Ultra-compact IPCs for the Industry 4.0 generation

BECKHOFF
Sensorik 4.0: Smart Sensors. Ideas beyond limits.

Industry 4.0 starts with the sensor or field device. These provide the basic data for the digital networking of plants and production processes in an Internet of Things. With its innovative sensor and interface technologies, Pepperl+Fuchs already enables process and production units to interact intelligently. Be inspired at www.pepperl-fuchs.de/sensorik40
Our cover

The complexity of machines in the Industry 4.0 era places additional requirements on the control components, particularly the need for space-saving devices with higher computing power. In order to meet these requirements, Beckhoff has developed a new series of IPCs, ideal for a broad range of applications. See the cover story on page 4, for more on this new range of ultra-compact devices.
SAIMC at the forefront of the Digital Industrial Revolution in South Africa

The Digital Industrial Revolution (DIR) – aka 4-IR or Industry 4.0 – will profoundly shape our efforts to promote industrial development. The scale, scope and complexity of this new technological revolution will bring experiences unknown to humankind in the form of cyber-physical systems (CPS), where computers, networks and physical processes are integrated. In particular, when compared to the previous industrial revolutions, the DIR is occurring at an exponential pace (IPAP 2018 – 2021, the DTI).

What will the nature of automation be in the future? And how well is the South African manufacturing sector prepared to meet these new challenges? The SAIMC (Society for Automation, Instrumentation, Measurement and Control) is actively addressing these and other challenges through its involvement in the adoption and implementation of Industry 4.0 to the benefit of the South African economy.

The SAIMC was established in 1957 as a non-profit organisation to act as a catalyst between industry and education. Today, its mission is to provide guidance with respect to education, training and automation thought leadership that is appropriate to current and future industry requirements. It is also involved in the recognition of automation as the 10th engineering degree, to provide an avenue for students into Industry 4.0 or the IIoT.

The Digital Industrial Revolution or Industry 4.0 talks about the usage and impact in an industrial environment of the Internet of Things, Data and Services. Decentralised intelligence helps to create object networking and independent process management, with the interaction of the real and virtual worlds representing a crucial new aspect of the manufacturing and production process.

Industry 4.0 represents a paradigm shift from ‘centralised’ to ‘decentralised’ production, made possible by technological advances that constitute a reversal of conventional production process logic. Simply put, this means that industrial production machinery no longer simply ‘processes’ the product, but rather that the product communicates with the machinery to tell it exactly what to do. Industry 4.0 connects embedded production technologies and smart production processes to pave the way to a new technological age that will transform value chains and business models through the concepts of the ‘smart factory’.

The South African perspective

Many business leaders believe that South Africa holds the potential to re-establish a leading role in the global economic environment. Hence the South African Government launched an initiative to step into the digital revolution through its Industrial Policy Action Plan (IPAP). The DIR will enable a growth policy allowing the country to improve its competitiveness, resulting in an upswing of the economy. However, some serious challenges need to be dealt with to make effective use of this opportunity, namely:

- Infrastructure: a solid Internet and communications network.
- Education and training: a need to educate lecturers and students on how to skill and re-skill new and existing workforces.
- Market structures: understand and adopt the change in different market structures and the interaction between them (primary vs. tertiary).

The South African economy is unbalanced through the scarcity of companies in the SME sector. Big business cannot solve the country’s unemployment problem on its own. In the developed world, for example, the SME sector is responsible for a much higher portion of GDP, therefore providing a healthier economic platform. However, with the right strategic cooperation, South Africa could revitalise its manufacturing industry and SME sector through digitalisation and the application of Industry 4.0 or the IIoT.

As a country, we have the opportunity to become an early adopter on the African continent. We should use it to leapfrog our competitors through unique, locally developed, high-tech products and services. These market changes are happening fast and might be disruptive in some domains. However, they offer the opportunity to revitalise the way we do things. Manufacturers need to adjust their infrastructures and develop new ones, upskill their workers and reorganisation their businesses. We need to attract the right digital talent/skills and (re)train and develop the existing workforce to understand and operate the new and smart technologies.

The Digital Industrial Revolution offers a huge opportunity for South African manufacturers to reinvent themselves and become more successful and competitive in local as well as global markets. The SAIMC is an active participant in this process of economic and technological transformation.

Marc Van Pelt,
Manager Industry 4.0 Task Team
IoT is not about technology it is about business strategy. To take your business into the future, speak to our innovative team to understand what our world-leading technology can deliver. Be an intelligent, interconnected business. Go beyond digital.

- Overall Winner & Best Commercial Solution 2017 MTN Business IoT Awards
- IT Personality of the year finalist 2017
- 2016 Gartner Aspiring Innovator
- Da Vinci TT100 innovation finalist 2016
- Microsoft Gold Partner: Data Platform
A new path appears for modular and IoT-capable machines and systems.

Ultra-compact industrial PCs: a new generation of devices for challenging automation, visualisation and communication tasks.

As machines and systems become more modular and control cabinets smaller, the space requirements of control components are increasingly scrutinised. At the same time, ever more complex and sophisticated machines require more computing performance. However, there are also more cost pressures in the field of automation. In order to meet all these requirements, Beckhoff has developed a new series of ultra-compact Industrial PCs (IPCs) – starting with the C6015 and leading to the high-end C6030. These devices are ideal for a broad range of applications, including environments with decentralised architectures and today’s IIoT and Industrie 4.0 applications.

The new series of ultra-compact IPCs premiered with the C6015 at the 2016 SPS IPC Drives trade show in Nuremberg. Equipped with an Intel Atom CPU, it is well-suited for all kinds of automation, visualisation and communication tasks in the medium performance range. Measuring only 82 x 82 x 40 mm, the ultra-compact and industrial-strength multi-core IPC is only one-third the size of the C6905, previously the smallest control cabinet IPC in the Beckhoff portfolio. With price savings of approximately 25 percent, the C6015 ranks far below the previously lowest-cost x86 IPCs from Beckhoff. With exceptional installation flexibility, it also opens the door to application areas that were previously closed to IPC technology because of cost or space limitations.

The four factors of a true success story

The ultra-compact C6015 IPC was a true success from the very start. It has already been deployed in a wide range of applications in high volumes, including many large-scale projects in Germany and abroad. The concept of the new IPC generation impressed users for several reasons:

• The most important and obvious feature of the C6015 is the extremely compact size that does not compromise suitability for industrial applications. This is underscored by a design with passive cooling and long-term availability in a robust aluminium and zinc die-cast housing. It also meets all other industrial requirements, such as an expanded temperature range from 0 to 55°C and exceptional vibration and shock resistance.

• Combining high computing power with low energy consumption, the C6015 leverages Intel Atom CPUs with up to four cores, providing the ideal basis to handle all applications in the low to medium performance range.

• The exceptionally flexible installation concept permits vertical or horizontal back wall installation in control cabinets. Moreover, with its symmetrical cooling fins, the C6015 can be positioned freely within the mounting frame. Features like these and the free orientation of the connector level, with all connectors on a single side, allow a wide range of installation scenarios that accommodate all incoming cable feeds in even the smallest spaces. In the past, this was often impossible, precluding the use of an industrial PC in certain machine designs.

• The features and interfaces of the C6015 are also designed for a wide range of applications with a 30 GB M.2 SSD, 2 GB of DDR3L RAM (expandable to 4 GB), one DisplayPort, one onboard dual Ethernet adaptor with 2 x 100/1000Base-T connectors, one USB 3.0 port, and one USB 2.0 port.
Overall, the C6015 is likely the first IPC on the market to offer such a high-performance density paired with all the interfaces needed in machine design.

**C6015:** popular for use as an IoT gateway
Beyond its typical use case as control hardware for automation and visualisation tasks, the success of the C6015 is also largely based on IoT applications. About half of the devices installed to-date are being used for communications purposes in IoT applications. These may include something as simple as the collection, processing and provision of process data or more complex tasks that are typical of an IoT gateway. The Microsoft Azure certification of the C6015 underscores that it is an ideal device for Industrie 4.0 applications. The C6015 is well-matched for such communication tasks, including connectivity with legacy systems, because it makes it easy to add IoT capabilities to existing machines and get them ready for future communication requirements, either as an IoT gateway or a basic data collection device.

**C6030:** Building on a successful concept with high-end computing power
Beckhoff is continuously adding models to its family of ultra-compact and flexible industrial PCs. At the 2017 SPS IPC Drives trade show, for example, the company unveiled the high-end C6030 with processors from the most advanced performance class. This is because the innovative concept introduced with the C6015 also quickly impressed users with automation, visualisation and communication applications who have requirements that go beyond the medium performance range.

The C6030, which is also Microsoft Azure Certified, advances the design of the C6015. In addition to dual-core Intel Celeron and Pentium CPUs, 6th and 7th Generation Intel Core i-processors are available. This is possible because of a new cooling concept based on a durable speed-monitored and controlled fan with dual ball bearings. With dimensions of 132 x 132 x 67 millimetres, the computer is nearly half the size of the closest comparable C6930 control cabinet IPC. The C6030 also offers more standard interfaces even in the basic configuration: an onboard Ethernet adaptor with four 100/1000Base-T connectors, four USB 3.0 ports, and two DisplayPorts. It also features two easily accessible slots for M.2 SSD drives (incl. RAID). Depending on the selected configuration, the C6030 costs up to 34 percent less than a comparable IPC from the C69xx family.

With processors ranging up to the Intel Core i7 with four cores running at 3.6 GHz and the Core i3 with two cores running at 3.9 GHz, the C6030 delivers what may be an unprecedented level of performance in such a compact format. As a result, the successful concept of ultra-compact Beckhoff IPCs has now become available even for very large and complex machine control applications. This can include CNC, XTS and HMI applications, multi-axis control, as well as applications with extremely short cycle times and large data volumes. For legacy equipment, the C6030 can serve as a powerful replacement in control platform retrofits and go well beyond the capabilities of alternate systems. With such a high level of performance, the C6030 can easily handle all machine automation and visualisation tasks as well as all IoT operations. Just like the C6015, the user benefits from an exceptionally flexible installation concept with vertical and horizontal back wall mounting and totally free positioning of the IPC within the mounting frame.

For more information contact
Michelle Murphy, Beckhoff Automation, +27 (0)11 795 2898, michellem@beckhoff.com, www.beckhoff.co.za
The early morning air was still cold when I arrived together with a colleague at the mine for our underground visit. Our hosts were keen to show us the practical challenges of the drilling and blasting operation, and the many ways in which rock fragments containing ore are removed to the surface for processing. At the ore face the drilling process was indeed an eye opener, hot, uncomfortable and hazardous in nature. Knowing where to drill to optimise the blast pattern is a skilled operation. When drilling started it was immediately apparent that this was a manual operation, and there was a lot that could go wrong.

Our visit was more than curiosity. Our team was interested to see how augmented reality might be used to improve the drilling procedures, while at the same time enhancing safety. Could an augmented reality display be used to help analyse and superimpose the most efficient layout of the drilling pattern on the rock face for marking the holes? Could a virtual/ augmented reality device such as Google glass or Microsoft Hololens be practically used in such a harsh industrial environment? If so, what might a future system look like? At the time, the technology was still immature, but the potential benefits were compelling enough to warrant further investigation.

This underground visit took place over five years ago and since then there have been many important developments in augmented reality technologies. Significant investments have been made by the vendors in hardware and software. New innovations in heads-up displays now make many suitable for use in industrial environments. These displays, together with artificial intelligence and cognitive technologies, promise to be a game changer in the way operators will work in future.

What is augmented reality?
As the name implies, augmented reality is the addition (or augmentation) of the physical world with context aware visual information that can be used to help operators make better decisions, or help guide their actions. The visual information is usually text, a 2D drawing or a 3D model, object or hologram, which is overlaid onto the physical world.

In the control room environment augmented reality can be seen as an evolution of the human machine interface (HMI). Until now, HMI design in a control system has largely been concerned with designing the best ‘mimics’ (graphical displays representing the process). With new augmented reality technologies, we can now move out of the control room and support field operators and maintenance technicians with real-time process information in the field.

Fundamentally, the same design considerations that apply to good control room HMI also apply to augmented reality systems. Remember that the goal is to provide additional information to improve decision making.
making, not replace human judgement or take away responsibility for decisions or actions taken. In practice, this can be a delicate balance that presents a number of problems which we will cover later.

**Practical applications**

In industrial manufacturing there are many practical examples of augmented reality applications. The business goal is often to reduce costs, improve productivity and enhance safety.

**Complex procedures**

In complex assembly or maintenance procedures, augmented reality can help you with a visualisation of the right way to assemble or disassemble a piece of equipment. The display can provide quick access to visualisations of the task at hand based on 3D models that provide a technician with step by step instructions.

