low maintenance

HANDHELD MULTITRACKER UNIT
- Plug 'n play Sludge Blanket Profile, DO & RAS / WAS (5% TSS)
- Backlight display, datalogging (with PC sync) & alarm points

...rather than trying to hear it!

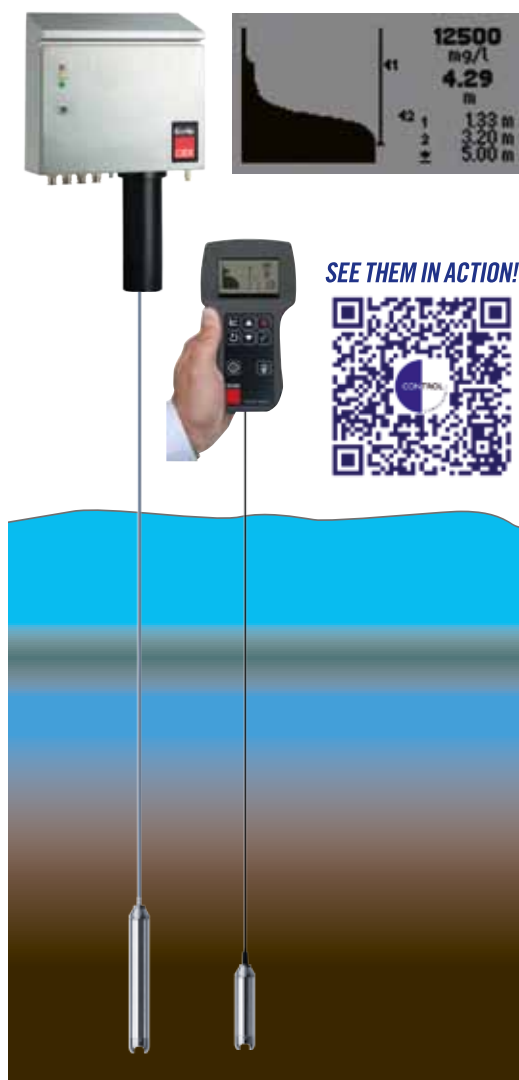**SEE THEM IN ACTION!**

KARI FLOAT SWITCHES

Reliable pump / valve control with multiple level alarms from a single float for tangle free operation

KARI

WEKA MAGNETIC VISUAL LEVEL INDICATORS

- *Custom made locally*
- *+GF+ PVC & PVDF*
- *316SS*
- *Measuring scales & level alarms.*

WEKA®

CCEZY.COM.AU +61 2 9542 8977
Distributors through Australia and New Zealand

Control Components
CONTROL