**Quality assurance**

Augmented reality technologies can be used to inspect items of equipment in the field for quality control purposes. The actual item can be compared with a reference image and AI techniques used to indicate a pass/fail when any defects are detected.

**Expert support**

Human experts can remotely assist field technicians with complex tasks by monitoring the work being done through a camera and providing guidance on complex procedures. This can be particularly useful where expert skills are scarce and not located on site.

**Navigational aid**

Augmented reality systems can assist in locating people and equipment in the field with context aware navigational information. This can be useful in certain environments where the location of equipment is not static, visibility is poor, or perhaps to help people navigate through complex or inaccessible plant areas.

**Safety support**

Augmented reality systems can identify elevated safety risk to warn people working in the field. This elevated risk can be determined by a visual analysis combined with data from the DCS/scada, IIoT devices and the maintenance/work permit systems.

**Tracking**

The location of people can be tracked through IoT devices and this information presented on an augmented reality display to improve coordination and productivity of teams in the field. This could be particularly useful in highly regulated or hazardous plants, as well as for supporting rescue operations.

In the underground mining example earlier, augmented reality can be used to assist with identifying the best drilling pattern as well as guiding the drilling operation itself by analysing the position and angle of the drill head.

**The HMI dilemma**

As mentioned earlier, an augmented reality system is really an evolution of the HMI. The system as a whole needs to take into account human behaviour and this can introduce several design challenges. There is a real risk of a human placing too much reliance/trust in the system and not paying sufficient attention to the whole environment. The system ideally needs to recommend rather than instruct the operator.

The introduction of augmented reality systems will also have an impact on the skills necessary to design, use and maintain these systems. Operators will in future have vastly improved tools available to enable them to work more efficiently, and they will need to learn how to maximise the advantage of these technologies. New skills will also be needed in the ‘back office’ to develop the algorithms and embed the necessary engineering and operational information in ways that are useful to an operator in the field.

**In closure**

The growth of augmented reality technologies will result in more and more industrial manufacturing applications becoming mainstream. Areas such as expert support and complex assembly/maintenance are the most likely to see early adoption of systems, particularly where there are many identical repetitive but complex tasks to be performed.

As usual, for most of us a great deal of caution is advisable as with any emerging technology. Start by becoming familiar with exactly what technology is available and immerse yourself in researching what the vendors are working on. Seek out practical case studies in your industry that can guide you away from making expensive mistakes. In deciding on augmented reality investments, always be led by the business priorities and do not get carried away by hype.
Controlling the IIoT

By John Boville, Schneider Electric.

How the Industrial Internet of Things is changing the role of the control engineer.

Realising the potential of the IIoT rests in large part on how well companies can manage and ultimately control the complex interfaces among connected industrial assets, which is the bailiwick of the control engineer. Their traditional skill set is expanding and being supported by evolving tools, including a new generation of IIoT-ready process automation controllers (PACs). These augment traditional PLC functionality with the processing power, connectivity and security necessary to meet the edge control challenges of the IIoT, equipping control engineers to become real-time business decision-makers who can add significant value to operational profitability.

Get acquainted with the IIoT

While the concept of the IIoT is still relatively new, ubiquitous interconnectivity is already becoming a reality. Having so many more elements in play means more assets and variables to control, plus exponentially more opportunities to help increase production value and reduce operating expenses – especially raw material, energy, and security costs.

Essentially, it’s a control issue. So who better to come to the rescue than the control engineer? Traditionally, process and chemical engineers focused at the process level, applying PID control and advanced optimisation software to solve processes across multiple assets. But as industry dynamics become faster-paced, more complex, and larger in scale, solving problems at the process level becomes increasingly challenging. The complexity of a process control strategy increases exponentially with the number of I/Os. Imagine the complexity when you ramp up beyond the asset to the unit, area, plant and enterprise levels.

For process engineers, there’s ultimately only one way to deal with this rising complexity. Don’t try to control the entire process; control the asset.

But that requires a fundamental shift in understanding assets.

IT programmers once faced similar problems as they attempted to integrate an entire enterprise’s business information. The solution: structured analysis – breaking the complexity into a number of small functional entities, solving each entity, and then combining it all into an overarching solution.

In industry, the equivalent functional entities are operating assets (equipment, units, areas, plants and enterprises). Start by building a comprehensive strategy for each equipment asset (pump, motor, compressor, evaporator, etc.). This is relatively simple due to the small number of I/Os associated with each asset.

Once each piece of equipment is autonomously controlled, moving to the unit level is an incremental control and communications issue, not a process issue. Control strategies for each equipment asset are already in place. Where we once talked about process control and manufacturing control separately, the next generation of industrial advancement will be characterised everywhere by real-time asset control.

For manufacturing engineers, the IIoT presents a different challenge. They have always been asset-centric, applying PLC running ladder logic to solve control algorithms asset by asset, thus controlling pumps, motors, compressors, evaporators, and so on. But now, these assets are expected to do more and to take on a broader scope of work. The critical challenge is controlling them within the context of how other assets and variables are performing, which means balancing safety/environmental risk, reliability, efficiency and profitability.

The right tools

Process and manufacturing engineers are under pressure to realise quick returns on their IIoT investments. Their companies expect paybacks to start rolling in within two years of implementation. To achieve those ambitions, they should give serious consideration to modernising the technologies that control their processing lines, especially the lines that are most critical to their businesses’ success. For those in the hybrid industries, which combine continuous, batch and discrete operations, the need is even more pressing.

To help, control engineers have many automation tools at their disposal, including PLCs, PACs, and DCSs. Technically all have similar control functionality, but each has its own strengths, and it is important to use the right tool for the job. As industry luminary Dennis Brandl puts it: “You can build a house with a chainsaw, but the result won’t likely be ideal.”

Whether you are a process control engineer taking an asset-centered approach or a manufacturing control engineer looking to optimise for the challenges of a world where IIoT is ubiquitous, you are probably going to need a faster, better connected and more reliable PAC – one that has been specifically IIoT-enhanced. And to meet management expectations for greater agility in adapting to market dynamics and improving product availability, you’ll increasingly need a PAC that is more powerful, more integrated and more secure.

A future-proof PAC should have at least the following features:

• A high-performance CPU, greater on-board
memory and faster scan times to handle complex processing and to compress steps in industrial operations.

- Ethernet connectivity to make production information available to other applications in real-time.
- Built-in cybersecurity protection to obtain the benefits of open computing while minimising the risk of cyberattack.

Such systems will be most effective when implemented within a flexible, open, object-based engineering environment. In addition, to take maximum advantage of new features with minimum risk and cost, a fast-track migration approach is essential.

Over the years, controller technology has strongly advanced in this direction. PACs are increasingly being implemented using pre-programmed application libraries and open, advanced, object-oriented engineering environments. These have allowed PACs to gain some traction in the market, primarily as low-end DCS alternatives.

In recent years, PACs have evolved still further. For instance, the Modicon MS80 ePAC adds embedded Ethernet communications and updated cybersecurity protection.

Whether you call them advanced PLCs, IIoT-ready PACs, or ePACs, modern controllers with the characteristics mentioned above are enabling engineers to control their most important risks whether they are in a process, batch or hybrid operation. It is happening already.

Driving real business value
Modern process controllers are already demonstrating that they can drive significant increases in business value as industry transforms, improving operational profitability and safety in ways that directly impact the organisation’s bottom line. They are helping to:

- Increase manufacturing productivity.
- Improve operational visibility.
- Achieve efficient energy management.
- Speed time to market.
- Strengthen cybersecurity.

The increases in business value to be derived from this new generation of controllers make upgrading easy to justify, even in times of continuing downward pressure on capital costs. With the right models, companies involved in brownfield or greenfield modernisation automation projects may see 100 percent returns on their controller investment in as little as three months.

Increased productivity
The IIoT is driving greater customer expectations for everything from faster delivery and more customisation to higher quality – all at lower prices.

It is surprising how much help even relatively modest automation upgrades can be in satisfying these demands. For example, making significant improvements in the pace of production usually requires eliminating steps in the manufacturing process. Conventionally, this may demand a wholesale process redesign.

Recent developments in controller technology point to a simpler approach: Just speed up the steps. For example, new ePACs deliver speedier performance than ever before, with scan times up to five times faster than previous models, plus up to eight times more memory. These are not just technical advances. They generate immediate impacts on the factory floor, adding value to products and accelerating time to market.

Consider a typical case in a hybrid or discrete manufacturing plant turning out a high-value product, which requires six manufacturing process steps with two scans between each step.

But with its significantly faster scan times – 6 milliseconds per scan, compared to 30 ms for older controllers – an ePAC can get to each step more rapidly, ultimately producing 969 cycles per shift, versus only 960 using a previous model. Assuming eight-hour shifts, five days a week for 50 weeks a year, the new controller could help produce nine extra products per shift. That’s 2 250 more products per year. And if each finished product were valued at $1000, the plant could gain $22.5 million in annual production. Thus, simply decreasing controller scan times can make a real difference to bottom-line productivity.

“You can build a house with a chainsaw, but the result won’t likely be ideal.”

In one real-world example, a feed mill in Vietnam used ePACs to achieve three times faster feed production. And, by standardising on one control product family, it has cut cabling costs significantly. Overall, the mill has increased production by 3 percent and reduced costs by 30 percent.

The lesson: for some discrete-industry applications, an automation project that adds the right IIoT-ready PACs, can greatly speed up a production line.

Faster time to market
In addition to streamlining production operations, modern controllers help meet new market requirements and pressures. By shortening the time it takes to adapt processes, they can help users take advantage of new business opportunities, expand operations, and even implement automation on greenfield projects.

Typically, these require teams of programmers to write custom code for each new installation. But newer controllers often offer comprehensive libraries of pre-programmed software for many common applications. This can greatly speed project time and substantially cut costs. Project engineers using modern controllers within open programming environments can integrate them with the rest of the enterprise via open backplane and embedded standard Ethernet connectivity, featuring architecture that is transparent from top to bottom with easy plug-in configuration.

This approach can get new projects (brownfield modernisation or greenfield) up, running and making money much sooner.

For example, using IIoT-ready PACs as described can cut up to three weeks from a typical three-month automation project. Assuming 120 production hours, at $2 000 per hour, a plant can typically save more than $2 million of extra production at launch, decreasing time to market by 25 percent.

Improved operational visibility
Small problems that are not detected can add up to large profit shortfalls. More connected devices means more chances for problems to sneak through. For example, in a typical discrete/hybrid manufacturing plant, information on the performance of an asset such as a pump or motor is confined to the control level. Granular results are not available on all levels of the plant. So engineers and managers alike frequently lack the insight into operational performance they need to make faster, better decisions.

Estimates indicate that lacking precise data on asset location, process status and so on, can cost up to 3 percent of yearly revenues. That can create a significant margin shortfall for the typical plant. The impact on the bottom line can be substantial. Fortunately, advanced PAC technology can help make granular production details available to interested users. The resulting operational visibility aids in stopping losses and delivering increased profitability.

IIoT-ready PACs with built-in Ethernet allow seamless access to advanced collaborative and integrated automation architectures, and to object-oriented integration environments. It is easy to link up controllers with other networks, and make any needed information visible throughout smart connected manufacturing enterprises.

For example, if a controller reading exceeds pre-set parameters, the engineer or operator receives a text message alert on his or her smartphone or tablet. He or she can then click...
through to the affected pump, motor, etc. Its location, coding and full documentation are instantly available – without time-consuming trips to the control room or plant floor PLC/PAC – for fast, efficient problem identification, investigation, and resolution. And fewer trips to the plant floor decrease the likelihood of adverse incidents and bring greater control of safety variables.

With this technology, engineers are also able to offer top management the fruits of today’s most sophisticated real-time accounting measures and tools. So a quite technical feature – transparent, open native networks embedded in an IIoT-ready PAC – can translate directly into real-world business improvements.

Cost-efficient energy management
Just a decade or so ago, the price of energy supplied to a U.S. manufacturing plant traditionally would change only once a year, with each new utility contract. Today, the price of energy at a plant can change every 15 minutes. It is typically only one element in a complex relationship among assets, raw materials and utility costs.

This complexity is one reason for a dawning realisation among engineers and executives: it may be a false economy to try to cut energy consumption across the board because you can cut consumption and still have your electricity bill go up – if you consume that lower amount mostly during peak-priced times of day. And meanwhile, expensive manufacturing capital assets cannot perform whenever required for peak efficiency. Do not shut your machines off, instead, build in better visibility.

New technology means IIoT-ready controllers can be integrated within collaborative and integrated automation architectures utilising built-in Ethernet. “Using these new IIoT-ready controllers, data is visible whenever and wherever it is needed,” says Sylvain Thomas of Schneider Electric. “Controllers are connected to power meters on machines and other assets across the plant. Their data can be gathered into a central point, while integrated connections make data flows visible to whatever users need it. That includes sending information up to IT networks at the business level and benchmarking all the relevant results.

“Active energy management is built into the process, allowing managers to take maximum advantage of fluctuating energy costs. Assets can therefore achieve optimum productive efficiency for the energy consumed.”

Using this advanced controller approach typical plants can reduce their annual energy expenditures by as much as 30 percent. And remember, that includes 100 percent returns on the controller investment in fewer than three months. For example, consider a typical large water plant processing 900 million litres per day. The facility might use 1500 kilowatt hours (kWh) per 3 million litres, 365 days a year, at a cost of $0.05 per kWh. Annual energy expenditure: about $8 million.

If the plant installs advanced controllers using pluggable programming libraries, the result would be managed consumption of process energy. Making smart decisions based on the transparent data the engineers supplied, managers could cut energy up to 30 percent – saving more than $2 million annually on the plant’s electricity bill.

Cybersecurity protection
Utilising open technologies and interconnecting more and more assets plantwide (and worldwide) creates many benefits. But it also points to a possible downside of the IIoT: mounting cybersecurity concerns.

In fact, studies show that manufacturers now have a 32 percent chance of experiencing a hostile cyber event or cyberattack every year. So, an average plant could experience a successful attack at least once every three years. Seventy-five percent of these attacks cost the target an average of $3.7 million. This means an annual risk of at least $1.2 million for the typical organisation – and that risk is increasing.

Adversaries constantly probe for weak points. The notorious Stuxnet worm, for example, reportedly infected PLCs when introduced via USB flash drives. Now IIoT connectivity opens up the possibility of attacks via the Internet. However they occur, cybersecurity breaches can degrade or shut down machine performance causing unexpected downtime and lost productivity, threaten the safety of plant personnel or the community, or even trigger catastrophic environmental disasters. High-profile cyberattacks have led to such serious consequences as a pipeline explosion in Turkey, an energy grid blackout in Ukraine, and even disruption to a nuclear plant at an undisclosed location.

The good news is that advanced cybersecurity can now be designed into each controller, right from the start. Cyber-equipped controllers block communications from unauthorised devices, they digitally sign firmware to prevent counterfeiting, they protect application programs to prevent tampering via unauthorised malware, and they can be set up to disable USB ports, require passwords, and so on. If intrusions or mistakes occur, cybersecurity-equipped controllers can refuse action and send alarms.

Using IIoT-ready PACs in key roles within comprehensive plantwide cybersecurity strategies can drastically reduce the likelihood of cyberattacks. This can save an average discrete or hybrid plant more than $1.2 million annually, and help prevent harmful consequences for production, safety, and the environment.

For instance, in the United States, the intellectual property of a ground calcium carbonate production facility is more protected than ever before. The plant’s grinding operation is now cybersecure at every level, with no additional training required. Since the operation cannot afford any downtime, this advanced IIoT-ready PAC approach helps it run 24/7.

Conclusion
As business and operations leaders respond to and leverage the IIoT, they are evaluating plant automation purchases in new ways. They still start with technical excellence and ease of implementation. But today, they must also make efforts to ensure they are advancing critical business activities such as real-time accounting, which draws on the business algorithms running at the control level to track the impact of control decisions on operational profitability and take corrective actions as needed to maintain or increase it.

Taking advantage of the most advanced PAC technologies has already been proven to deliver such business benefits. For example, consider the Modicon M580 Ethernet-enabled programmable automation controller (ePAC) platform from Schneider Electric. It possesses industry-leading processing speed and memory, as well as stronger embedded cybersecurity. Additionally, its core Ethernet capabilities allow seamless, faster, plant-wide access to operating data: for the hybrid industry, it is considered one of the best performing PACs in the marketplace. The M580 continues Modicon’s pioneering controller heritage, and is built to sustain it. Its makers designed it as the ideal controller for the IIoT, and beyond.

Recommending these advanced PACs can also assist the organisation to achieve fast ROI, and, even more importantly, help it realise substantial improvements on overall profitability for years to come.

For more information contact Jason Ullbricht, Schneider Electric SA, +27 (0)11 254 6400, jason.ullbricht@schneider-electric.com, www.schneider-electric.co.za/en/work/campaign/m580-epac
Turn industrial automation into the profit engine of your business

The Industrial Internet of Things is transforming industry today. Schneider Electric’s value-focused technology and expertise can unlock the full potential of your operations and help you shift from managing your business to actually controlling it. In real time.

By enabling smart control and empowering your workforce, you can continually optimize the performance of all your industrial assets, measurably improving operational profitability, safely and sustainably.

Welcome to the future of automation.
Aspects to consider when securing industrial automation control system networks

By Alvis Chen, Moxa.

Operational technology (OT) consists of a combination of hardware and software to monitor and control physical devices such as valves or pumps on a network. OT is facilitating the expansion of the IIoT by ensuring that different hardware and software can communicate in industrial environments. The most common examples are PLCs, DCSs, and SCADA systems. Such networks are known as industrial automation control systems. The main benefit of an IACS is that it allows greater efficiency by facilitating remote management and more automated processes. However, the vulnerability of the network increases as it expands and more networks require access to the IACS backbone, which is common within the IIoT.

For many years, industrial networks were isolated from enterprise networks, which meant that cybersecurity was not a primary concern for system operators as the networks were well protected due to their isolation from other networks. However, as this is no longer the case, therefore system operators must not use out of date security practices if they want to keep their networks secure. The focus of this white paper will be to analyse why cybersecurity is of paramount importance for IACS networks, and what has to be achieved in order to build, manage, and maintain secure IACS networks.

Challenges that must be overcome to increase the cybersecurity of IACS networks

As no networks are exactly the same, and the risks posed by each threat are unique, there are numerous possible cybersecurity threats facing system operators. Before an IACS network can be deemed secure, it is essential that system operators have a thorough understanding of all of the risks. The challenges system operators face will now be explored in detail, which will assist them to implement successful solutions.

How to design and deploy a secure network

Typically, parts of an industrial network and certain devices are secure from the threats that are posed to them. However, in order to violate the security of the entire network, all that is required is to infiltrate one device or area of the network. Once someone with malicious intent has gained access to a single device on the network, it is very easy to corrupt and control other areas and devices on the network. Most network designs are intended to stop unauthorised users from gaining access to the network, but once a device on the network has been infiltrated, it is very difficult for other devices within the network to understand that it poses a security risk. As IACS networks become less isolated by adding more devices and networks to the originally closed network, they become more vulnerable to attacks. System operators that only previously managed isolated
networks often have insufficient knowledge about how to ensure that an IACS network is kept secure.

How to prevent cyberattacks against industrial network devices
All it takes is for one device on the network to be corrupted, and it is very easy for those who have control over a single device to modify the configurations of any device located on the network. The effect that this can have on IACS networks can be devastating. In addition, as industrial networks continue to evolve to keep pace with modern trends, there are still some legacy features that need to be updated. Previously, isolated industrial networks did not know who accessed a device or from which location, but only knew that the automation process had been logged into. However, as modern industrial networks frequently converge with other networks, this makes them more susceptible to hacking. In order to combat this threat, the devices on industrial networks must record and keep log files that are capable of determining when an event with a potential security risk occurs on the network. This can include events such as a firewall blocking communications or a user unsuccessfully trying to log in three times. Another countermeasure to ensuring network devices are not affected by cyberattacks is data encryption. Previously, system operators rarely encrypted sensitive data because industrial networks used to be isolated from enterprise networks. However, as modern industrial networks continue to expand, there is a high chance that data will be stolen or corrupted as it is transmitted outside of the closed network. It is for these reasons that data encryption is essential for modern networks.

How to manage network security throughout the entire system lifecycle
Modern industrial networks are continuously evolving. This means that the security settings need to be constantly reviewed to ensure that the network remains secure for its entire deployment. Many cybersecurity experts have observed that as an IACS network adds more devices and connects other networks for IIoT opportunities, it requires more maintenance and firmware upgrades. The more changes that happen on the network increases the chance that a vulnerability will occur that allows someone with malicious intent to gain access and corrupt the network. An example that frequently occurs is when a new device is added to the network and the default password settings are not changed. As soon as default passwords for devices are used on a network, it is much easier for hackers to gain access to a device, which puts the entire network at risk. In addition, as networks expand over the duration of their lifecycles, they often require new types of connections with different networks or devices that the system operator has not encountered before. When this scenario occurs, the system operator will often be unaware of what needs to be done to ensure these new connections are secure. This will increase the number of potential weaknesses and open vulnerabilities on the industrial network.

There are a wide range of options available in order to counter the numerous cyber threats posed to industrial networks. Solutions tend to focus on hardware and software that allows system operators to build secure IACS networks. In addition, there are cybersecurity guidelines developed by leading professionals, such as the IEC 62443 standard, NERC CIP, and NIST 800-53 that advise system operators on how to protect their networks. Each of these standards focuses on specific parts of a network for those who perform maintenance there. Even though there are multiple security standards that address different security areas, this white paper will focus on the guidelines set out by the IEC 62443 standard as they contain the most relevant details for the security of industrial networks (Figure 1).

Three factors that help ramp up the security of industrial networks
Industrial networks must be protected from unauthorised access that could damage them and therefore decrease productivity. Many cybersecurity experts believe that in order to ramp up the security of industrial networks, there are three aspects that need to be addressed. These aspects will be briefly introduced before being considered in detail.

1. Device security
This section will focus on how the evolution of industrial networks over the past few years has changed the procedures system operators must perform in order to secure network devices from cyberattacks. The first concern that will be considered is device authentication and access protection. The second concern is how to utilise an easy-to-use, effective password policy when system operators have hundreds of devices installed on their industrial network. Finally, it addresses how to ensure that all devices have the ability to collect and store event logs. Event logs alert the system operator to what happened on the network and why it happened, which will allow them to fix the problem as quickly as possible.

Network security
In the network security section, the focus will be on which devices or systems need to have the highest levels of protection. In addition to this, an explanation of the defence-in-depth approach will be given that includes examples of why it should be utilised in order to ensure that the network remains secure. Finally, the challenge of how to ensure secure remote access through the use of firewalls and VPNs will also be explored.

Secure management
The secure management section will consider a list of the recommended procedures for security policies and guidelines developed by experts in order to ensure that the network is protected throughout the entire network lifecycle. This section will also consider device security and how to manage the security of the entire network. Finally, this section will consider how to simplify the configuration and management of security settings. When security settings are too complicated, as is
often the case on industrial networks, system operators will tend to ignore recommended guidelines and not implement security settings. Figure 2 shows the relationship between these concepts.

How to implement a secure industrial network
This section will give system operators a step by step overview of the three aspects that need to be considered in order to implement a defence-in-depth security architecture.

Defence-in-depth
When designing a network, many system operators have stated that the best way to secure it is to use the defence-in-depth security architecture, which is designed to protect individual zones and cells. Any communication that needs to take place across these zones or cells must be done through a firewall or VPN. Deploying this type of architecture reduces the chance that the whole network will fail because each layer is able to address a different security threat. It also reduces the risk to the entire network; if a problem occurs in one part of the network, there is a higher chance that the problem can be contained within that layer and will not spread to other layers. Experts have identified three steps that should be taken in order for a reliable defence-in-depth cybersecurity architecture to be deployed, which will now be considered in detail.

Step 1: Network segmentation
Network segmentation involves breaking down the network into physical or logical zones with similar security requirements. The benefit of segmenting the network is that each section can focus specifically on the security threats that are posed to that section of the IACS. Deploying the segmentation approach is advantageous because each device is responsible for a particular part of the network, as opposed to being responsible for the security of the entire IACS.

Step 2: Define zone-to-zone interactions in order to scrutinise and filter network traffic
In order to enhance network security, the traffic that passes between zones in the IACS must be scrutinised and filtered. Cybersecurity experts believe that one of the best methods to filter traffic is for the data to pass through a demilitarised zone (DMZ). By utilising a DMZ, there is no direct connection between the secure IACS network and the enterprise network, but the data sever is still accessible by both. Eliminating a direct connection between secure and enterprise networks significantly reduces the possibility that unauthorised traffic can pass to different zones, which has the potential to jeopardise the security of the entire network.

Step 3: Support secure remote access on industrial networks
Finally, within the IACS industry there is a growing need to provide access to remote sites where functions such as maintenance can be performed. However, this significantly increases the risk that someone with malicious intent can access the network from a remote location. For networks that require the remote site to be constantly connected to the IACS, it is advised to use a VPN that supports a secure encryption method such as IPsec, which prevents unauthorised users from accessing the network. There are three main advantages of using a VPN that supports IPsec. The first is that the data will be encrypted when it is transmitted. The second is that it forces the sender and recipient to authenticate who they are, which ensures that data is only passed between verified devices. The third is that by enforcing encryption and authentication, integrity of the data can be ensured. For many experts, data integrity is the most crucial aspect for system operators to use their data reliably. IPsec ensures that security keys must be between 20 and 40 characters in length, which is considered strong enough encryption to transmit data securely on an IACS. In order to ensure data is complete, system operators need to use secure transmission methods that ensure data is encrypted and authenticated at all times.

Secure industrial network devices
After the network has been secured, the next step is to consider how to ensure that users cannot adversely change settings by accident or on purpose. This problem can arise from users who operate and manage the network, third-party system integrators, and contractors that are required to perform maintenance on the network. The best way to secure against this threat is to enhance the network devices’ cybersecurity to ensure that they cannot have their settings altered in a way that puts the devices or the network at risk. Many cybersecurity experts view the IEC 62443 standard as the most relevant publication for how to secure devices on industrial networks. This standard includes a series of guidelines, reports, and other relevant documentation that define procedures for implementing electronically secure IACS networks.

The IEC 62443 standard contains seven foundational requirements for device security on industrial networks, which will now be listed and their relevance explained:
1. Identification and authentication control: public key authentication should be used in order to ensure server-to-device and device-to-device connections are secure. In order to ensure identification and authentication control, each network device must be able to validate security certificates by checking the authentication of the signature as well as the revocation status of a certificate.
2. Use control: every device that appears on a network must support login authentication. To restrict unauthorised users from gaining access to devices or the network, the application or device must limit the number of times a user can enter the password incorrectly before being locked out.
3. Data integrity: across all IACS networks, the integrity of the data is very important because it ensures that data is accurate and that it can be processed and retrieved reliably. There are several security measures
4. Data confidentiality: when data is stored or transmitted across networks, it has to be safe and secure. The data should be protected from all types of threats ranging from very basic ones to highly sophisticated attacks. Data must be secured at all times from those who wish to eavesdrop on communications, alter settings, or steal data.

5. Restrict data flow: one of the most effective methods of restricting the flow of data is to split the network up into different zones. Each of the different zones utilises specific security features to ensure that only those with authorisation can access and send data from a specific zone. Another benefit is that if a zone is infiltrated, the threat cannot easily spread to other parts of the network, which helps limit the damage caused by the security breach.

6. Timely response to events: it is essential that system operators are able to respond quickly to security incidents that happen on the network. In order to facilitate this, the network must support the features needed to alert system operators if a problem occurs and also keep a record of any abnormalities that happen on the network. All of the events that happen on the network should be processed in real time or at least fast enough to ensure system operators can respond quickly enough to prevent further damage being caused to the IACS network.

7. Network resource availability: devices on IACS networks must be able to withstand denial of service attacks from people with only a basic understanding of IACS networks or who are presented with an opportunity due to operator error. Devices must also be able to withstand attacks from entities that...
have high motivation and high levels of IACS specific skills. The important point is that the network must not experience downtime regardless of who is attacking the network. Now that the security requirements have been outlined, some examples will be explored in order to demonstrate how the fundamental requirements of the IEC 62443 standard can help protect against security threats.

The first example involves the importance of strong password-based authentication, which relates to the first foundational requirement:

- Most devices on industrial networks still use default passwords that make them vulnerable to security breaches. The reason why some engineers prefer to use default passwords is because it simplifies their work processes. However, this puts not only the devices but also the entire network at risk. In order to overcome this security issue, the devices located on industrial networks must enforce password policies that are based on a minimum password length and a variety of character types. The password policy should also include guidance for the user in the event that a password is input incorrectly. Passwords that adhere to a strong password policy will help protect against brute force attacks as they are much harder to guess.

The second example explains the importance of why devices on the network must be able to protect the integrity of transmitted data, which relates to the third foundational requirement:

- The best way to enhance the security of the industrial network devices is by ensuring they support secure communication protocols such as SSL, SSH, or alternatively password protection for device configuration through HTTPS. However, most of the devices on IACS networks still use non-secure plain text communications. If secure communication methods are not used, system operators leave their devices vulnerable to being hacked. Another more dangerous scenario is when operators continue to use devices on the network and are unaware that their data has been corrupted. This can lead operators to making operational decisions based on inaccurate data, which has the capability to wreak havoc on the network.

The third example is that all devices on the network must support a method to retrieve critical information if the network fails, which relates to the seventh foundational requirement:

- In order to do this successfully, devices must be able to verify that the data has been backed up reliably and accurately. All network devices must utilise appropriate mechanisms to ensure that once the data has been backed up, it is stored reliably and can be retrieved when it is needed. It is not only the data on the devices that is important to keep secure but also the configuration settings. As there is a very real risk that an industrial network will be attacked, it is highly advised to use devices that can backup network settings and device configurations. On IACS networks with thousands of devices, this can save system operators many hours by allowing configurations to be uploaded automatically as opposed to entered manually.

### Maintenance of an industrial network

Throughout the automation system lifecycle, maintenance will often need to be performed by local engineers or system integrators. This maintenance will typically include changing, replacing, or updating devices located in the network. It is important to note that whenever a device has some of its settings modified, there is a possibility that it is no longer secure and is now vulnerable to cyberattacks.

As networks, especially IACS networks, continuously evolve and change, there needs to be constant monitoring of the network and all the devices located on it. As there are almost always a large number of service personnel who are responsible for monitoring and maintaining different devices on the network, it is not a good idea for all of them to perform security settings based on their own knowledge or experience. For this reason, a good standard operating procedure that clearly defines how to configure device settings should be adhered to at all times.

It is important to ensure that constant monitoring of the network takes place to ensure that no errors occur and that the network can be kept safe from all security threats. In addition, system operators will often ask their device suppliers how long it will take to have a firmware upgrade in the event of a vulnerability being discovered on the network. A quick response time to this type of request is very important for ensuring the security of the industrial network. Therefore, network operators should know how long they need to wait for a firmware upgrade or device replacement if a security risk occurs.

### Operating an industrial network

Now that some of the best practices have been established for ensuring IACS networks remain secure, the question of how to simplify this process will be considered. On almost every IACS network, there are multiple security setting options for all of the different devices located on the network. Therefore, it is very challenging for system operators to monitor the security status of every device. In order to overcome this difficulty, one method that is frequently employed by system operators is to export all of the devices’ configuration settings to a storage device. When a device needs to be replaced or reset, all the system integrator has to do is import the device’s settings from the storage device directly into the network device. This avoids the aforementioned problem of engineers relying on their own experience or knowledge to configure device settings as well as saving time and avoiding human error. System operators must choose a suitable device that will securely store configuration settings and reliably upload configuration settings to devices without any errors.

It is important to remember that industrial networks are only secure when all the network devices support the necessary security features and when these features are adhered to throughout the entire network lifecycle. In addition, the system operator must be able to respond very quickly to any event that occurs on the network and ensure that any configuration changes are done securely and accurately. Being able to efficiently maintain and operate a network will greatly assist system operators to monitor and manage their network in a secure manner throughout the whole network lifecycle.

### Conclusion

Ensuring that a network and the devices installed on it are secure is not easy because the threats posed to industrial networks are constantly changing and evolving. In order to protect the network as well as possible, system operators should adopt the defence-in-depth network architecture. Aside from a good overall network design, system operators should select hardened devices that are compliant with the IEC 62443-4-2 standard. Overall, system operators should have a thorough understanding of the possible threats facing their network as well as detailed knowledge of the best practices for designing and maintaining networks. Finally, ensuring that the network is constantly monitored throughout the network lifecycle will mitigate any security risks that arise as the network evolves.

For more information contact RJ Connect,
+27 (0)11 781 0777, info@rjconnect.co.za,
www.rjconnect.co.za
System 800xA High Integrity
It’s all about safe and secure operations

ABB provides the enabling technology to integrate safety into the core of your operations. ABB has addressed the fundamental design elements required to maintain independent layers of protection while fully integrating safety systems into our System 800xA automation platform. Take control of your plant safety and productivity. [www.abb.com/highintegritysafety](http://www.abb.com/highintegritysafety)
Endress+Hauser aims to improve the processes of its customers with regards to efficiency, quality, safety and sustainability. When it comes to the mining business, the company is intent on mastering the challenges of extracting and processing precious metals and minerals by increasing efficiency, improving safety and protecting the environment.

Integration as the first step
The question is: how much can Big Data help mining companies master these challenges?

Data is already produced in abundance within a mining operation: process information from the field, inventory values, plant status and market prices to name just a few. The challenge is that most of this data is stored and visible only in different systems. So the first step towards the IIoT has to be the integration of this data to open up its real potential.

Integration has to be aligned along three axes: horizontally along the value creation chain, vertically from the field to the control level, and thirdly, from planning to maintenance to ensure consistent engineering. With the help of Endress+Hauser, users can boldly take the first step today.

With respect to the horizontal axis: an exact forecast of consumption based on current inventory values and planned material movements is the key to reducing warehouse stocks and improving delivery services. Reliable measurement is the basis for this and Endress+Hauser can provide a complete range of technology. For data communication, most available fieldbus technologies can be plugged directly into smart measurement sensors. In addition, the local data transmission unit, Fieldgate, with integrated web server, allows for global data acquisition via private and public communication network.

A standard Internet browser is sufficient for querying inventory data. Fieldgate not only provides current measured values, but also offers the possibility of monitoring device stations, requesting information and sending data directly to a superordinate inventory management software system such as SupplyCare from Endress+Hauser.
SupplyCare offers convenient access to the current fill levels in tanks and silos from the comfort of the office, and offers extensive functions for inventory management. With the integrated email function, users can request supplies quickly and easily. With the analysis module, they can also calculate and evaluate KPIs.

**Full control of basic processes**
When it comes to vertical integration, intelligent networking between subsystems of the mining process, from the ERP system to the operating and control level, and on to the field level, is essential for optimised functionality and the highest efficiency. The reality today is often something less than a smooth, streamlined operation. It is characterised by closed system silos, missing interfaces and many manual data transfers, all of which are potential error sources. However, thanks to Endress+Hauser’s business process integration (BPI) concept, it is now possible to connect these currently decoupled system silos to form an elegant overall system with a continuous data flow. BPI acts as an interface beneath the sub-systems and thus forms a shared platform for data exchange.

By using industrial Ethernet at field and control level, automation components can also be integrated in the overall system. Digital communication, for example, enables advanced measurement sensor diagnostics, which can form the basis of effective process condition monitoring and preventative maintenance strategies, or calibration requests triggered in the ERP system.

Many of Endress+Hauser’s smart measurement sensors can be used to monitor process condition and verify measurement integrity. Simply look for the Heartbeat Technology logo. Several examples of Heartbeat Technology benefits are already used in the concentration processes in many copper and gold mines. For example in froth flotation tanks a Promass 100 Coriolis flowmeter will schedule a flocculant batch remix by measuring changes in the medium chemistry. The aim is to produce process optimisation and stability using a combination of smart sensors which monitor their own performance, indicate process anomalies and inform maintenance when cleaning or recalibrating are required.

**Big Data made easy**
In order to get close to the goal of maximum process efficiency at the lowest possible cost, intuitive and reliable process asset management is crucial. To facilitate this, Endress+Hauser offers Big Data asset management software that is vendor neutral. The cloud-based asset management toolbox, W@M, has proven beneficial to management executives, maintenance personnel, process engineers and metallurgists in generating plant wide process improvements and providing relevant and reliable data on process performance. A simple example is a ten percent proven increase in heap leach and stripping performance in a copper mine when it introduced W@M’s powerful capability to monitor variations in performance of critical measurement parameters such as acid usage, PLS output, organic to aqueous stripping rates against pipeline breakage, filter rupture, and other process imbalances.

In short, what does the software deliver that is Industry 4.0 or IIoT ready?

• Quick, visual and targeted access to the right data exactly when it is needed.
• Easy to download cloud-based tools including apps for mobile devices.
• Wireless and wired connectivity to smart sensors and other process equipment for diagnostics, verification and condition monitoring

“Our customers are sometimes surprised to find that for their first implementation of Industry 4.0 they do not need to completely revamp their operation,” explains Endress+Hauser industry manager, Susan Buitendag. “The fourth industrial revolution is in fact more a gradual evolution than a big bang approach to change. We at Endress+Hauser take pride in being an innovative company and our engineers keep us ahead of the game when it comes to smart sensor development. This means that the first step towards Industry 4.0 and the ‘digital mine’ is a small one for our customers.”

**For more information contact**
Dhiren Naidoo, Endress+Hauser, +27 (0)11 262 8077, dhiren.naidoo@za.endress.com, www.za.endress.com
The Fourth Industrial Revolution (Industry 4.0) refers to the current era of convergence between automation and data exchange technologies in manufacturing. The top 5 trends that will characterise automation technology in this new age of ‘smart factories’ include the Industrial Internet of Things (IIoT), augmented reality (AR), mobile access to machines, reprogrammable robotics and industrial automation security.

The Industrial Internet of Things
Automation, in a broad sense, refers to the integration of mechanical systems with electronics and embedded firmware. It is implemented to facilitate standardised, reliable production systems, effective monitoring, reduced waste and optimised production processes. During the paradigm shift of the digital age, the IIoT will develop these aspects of manufacturing by enabling accessibility to greater amounts of information at greater speeds than were possible before.

The IIoT is the convergence of information technology (IT) and operations technology (OT) systems in ways which give operators access to the information (big data) they need to make more informed process related decisions. Big data mitigates risk and improves efficiency. It builds a connected enterprise to improve productivity and helps workers to develop new skills.

Today’s reality indicates that software, sensors and controls are at times outdated and difficult to upgrade. At the same time, there is limited integration between internal systems (plant data sources) and external systems (ERP). Tomorrow’s vision shows how through communication, sensors and operational technologies will work as an integrated system along with IT. Standard, fast software development techniques will be used to create intelligent industrial products in a common sensing and control architecture. Research indicates that these improvements in the industrial sector could yield revenue growth of up to 70% and an improvement in workforce productivity of up to 30%.

Remote access to machines
Building Android and Windows apps are some considerations for mobile access. Waiting for a third party to develop an app for a mobile device could take time, and if not skilfully coded, the result could be poor performance. Factors like time, complexity and expense result in a native mobile version of the app to be more productive, thereby optimising this process. At times a single device sacrificing performance is optimised to run the app on a website geared for several mobile devices. In terms of IIoT, the Siemens WiFi ETH-MPI DP S7-300 Ethernet communication adaptor module CP343/5611 can be incorporated with the S7-1500, S7-1200 and ET 200SP controllers or S7-1500 and ET 200SP CPUs running V1.8 firmware or S7-1200 running V3.0 firmware, to facilitate mobile access.

Augmented reality
Augmented reality is the real-time integration of digital information into the user’s environment. Unlike virtual reality, AR uses the existing environment and overlaps new information, by written application, in special 3D programs. AR applications incorporate GPS, machine vision, and object and gesture recognition technologies. An AR system provides a mixture of real and virtual images in the user’s interface unit, e.g. a cellphone. The objects of the real world observed by the user are sent to a processing system, e.g. a computer, which generates the virtual object. The real and virtual objects are synchronised in a way that produces a perception of observing a common graphical representation. The type of industrial system determines the approach to be used in terms of the resultant output. Displays, monitoring systems, interaction devices and computer systems are the
primary components of AR. The display is crucial to provide a representation of the system. Accurate location in real-time is the responsibility of the monitoring system, which aligns the virtual and real objects. The interactive device provides a physical interface for the user whilst the computer system is responsible for generating the virtual objects.

Problems and related solutions
- An adjustment must be made to a machine: visually direct workers to the adjustment port.
- Worker is in an unfamiliar environment: provide contextual visual instructions.
- Worker spends time searching for data on equipment they are repairing: identify the equipment and display the data.
- Technical resources are required to evaluate an unplanned incident: provide communication tools and a real-time ‘snap shot’ of the equipment.

Reprogrammable robotics
The primary driver for manufacturers is the need to embrace automation to remain commercially competitive. Automation can be extremely cost-effective on a scale from SMMEs to large factories. In terms of flexibility, manufacturing processes can be adapted to different options from a single product in a given operation, e.g. a two-position gripper functions on two axes to offer flexibility and rigidity. Robotic effectors adapt to different sizes, shapes and textures to offer optimal performance and introduce cells or modules to facilitate flexibility, e.g. incorporate a ‘pick-and-place’ function but keep the remaining line unchanged. There is no waiting time for operators as the robot is programmed to perform basic repetitive operations, and can be reprogrammed to perform intermediary ones. In the long term, robots are less expensive than manual labour and can be programmed for specific tasks and then reprogrammed to change tasks, thereby increasing accuracy and preventing bottlenecks. A 2014 survey by PWC and Zpryme showed that 27% of respondents planned to implement robotics in assembly processes, 26% in machining, 22% in dangerous tasks and 16% in warehousing, within the next three years.

Industrial automation security
Alongside all the potential benefits offered by Industry 4.0, industrial automation security is one of the biggest challenges. Manufacturers will have to remain vigilant as their networks permeate down from the top floor to the shop floor. Any new device on the network is a potential access point for hackers and this will need to be addressed without compromising the high resiliency required by OT or the interconnectivity and compliance required by IT. Viable new security models must be developed to work with both new and existing systems. In terms of security threats: remote code execution (RCE) vulnerabilities enable arbitrary code to be remotely executed in a target system; denial of service (DoS) vulnerabilities enable DoS attacks to be carried out remotely; code injections include vulnerabilities that enable SQL additions to be performed remotely. File manipulations enable various file operations to be performed remotely, while user access account manipulation enables attacks on legitimate user data to be performed remotely. In addition, ageing operating systems and vulnerable technologies add to the posed security risks.

For more information contact Prof. Ralph Naidoo, Department of Electrical Engineering, Mangosuthu University of Technology, Durban, +27 (0) 31 907 7426, pnaidoo@mut.ac.za.
Preparing for digitalisation and an era of collaborative robotics

Digital transformation and its associated technologies – collaborative robots in particular – are generating enormous interest in manufacturing. Industry 4.0 will have a strong impact in the coming years in Africa, especially in the South African manufacturing industry. Scratch the surface and behind the enthusiasm generated by the technological developments lie issues for society concerning the impact and effects of this digital transformation.

Education 4.0
“For Industry 4.0 to be fully realised in the future, education systems will have to place an urgent focus on mathematics and science,” says Victor Marques, country manager of Omron South Africa. “Secondly, tertiary institutions and industry need to be closely aligned regarding the curricula of the degrees and diplomas to meet industry demands of the future. Technology is evolving at an ever-increasing pace. We as a nation cannot afford to be left behind.”

Changes in the workplace
South African industry needs to find ways of adapting and using the technologies driving the fourth industrial revolution to remain globally competitive, yet maintain and create jobs in a high unemployment environment. Industry 4.0 will influence the conditions of and requirements for employees in many areas. Driven by the application of machine-to-machine communication and an increase in the realisation of autonomous systems, the demand for qualified production controllers and managers has increased, but the demands placed on workers themselves can be reduced. The impact on the general situation of workers and unskilled labour can be positive. On the other hand, their skilled counterparts will have to come to terms with growing pressure on performance and skills.

“The world is a far more connected place with a tremendous need for data,” continues Marques. “The age of Big Data is here, and the costs for transmitting, receiving and storing it will drop as competition and market demand increase. Therefore, education remains key, as does a rapidly accelerated installation of infrastructure such as fibre coupled with cost effective and ubiquitous access. We in Africa are faced with unique challenges and opportunities. Our creative think tanks will have to come up with innovative solutions to fully utilise these to leverage benefit for all of the continent’s people.”

Discourse on Industry 4.0
Industry 4.0 and the digitisation of our day-to-day lives are bringing many improvements in their wake. The increased efficiency, improvements in productivity and new services will change our society, behaviour and the corporate landscape. The transformation will mean that countries that promote digitisation will be able to defend and build on their competitive position. The change to a digital society will take place over the next 20 to 35 years. The availability of digital infrastructure, an increase in the availability of data sources and a requirement for the efficiency of services and algorithms, in line with Moore’s Law, are the prerequisites for the change to a digital society.

The effects of Industry 4.0 and the further use of robotics in the world of work are many and various, and are influenced by the availability of infrastructure in a company, as well as by digital investment strategies and cooperation between social partners. Digital transformation will change the demand for skills. More highly skilled workers with an understanding of complex relationships will be required. The knowledge surrounding these relationships will become obsolete more quickly as technology continues to develop, and will constantly have to be kept up to date. Society will experience a new and greater dependency on up-to-date knowledge, while at the same time processes considered monotonous and irksome will be eliminated as machines become capable of making decisions autonomously. In some cases even specialist workers will no longer be required in a production environment, and it is also possible that Industry 4.0 could bring about ‘technological unemployment’ among both specialist personnel and their lower-skilled counterparts.

Marques concludes that as South Africans, we need to start at grassroots and foster an interest in the sciences at primary and secondary level. As for industry, all the relevant stakeholders need to familiarise themselves with the concepts of Industry 4.0 and the benefits and value that this technological revolution can bring. Integration and service providers need to ensure that they are always ready to implement the latest innovations – those who do not, simply will not survive.

For more information contact Omron Electronics, +27 (0)11 579 2600, info.sa@eu.omron.com, www.industrial.omron.co.za
Yokogawa’s cybersecurity solutions

Cybersecurity is a hot topic in the industrial automation world and includes network and system security. Yokogawa has strengthened its product line to face these challenges by strengthening its cyber strategy on multiple levels from a security standpoint.

Network security has become critically important in recent years, as it is constantly being subjected to new threats, which are continually increasing in number and becoming more sophisticated. Network security should not rely on one method only, but use a defence-in-depth strategy to secure a business in different ways.

Yokogawa cybersecurity for industrial control systems

Yokogawa has developed comprehensive network and system security for its industrial process control systems, which address common and known internal/external system vulnerabilities. The solutions can be deployed to new projects or to existing facilities and comprise the following network and system cybersecurity components:

- Security competence: the research and development centres of Yokogawa are located across the globe to develop security techniques for process control systems. With extensive experience in control system integration, these centres develop security techniques and solutions optimised to each industry, application and system configuration.

- Security in products: the product lifecycle addresses by professionals of both IT and OT.

- OT vs. IT

Connecting industrial devices and applications so as to provide plant and enterprise personnel with actionable information is not a new concept. Leading automation and software suppliers have been working diligently to address this requirement for decades. However, these efforts have not always been successful due to poor interoperability between operational technology (OT) and information technology (IT). This has hampered business performance.

At the OT level, a large number and variety of different sensors, intelligent field devices, controllers, systems, mobility devices, application software, networking, and security components related to the IIoT come into play. While these are available in a wide variety of ‘shapes and sizes,’ all feature some degree of built-in intelligence, self-diagnosis capabilities, connectivity, and support for analytics.

In order to benefit from the connected world, cybersecurity issues need to be addressed by professionals of both IT and OT. As a proven and trusted partner, Yokogawa delivers Plant Security Lifecycle Services to ensure plant safety and security for mission-critical industrial applications, based on the defence-in-depth approach and corresponding to international standards.

Plant Security Lifecycle Service

Yokogawa’s cybersecurity approach is composed of four phases that start from the assessment of the system through to the validation of the security controls. This approach ensures that the design and implementation cater not only for the industry, but also for each customer’s unique environment.

- Assessment and analysis: proposal for the lifecycle security service solutions for both new and existing systems.

- Design and implementation: deployment and enhancement of optimal security controls.

- Operational support: provision of security training, regular security updates and continuous security monitoring. Support for security incident response and prompt recovery from such incidents.

Conclusion

For more than a decade, Yokogawa has developed and provided proprietary cybersecurity solutions and technology for its customers. During the time, the Yokogawa Industrial Cybersecurity group has gained experience and knowledge through various cybersecurity projects around the globe to become a trusted co-innovation partner for minimising security risks and maximising value creation for customers.

For more information contact Christie Cronje, Yokogawa South Africa, +27 (0)11 831 6300, christie.cronje@za.yokogawa.com, www.yokogawa.com/za
How to prove payback on an Industry 4.0 project

As industry changes amid the drive towards digitalisation, organisations are looking to achieve real business results from their engagement with new technologies. Marketing hype detailing theoretical benefits of an IIoT-enabled future is no longer enough; companies want to see real returns on investments in new technology. Festo, for example, not only implements IIoT functions and services into its product portfolio, but also adds training and consulting, for students as well as professionals, using the latest ideas in its Technology Factory at Scharnhausen, Germany.

Industry 4.0 products: from the mechanics to the cloud
Festo already delivers some real automation technology products for the fourth industrial revolution: integrated drive packages, modular valve terminals with open platform communications (OPC) universal architecture (UA) and IoT gateways, decentralised Codesys controllers and autonomous mechatronic subsystems with IP20 or IP65. In addition, there are IoT driven apps and services, as well as dashboards for products and subsystems. Festo is able to provide consistent connectivity from the mechanics right up to flexible and multiple cloud concepts.

The company has the advantage that it can draw on a wealth of user experience from pilot projects at the Scharnhausen plant. These include energy management and optimisation as well as innovative one-piece-flow concepts based on standardised networking, mobile maintenance with tablets or automated, flexible test systems for individual products.

Big data analytics figure out bottlenecks to reduce cycle time by 15%
The example described below refers a significant 15% improvement in performance of an assembly line, enabled by big data analytics. It highlights, how Festo's new automation platforms with a direct link to a cloud can be a basic ingredient for success.

A large assembly line was designed for mass production, as well as lot size 1. (Current customers demand lot size 200-2000.) The volume each year adds up to 1,2 million at a cycle time of 13 seconds.

The change of the batches is done by SAP ME/order management, but inside the machine RFID at each work station triggers all parameters. Technically, the basics of the assembly line are mechatronic subsystems in all machine cells, which are operated by decentralised control concepts for the electric and pneumatic drives and actuators. All stations provide the data relevant to operate and maintain the line, and are networked with all testing stations and quality systems. Data which is relevant for the machine operation is processed locally in real-time. All data, from around about 400 IP addresses in total, is gathered, condensed and provided via OPC UA to either support motion control, or for analysis by a PC or a cloud-based solution. Such a concept generates a mass of data, which requires additional skills for the data analytics. Data scientists are needed to get the most value out of the data.

After two years in operation, a first big data analysis was executed and turned out to be highly valuable. Typical patterns could clearly be found and bottlenecks were identified. It was found possible to overcome these and optimise the machine's cycle time by 15% – from 13 to 11 seconds. The changes made include modifications inside the test cells and their procedures. The work stations now trigger the test cells in advance and thereby save booting and routing time. Other bottlenecks required a more powerful CPU be installed. The value of data made such an optimisation possible without the time wasting associated with guesswork and trial and error approaches. This example shows how to transform measured value into added value with a payback period of less than one year.

Automation solutions for mechatronic subsystems in Industry 4.0 environments
To get all the relevant data out of a machine requires several ingredients. Depending on the production system, it could include integrated drive solutions, electric as well as pneumatic, plus associated sensors, quality inspection, tracking, energy monitoring, connection to logistics and order management. A possible Festo solution is the CPX system, a high-performance control platform for factory automation. It consists of individual function modules that can be used to create a modular, compact and flexible (sub)systems. Depending on the module combination, it can be used as a purely remote I/O system, or as a (centralised or decentralised) control system for factory or process automation.

Festo can thus offer a portfolio for the decentralised automation of sub-systems and small machines/installations with IP20 (CPX-E platform) and IP65 (CPX platform). All in line with a flexible Industry 4.0 host environment, including the CPX-IOT gateway and the first customised dashboards in the clouds of Festo, Siemens MindSphere or Rockwell FactoryTalk.

For more information contact Kershia Beharie, Festo, +27 (0)11 971 5509, kershia.beharie@festo.com, www.festo.co.za
Siemens turns Industrie 4.0 vision into reality with Digital Enterprise portfolio

Siemens is continuously enhancing its Digital Enterprise portfolio for Industrie 4.0, the fourth industrial revolution, i.e. created the technical platform for this transformation with its range of innovative solutions. By implementing Digital Enterprise solutions, Siemens customers can now tap into the full potential of Industrie 4.0. These offerings enable users to achieve greater flexibility, shorter times to market, higher efficiency and better quality, all accomplished with no disruption to current operations. This is a testament to the added value that the Siemens Digital Enterprise offers the discrete manufacturing and process industries.

Expanding the MindSphere

The focus is on further expanding the range of offerings for the Digital Enterprise with solutions featuring greater flexibility for design, manufacturing processes and structures. This includes solutions for digital twins, which are being used today to create a holistic virtual model of the value chain, along with Siemens’ leading automation portfolio, as well as the open, cloud-based IoT operating system MindSphere. Connecting to MindSphere is one of the foundational aspects of new, data-driven business models for customers. By founding MindSphere World, Siemens has taken another step toward expanding the ecosystem around MindSphere. For customers, the MindSphere IoT operating system provides access to new dimensions of connectivity and data analysis.

The Digital Enterprise portfolio offers the levers needed to gain these benefits. This includes such aspects as full integration of the individual stages of production and the establishment of a uniform basis for the data, from car design to production planning and all the way to manufacturing and the provision of follow-up services. This applies both to the construction of new production plants and to the upgrading of existing factories, particularly when it comes to expanding the portfolio to include electric and hybrid vehicles.

The digital transformation of the processing industry is already in full swing. For this task, Siemens offers the required portfolio of solutions with integrated hardware and software and thus enables companies of any size to implement digitalisation.

Through Siemens’ Digital Enterprise portfolio, small and medium size businesses, as well as large enterprises, can achieve international competitiveness. Greater flexibility makes it possible to manufacture increasingly diverse model variants efficiently, even when they are produced in smaller quantities.

For more information contact Jennifer Naidoo, Siemens Digital Factory and Process Industries and Drives, +27 (0)11 652 2795, jennifer.naidoo@siemens.com, www.siemens.co.za
Smart irrigation system saves water and energy

Founded in 2008, Shock Wave Engineering provides Internet of Things (IoT) solutions in the agriculture and mining industries. The company provides systems for both standard and customised development projects and is a sought after solutions provider for its ability to addresses unique problems in specialised areas.

The challenge
In agriculture, Shock Wave Engineering focuses on reducing the water usage per unit of crops produced, as well as improving the energy efficiency and maintenance needs of the pumps used for centre pivot irrigation systems. The company had previously developed its own cloud platform to achieve this goal, but experienced serious scalability and flexibility limitations.

There are several variables influencing a pivot system’s efficiency (e.g. worn pumps, incorrect pump sizes, small or blocked pipelines, and excessive pivot pressure among others). Therefore, running pivot systems sub-optimally results in high energy consumption, unnecessary water usage and increased maintenance costs. The result is a reduction in farm profitability. A broken pump or pipe, at a critical time in the growing phase, can lead to crop failure. Similarly, over or under-watering could have the same result.

The solution
To overcome the scalability and flexibility issues, as well as assist clients to optimise their water and energy usage, Shock Wave Engineering uses the PTC ThingWorx platform, supplied by 1Worx in sub-Saharan Africa. The ability to have real-time visibility into a system’s performance, to identify system bottlenecks and improve operational efficiencies, is a core feature of the Shock Wave system. It also provides actionable insight through the use of real-time alerting, making it possible to respond quickly to problems, and to manage by exception, saving time, effort and money.

The result
Since implementing the ThingWorx based Smart Connect Pivot Irrigation System, Shock Wave Engineering has been able to improve client water and energy consumption with a typical energy savings of around 40%, and a guaranteed energy savings of 15%. One of its clients saves the equivalent of a dam full of water every two years. This smart digital solution reduces the energy, water and maintenance requirements of irrigation systems in the agriculture industry, thereby reducing the cost per unit of produce.

ThingWorx platform
The ThingWorx Industrial Innovation Platform is a complete, end-to-end technology solution that enables industrial businesses to unlock the value of the IoT. It delivers the tools and technologies needed for rapid development and deployment of powerful applications and augmented reality (AR) experiences.

The platform includes compatible modules that deliver the functionality, flexibility and agility enterprises need to implement IoT apps and AR experiences. This includes industrial connectivity, analytics, application enablement, orchestration and AR authoring.

ThingWorx delivers:
• Purpose-built platform: the platform contains specific functionality designed with the scalability and security to grow as a business expands.
• Rapid development, deployment, and extensibility: platform modules come together via the ThingModel – a true digital representation of a physical object – enabling apps and experiences to be delivered quickly and easily.
• Ultimate flexibility: the platform can be deployed in the cloud, on premise, or a hybrid of the two. Apps and experiences are made available to users in multiple formats – desktop, web and mobile and AR. Integration with external data sources simplifies processes and ensures more meaningful results.
• Vibrant ecosystem: ThingWorx partner ecosystem offers one of the world’s largest networks of IoT-focused companies, and ThingWorx partners offer a wide range of products and services that simplify, accelerate, or enhance processes and strategies for industrial IoT.

Industrial connectivity
The Industrial Internet of Things leverages existing technologies in industrial settings – including machine-to-machine communication and automation technologies – and incorporates newer big data and machine learning technologies to enable smart, connected machines.

Meet 1Worx
1Worx is the sole ThingWorx supplier for sub-Saharan Africa with a client base that includes companies in the mining, agricultural and manufacturing industries. 1Worx has a highly competent team of subject matter experts that includes certified ThingWorx associate developers, as well as a certified ThingWorx trainer. 1Worx prides itself on creating awareness around Industry 4.0 in South Africa through programmes at academic institutions and ThingWorx training.

For more information contact
Duan Gauché, 1Worx, +27 (0)83 327 7069, duan@1worx.co, www.1worx.co
Safe landing every time

Aeronautics research institute studies aircraft braking operations using simulation software from Siemens.

The Brazilian Aeronautics Institute of Technology (ITA) is involved in training, research and technological development in the field of aeronautics. The ITA attaches particular importance to fostering links between research and industry and works in close cooperation with the Brazilian Government to ensure that research aligns as closely as possible to the needs of industry. Issues currently in the spotlight are brake system performance and anti-skid technology in normal and failure modes. To play through possible scenarios, the ITA relies on the use of simulation software from the Siemens PLM Software Simcenter portfolio. This allows students at the ITA to gather experience with the latest features of the advanced simulation setup during their course training. Quite apart from this benefit, ITA has also been able to speed up the evaluation of brake system performance under failure conditions, helping to strengthen Brazil’s position in the highly competitive aeronautical industry.

Aircraft brake systems are not only highly complex but also crucial to aircraft safety. The blocking of brakes during braking manoeuvres, for instance, must be avoided at all costs. Traditionally, brake system performance has always been tested by executing multiple load rig tests and test flights. This is time-consuming and also a costly process, which explains why the research team at the ITA set about looking for a new method that would involve simulation of the aircraft’s hydraulic brake system. A study carried out by the ITA demonstrated the usefulness of system simulation to design and validate the model of a hydraulic brake system in order to assess functionality in both normal operation and in the event of a failure. The experts at the ITA used the LMS Imagine.Lab Amesim from Siemens PLM Software to model the hydraulic system.

Computational parameterised model
The researchers at ITA decided to base their study on a braking system supplied with power by the aircraft’s own hydraulic power generation system. This system is later duplicated to independently provide hydraulic power to each brake. The model generated in LMS Amesim is composed of three elements: the valve assembly, the brake assemblies and the input blocks. “LMS Amesim is a great tool for quickly creating system models, mainly due to its facility for dealing with the physical blocks found in its software libraries,” says Mario Maia Neto, a PhD candidate at ITA. As he explained, this enabled the creation of complex models without the need to write entire mathematical formulas for each subsystem. Using LMS Amesim helped ITA develop a computational, parameterised model for the aircraft hydraulic brake system to assess the behaviour of its relevant variables in normal operational conditions, as well as when typical failures are simulated.

Potential far from exhausted
Subsequently the results were compared in order to find a way of compensating for the loss of performance in the ‘failure mode’. The last step of this computational method was to devise a strategy or actions such as the definition of specific maintenance tasks to maintain the required system level. Neto envisages enormous potential for the new methodology. “In the current context, modelling and simulation has the potential to improve the execution of several design development activities, such as system architecture study, requirements validation, performance analysis and optimisation, safety and assessment, fault detection and diagnosis,” he concludes.

Using LMS Imagine.Lab Amesim from Siemens PLM Software, the experts at the ITA are able to quickly and simply generate a virtual model of a hydraulic aircraft brake system. The model – composed of the valve assembly, brake assemblies and input blocks – is used to analyse brake system performance and anti-skid technology in the normal and failure modes. The brake’s normal torque response can then be directly compared to braking behaviour in the simulated failure mode.

For more information contact Jennifer Naidoo, Siemens Digital Factory and Process Industries and Drives, +27 (0)11 652 2795, jennifer.naidoo@siemens.com, www.siemens.co.za
Cables for robots in the Industry 4.0 era

It’s a time of revolution in industry – automation, digitalisation and Industry 4.0 are just some of the current buzzwords. Robotics is an area that is developing rapidly.

Worldwide, annual growth in the installation of industrial robots has been 16% since 2010. The automotive industry continues to dominate, but other sectors are catching up, with use in consumer electronics increasing sharply. As part of this trend, small and medium-sized producers are increasingly investing.

Manufacturers of robots are responding with new models that are more compact, more versatile and last longer. In the past, robots would be replaced when a product generation was phased out, but today they are taking on new tasks and these change more frequently than before. The variety of movements means that the loads on certain components are increasing, particularly the cables. They perform torsion and kinking movements, frequently a mixture of the two, and with different bending radii and torsion angles as well.

Standard cables often unsuitable
Lapp has numerous robust cable types in its standard range, which have performed for years without failing on many robots. However, these standard cables are not always suitable for special applications such as those outlined above, and these applications are on the increase. This is where cables uncompromisingly tailored for a specific use come into play. For cable manufacturers, robotics is the supreme discipline.

The most important difference between robot cables and conventional moving cables is that the former have to withstand both bending and torsion over their entire service life, and in development they are designed fundamentally differently to a power chain cable, for example. There are three key parameters:

Braided conductor class
Robot cables should have at least class 6 conductors, which are designed for continuous movement in line with the standard. Lower classes are less suitable, or totally unsuitable. However, sometimes even braided conductor class 6 is not sufficient. For cables that need to be highly bendable and twistable, Lapp uses braids outside the standard in which the individual wires are just 0,05 mm thick, considerably thinner than the thinnest braided wires covered by the standard.

Torsion angle
A typical value is ±360°/m, which means that a cable can be twisted one full revolution to the left and once to the right about its axis per metre of cable length. This applies to cables without shielding. With shielding the value is typically ±180° or half a turn per metre.

Bending radius
Ideally, this is between four and 7,5 times the outer diameter and thus in some cases lower than for cables that are only subjected to occasional movement. This allows the cables to be coiled in tight radii and in tightly packed hose assemblies.

Three times about its own axis
For some applications, even these properties are not sufficient. For these, Lapp supplies special cables qualified for even higher torsion angles, including a cable for a 3D laser welding robot that allows torsion of over ±1000°/m. This means that the cable can be twisted almost three times about its own axis. This is unique worldwide. For the robot concerned this is definitely not overkill, as the robot arm moves completely freely in three dimensions, twisting several times about its own axis.

The amazing thing is not the sheer extent of the torsion angle, but the fact that this movement is possible over many years with no deterioration in properties. This particular cable is qualified for a minimum of seven million cycles, proved by tests at the Lapp testing centre, which is currently being extended for even more dynamic movement tests. Another special robot cable is certified for over 15 million cycles and, with ±720°/m, allows two turns about its own axis per metre. To create cables capable of handling such extreme loads, the Lapp engineers have to dig deep into their
box of tricks. For the cable discussed above with a ±1000°/m torsion angle, for example, braids made of a special copper alloy were used. They retain their minimum electrical resistance even when bent or twisted and after a large number of movement cycles.

**Sophisticated construction**
These properties can only be achieved with a sophisticated and complex cable construction. There are several factors that can be influenced:

- **Stranding types:** Bundle stranding is usual for robot cables, with the individual conductors combined in one or more bundles. These cables withstand both bending and torsion. If the electrical properties demand it, for example for data or servo cables, cables suitable for use on robots are stranded in pairs.

- **Core insulation:** The insulation of the cores has to be able to withstand several million movement cycles. The best solution is a thermoplastic elastomer, or TPE.

- **Sliding support:** Elements help the components in the cable to move against each other with as little friction as possible. They also act as a filler to make the cable circular. Sliding supports can be stranded plastic fibres that fit into the gaps or voids between the cores. Correct placement of these filler fibres requires a high degree of know-how. Thicker cores are often wrapped in a polytetrafluoroethylene or polyester film fleece wrapping to make it easier for them to slide against one another, particularly under torsion.

- **Shielding:** Tests have shown that under torsion the gaps in the braided shield increase in size over time, because the small wires that make up the braid are pulled apart by the torsion and break over time. This pushes up the contact resistance, which has a detrimental impact on the desired shielding effect. Above half a million torsion cycles, spinning with copper wires is superior to braiding. All the wires point in the same direction and the contact resistance hardly changes over the service life.

- **Outer sheath:** Here, as in many industrial applications, the material of choice is the very robust polyurethane (PUR).

**Thinner is better**
Customers are increasingly expressing a demand for the cables to be as space-saving as possible because robots are getting smaller all the time. Increasingly, hybrid cables are being used, containing all kinds of cables such as power, data and signals, and even hoses for pneumatics or the air or protective gas supply. For example, Lapp has developed cables for a welding robot that contains dozens of cores for power, signals and industrial Ethernet in a single sheath. Although some of these hybrid cables are 30 millimetres thick or even more, they take up 30% less space than laying individual cables.

As the requirements for robot cables are so diverse, extensive tests are unavoidable for the manufacturers. However, many cable suppliers also have high minimum order quantities, in some cases several kilometres. In the case of Lapp, sample lengths starting at 100 metres are possible. This enables manufacturers to carry out tests without having to spend a lot of money on the cables.

For more information contact Lapp Group, +27 (0)11 201 3200, info@lappgroup.co.za, www.lappgroup.co.za

---

**Festo**

**Modular control system CPX-E**

Compact and inexpensive!

You want easy and seamless connectivity? You are looking for lasting and compatible concepts? We connect the present to the future.

→ WE ARE THE ENGINEERS OF PRODUCTIVITY.

Intelligent communication amongst all control partners: that's what connectivity with Festo is about!

The powerful automation system CPX-E with EtherCAT® master controller and motion controller with IP20 protection provides central control of automation solutions in handling technology. Several bus modules are available so that it can be configured as a compact, low-cost remote I/O.
Bringing the connected enterprise to life

Rockwell Automation simplifies analytics for industrial productivity.

Industrial organisations must be able to identify ways to tighten production schedules and maximise revenue. Gaining insight into operations and production capabilities to make informed decisions has often involved time-intensive IT projects and a highly specialised skillset. Today, Rockwell Automation has expanded the FactoryTalk Analytics portfolio, a robust advanced analytics environment that empowers users with the ability to make informed decisions. These latest advancements were developed to reduce the complexity of the operations environment for manufacturers and producers and their employees who are driving operations.

FactoryTalk Analytics has been developed for scale, discovering and connecting data sources from the edge of the network up through the enterprise, and then intelligently fusing the information to resolve issues close to the source. At the edge or device level, this can result in near-immediate resolution of production issues. Empowered with machine learning capabilities, FactoryTalk Analytics learns the process and looks for trends in the data, proactively presenting users with insights before an issue arises.

FactoryTalk Analytics brings contemporary user experience capabilities, which are common for consumer experiences, to the production environment. Focused on driving ease of use and productivity, it features Internet-like search capabilities of production data, as well as self-serve drill-downs, allowing the user to make data-driven decisions quickly. Rockwell Automation has chosen the Microsoft Azure cloud as the preferred platform, to help develop and power advanced IIoT solutions.

In one pilot project, a manufacturer of solar panels used FactoryTalk Analytics to connect the data sources of legacy systems spread across multiple facilities. They are now able to more efficiently manage data both on premise and in the cloud, which minimises downtime and saves significantly on IT spend.

In another pilot, a global automotive manufacturer implemented FactoryTalk Analytics to help improve operational productivity. Purpose-driven applications brought data together from disparate systems, which had previously proven difficult to integrate and had limited workers’ ability to investigate production issues. The solution is giving production managers and executives new visibility into key areas of operations, and helping them more accurately forecast production targets.

“Smart manufacturing promises to remove blind spots between organisational silos, putting users directly in touch with information,” said Christo Buys, business manager control systems, Rockwell Automation Sub-Saharan Africa. “Our deep experience in production applications, coupled with technology that integrates control and information, provides outcomes of increased productivity for both existing and Greenfield sites. Importantly, our partners are taking advantage of these solutions to enhance the value of their own offerings.”

For more information contact Christo Buys, Rockwell Automation, +27 (0)11 654 9700, cbuys@ra.rockwell.com, www.rockwellautomation.co.za

Yokogawa launches amnimo

Development of new services that will leverage IIoT architecture.

Yokogawa has announced the launch of amnimo Inc., a business unit that will be tasked with identifying, developing, and offering services that can add value by leveraging the IIoT architecture currently under development. The first of these services are scheduled to be rolled out later this year.

Objectives of launching the company

In November 2016, Yokogawa set up a new division on the US West Coast, Architecture Development Division California, to develop a robust and flexible foundation for the provision of new IIoT services. Based on a collaboration agreement concluded in February 2017, this division began partnering with Microsoft and other leading IT companies to develop a secure and easy-to-use IIoT architecture for customers.

The launch of amnimo Inc. to identify, develop, and deliver IIoT architecture-based solutions is one of the measures that Yokogawa is taking under its new Transformation 2020 mid-term business plan to enable its customers to achieve a transformation in their businesses. By simplifying its business processes, the company will be able to speed up decision making and respond promptly to swift changes in the market environment. Also, it is expected that this company will be able to build strong relationships with customers and partner companies in various fields by working closely with them to co-create IIoT technology solutions that deliver new forms of value.

For more information contact Christie Cronje, Yokogawa South Africa, +27 (0)11 831 6300, christie.cronje@za.yokogawa.com, www.yokogawa.com/za
How secure is the smart factory?

Secomea provides secure remote access without the need for advanced firewall configuration.

Industry 4.0, IIoT and the connected factory are beyond the point of just being buzzwords. In reality, they offer huge opportunities for manufacturers. But as a smart factory goes online, how secure are communications in and out of the site? How can companies enable remote access and protect themselves against cyber threats at the same time?

Remote access to machines has become vital for OEMs and system integrators to meet response-time and up-time obligations. Engineering resources and budgets are limited, therefore efficiency is key. Resolving issues without the need for onsite visits saves time and money, but as businesses embrace connectivity, the threat of a cyber attack increases. Protecting data when connected to a network can be a complicated challenge.

Cyber security is top priority for the Danish solution, Secomea. Designed specifically for remote programming, monitoring and data-logging, it provides secure remote access without the need for advanced firewall configuration.

Moving on from VPN

Traditional VPN technology is widely used and suits the job of connecting networks remotely or providing remote access to a central site. However, it has some serious limitations for remote device monitoring and management.

VPN solutions can be complex. Connecting different engineers to different sites around the world by traditional VPN solutions would be an onerous task. Setting up a VPN is resource heavy, time consuming and requires the involvement of IT personnel. Subnet conflict issues, firewall setups and single level authentication can also trigger security concerns.

Secomea has developed an Internet-based technology that specifically addresses the security and usability requirements of linking service engineers with industrial equipment.

Each machine has a SiteManager, a small piece of hardware that the engineer connects to and uses to control the machine. The SiteManager can connect to industrial equipment via LAN, serial or USB ports. There are also multiple Internet access options including LAN, 3G and 4G or Wi-Fi. The LinkManager Windows based client provides (VPN-like) access to serial and USB devices, no configuration is required. A web version, the LinkManager Mobile, can be operated from multiple platforms with a browser allowing users to remotely access equipment via a phone or tablet.

The solution also includes a GateManager, a M2M server that is either hosted by Secomea, or by the customer themselves. All communication between the factory and the engineer through GateManager is via an encrypted connection. Through the web-based GateManager Portal, users can administer accounts, manage SiteManagers, and also manage devices. It is straightforward to determine who has access, what equipment and which sites can be accessed, and also when and for how long that access remains active. The engineer can securely log on to the system via a X.509 certificate and associated password. GateManager also logs all events.

Secomea has two- and three-factor security authentication, event audit trails, role-based account management and standard measures for eliminating the risk of vulnerabilities from configuration or human errors.

Future-proofing

Secomea says it has achieved Industry 4.0 certification by enabling these connections in a secure way. Unlike an open VPN network, restricting access to certain devices for a specified time is easily achieved using a simple folder, and drag and drop system.

The development of smart factories offers significant benefits for the automation industry. If companies are to take full advantage, they must make timely decisions about how to utilise new technology that is designed to keep those connections secure.

Secomea has not only made its system secure, it has also utilised third-party test laboratories to assess its system and ensure they comply fully with the requirements of Industry 4.0. Unfortunately we live in an age where criminals, fraudsters and hackers have upped their cyber game. No one can afford vulnerabilities in their system.

New technologies afford many benefits, but they need to be kept secure and stay ahead of the threats.

For more information contact Bob Petrie, Throughput Technologies, +27 (0)11 705 2497, bob@throughput.co.za, www.throughput.co.za
Parts of the so-called ‘smart factory’ are already reality, and many processes and functions between information and operations spheres are becoming increasingly coordinated.

At the centre of implementing Industry 4.0 is the requirement for intelligent and communication-enabled sensors to provide the smart factory with the data it needs. A communicating, intelligent sensor network, where sensor data is exchanged with a machine controller, or a cloud-based application, allows automatic adaptation of process parameters to new production orders within seconds. That means increased agility and better process efficiency across the enterprise.

Best-in-class sensors
‘Sensor Intelligence’ has been at the core of the SICK brand since 2004, manufacturing sensors that are best in their detection class. They also support the communication standard IO-Link, in whose development SICK played a major role. They become smart through wide-ranging potential for self and process diagnosis, and through integrated logic functions for processing signals directly at the sensor itself.

However, what, in concrete terms, does intelligence through diagnostic capabilities and integrated functions mean in the context of the smart factory? Smart photoelectric sensors, for example, can detect patterns in an object structure and any changes in them. This takes place directly and autonomously in the sensor – not in the PLC. Machine processes are therefore accelerated and the control program streamlined. This means greater plant efficiency and lower costs for customers. The wide-ranging diagnostic functions of smart sensors can detect critical situations, and correct them, promptly, before the machine experiences an unplanned stoppage. This increases operating reliability, and thus the productivity of the entire plant.

An example of the benefit of upgrading to smart sensors can be seen in the case of inductive devices. The SICK portfolio includes a range of inductive smart sensors that, for example, detect the distance between the object and the sensor. They can detect when machine processes deviate from the target state and provide a warning in good time, or even make autonomous statements regarding product quality.

Smart sensors for the smart factory
Ultimately consumers also profit from intelligent sensors and dynamic interactive production processes. The key term is batch size 1. Many people are searching for ways to express their individuality. They want to have products that are perfectly adapted to their individual needs. Such true one-offs are either impossible or very expensive using classic production structures. This is where smart sensors can open up new innovation potential.

Furniture, for example, can nowadays be configured on the Internet. Dimensions, design elements, the type of wood and colours can be freely selected, combined, and ordered. The customer order reaches the production system and the machines via the network. The machines are equipped with intelligent sensors that the controller can parameterise appropriately for the particular product, so that the desired piece of furniture can be produced automatically. Production, inspection, packaging and dispatch all take place according to that individual order – and without any manual interventions. The customer receives their personal one-off piece at the price of a mass-produced item.

This, however, is by no means the limit of the potential of smart sensors. Structures that are more autonomous; plants and factories with greater networking; production (and products) that involve more software and IT – all this can already be seen, and makes smart sensors a critical technology of future production processes. Flexibility will therefore be in greater demand in future. Highly individualised requirements will mean manufacturers have to be able to react rapidly and precisely to each specific requirement. This will lead to a continuing demand for new functionality in sensors that will keep getting smarter.

For more information contact Mark Madeley, SICK Automation Southern Africa, +27 (0)11 472 3733, mark.madeley@sickautomation.co.za, www.sickautomation.co.za
EtherCAT: the rock in the surf of digital transformation

Industry 4.0 is the digital transformation that is characterised as the fourth industrial revolution. The perception of a revolution is that it is a fast process, dramatically changing the current situation within months, not years. However, industrial revolutions are comparatively slow processes. The first industrial revolution – the transition from agricultural to industrial society – took over 100 years. Although the fourth revolution is much faster, it is also a process that will take decades to become fully operational.

A large part of Industry 4.0’s concepts and approaches are based on industrial communication: data must be collected at the manufacturing processes, condensed and then sent upwards into databases, towards servers, and into cloud based systems. Conversely, commands and recipes are sent to the machine and plant controllers, which then implement and execute them. In order to manage and control this amount of data, a hierarchical architecture and structure is required. At the field level, it is important to communicate in hard real-time, whereas further up the time requirements are more relaxed. And currently, in particular at the level between the controllers, servers and Internet services, much is still unclear with regards to the communication technologies. OPC UA with its different protocol variants continues to gain ground at this level, but device profiles and real-time capability are still missing. TSN is a promising emerging technology, but it is not yet finalised, and there is still specification work to be done, especially for the system configuration. Different cloud protocols, encoding schemes and cloud providers are competing and unified interfaces have not yet been established.

So it is good that things look different at the field level: EtherCAT is stable, widely adopted and ideally prepared for the challenges of digital transformation. The EtherCAT technology has outstanding characteristics, including leading performance, high flexibility and open interfaces. As a result, EtherCAT is inherently suited to meet and exceed the requirements of the digital transformation. The exceptional performance of the technology allows one to add Big Data applications to control networks. In addition, the flexibility of EtherCAT makes it possible to establish cloud connectivity in existing systems without having to alter the control system, or manually update the network devices. The open interfaces permit the easy integration of any IT-based protocol within the master, or directly into the slave devices. Ultimately, this enables direct connection from the sensor to the cloud without protocol discontinuities, regardless of which protocol eventually becomes the winner on the level above the EtherCAT system.

For more information contact EtherCAT Technology Group, +49 911 540 56 226, press@ethercat.org, www.ethercat.org

One network, all options
Make the most of all the options offered by your Ethernet network.

Industrial Ethernet components from Phoenix Contact offer you more real time, more wireless, more security, and more availability. Integrate industrial Ethernet components from Phoenix Contact with ease into your automation infrastructure and benefit from our many years of experience.

For more information:
JHB: 011 801 8200
DBN: 031 701 2701
www.phoenixcontact.co.za

CT: 021 930 9666
PE: 041 364 0415

www.instrumentation.co.za  Technews Industry Guide: Industrial Internet of Things & Industry 4.0  33
Effective plant asset management

Siemens offers an ideal solution for the efficient monitoring of intelligent field devices.

With its Simatic PDM Maintenance Station V2.0, Siemens provides the ideal solution for efficient monitoring of intelligent field device statuses independently of the automation and control system used. Their integration is based on DD (Device Description)/EDD (Electronic Device Description) technology. Diagnostic, parameterisation and status data from the field devices is read out cyclically and depicted in a clearly arranged format. The collected data can also be transferred using an export function for further processing in enterprise asset management or cloud-based condition monitoring systems. Version 2.0 has been further developed to comply with Namur recommendations NE 105, NE 107 and NE 129.

The Simatic Process Device Manager forms the basis for data and status monitoring of smart field devices in the maintenance station. Simatic PDM is a universal, manufacturer-neutral tool used for project engineering, parameterisation, commissioning and monitoring of intelligent field devices and field components. It supplies diagnostic data, status data and parameter data to the Simatic PDM Maintenance Station, where the information is processed and supplemented by functionalities such as overview or work progress lists, overview, segment and detailed images, status logs, parameter data archiving, global and device-specific message lists as well as cyclical functions for reading out or exporting field device information.

Maintenance and servicing system

The maintenance and servicing system is designed for use by small to medium-sized enterprises or production plants used for processes such as hybrid or biogas, wastewater treatment, painting lines in the automotive industry or paper manufacturing. The Simatic PMD Maintenance Station can also be used in specific plant sections. Version 2.0 of the Simatic PMD Maintenance Station can be used wherever intelligent field devices are in operation. The system is optimised for up to 500 field devices, and it is also possible to combine several Simatic PMD Maintenance Stations within one plant.

In production plants with Simatic automation stations, the Simatic PDM Maintenance Station is directly connected to the plant bus, and so communicates over the automation stations with the field devices of the lower-level field bus systems. In addition, a separate network can be created to the field devices if direct access is not possible.

The Simatic PDM Maintenance Station offers the same functionality and user guidance as the Simatic PCS 7 Maintenance Station, which is recommended for larger-scale applications using Simatic PCS 7 as a control system. “The special feature of the Simatic PDM Maintenance Station V 2.0 is that it can be used independently of Simatic PCS 7,” says Siemens product manager Holger Rachut. “Even if it is not integrated into a Simatic PCS 7 project, it can use the existing infrastructure of a Simatic S7/PCS 7 project, or create its own communication infrastructure. It makes no difference how the field devices are connected, for instance using Profinet, HART or Ethernet.”

The compact Simatic PDM Maintenance Station is flexible and offers scope for expansion. It can even be used several times over within a single project for different tasks, for instance as a diagnostic station for sub-plants or a data collector for selected field devices. Used as a data collector, the Simatic PMD Maintenance Station enables the cyclical capture and transmission of identity, event and parameter data to the relevant data evaluation systems.

In its recommendation NE 107, Namur has defined four status signals to be used for project engineering, parameterisation, commissioning and status data to the relevant data evaluation systems. For more information contact Jennifer Naidoo, Siemens Digital Factory and Process Industries and Drives, +27 (0)11 652 2795, jennifer.naidoo@siemens.com, www.siemens.co.za
Alongside serial production, there is a trend in industry towards the customisation of products. A key role when it comes to production in batch size one, besides the digital networking of entire installations, is also played by systems capable of learning using artificial intelligence and robots that work hand in hand with humans. In the BionicWorkplace, all these requirements are combined in a future oriented working environment.

**BionicCobot: robot arm with human movement patterns**
A central part of the working environment is the BionicCobot. This pneumatic lightweight robot is based on the human arm in terms of its anatomical construction and – like its biological model – solves many tasks with the help of its flexible and sensitive movements. Due to its flexibility and intuitive operability, the BionicCobot can interact directly and safely with people. In doing so, it supports workers doing monotonous jobs and takes over tasks that are dangerous for humans.

**Intuitive operating concepts for safe interaction**
In the BionicWorkplace, the bionic robot arm works together with numerous assistance systems and peripheral devices, which are networked and communicate with each other. At the same time, artificial intelligence and machine learning methods turn the BionicWorkplace into a learning and anticipative system that continuously optimises itself. The whole workplace is ergonomically designed and can be adapted to people individually down to the lighting. At the centre of the worker’s field of vision is a large projection screen. It supplies the worker with all the relevant information and reacts dynamically with its contents to the relevant requirements. All around the projection screen, various sensors and camera systems are fitted, which constantly record the positions of the worker, components and tools. In this way, a human can directly interact with the BionicCobot and control it using movement, touch or speech.

**Recording the worker’s position using wearables**
The system recognises the worker and their movements by their special work clothing. These so-called wearables consist of a long sleeved top, which is equipped with inertia sensors, and a work glove with integrated infrared markers. With the help of the recorded sensor data, the BionicCobot is able to hand over objects to its human colleague with pinpoint accuracy and move out of their way if necessary – an essential requirement for direct collaboration between humans and robots.

**Machine learning optimises work flow**
The intelligent software simultaneously processes all the camera images, positional data and inputs from the various peripheral devices. It uses all this information to derive the optimal program sequence. The system then divides the tasks expeditiously to the robot and other tools in order to give the human the best support whilst working.

With every action solved, the system learns something new. This creates a semantic map that grows continuously. Along the network paths, the stored algorithms constantly draw dynamic conclusions. As a result, a controlled, programmed and set sequence gradually turns into a much freer method of working.

**Remote manipulation via virtual-reality goggles**
Another element of the intuitive operating concept is remote manipulation. For this purpose, a 3D stereo camera with a viewing angle of 180 degrees records the whole working space. At the same time, the worker, who is spatially separated, wears virtual-reality goggles besides the textile wearables. The worker can use these to access the images from the camera in real time and follow them. In this way the robot can be controlled in case of spatial separation or from a safe distance.

**Learned knowledge building blocks applicable worldwide**
By means of intelligent workplaces capable of learning, such as the BionicWorkplace, and the use of multifunctional tools, collaboration between humans and machines will be even more intuitive, simple and efficient in future. Knowledge building blocks and new skills, once learned, can be limitlessly shared and made available on a global scale. It would therefore be possible in future to set up workplaces as a worldwide network with local adaptations, in each case adjusted to the local individual tasks and customer requirements.
The Internet of Things (IoT): a world of connected devices, smart factories, cities and homes all powered by the latest technologies available from RS.

Get everything you need to bring your IoT project to life

- Capacitors
- Development Kits
- Inductors
- PCB Connectors
- Power Management ICs
- RF and Microwave ICs
- USB, D-Sub & Computing Connectors
- Data Converters
- Discrete Semiconductors
- Low Power RF Modules
- Microcontrollers
- Resistors
- Sensors

South Africa: www.rsonline.co.za
Email: sales.za@rs-components.com

Africa: www.rsonline.africa
Email: africa@rs-components.com
Tel: +27 11 691 9300
RS Components SA, No.20 Indianapolis Street, Kyalami Business, Midrand 1684 , South Africa
Raspberry Pi 3 Model B with 802.11 b/g/n Wireless Lan and Bluetooth 4.1 perfect for IoT projects.

SX1276MB1MAS long-range LoRa™ technology evaluation module ideal for IoT connecting sensor circuits and wireless battery powered end points in an IoT network.

The Neural Network Compute Stick from Movidius™ allows Deep Neural Network development without the need for expensive, power-hungry supercomputer hardware.

The IoT 2040 is an open and flexible IoT gateway that is designed for continuous industrial operation and comes with the appropriate certificates.

The boards offer a platform for connected things with multiple communication standards. Using the Espressif ESP32 chipset dual processor, that can connect devices via WiFi, BLE, LoRa and Sigfox.

Low power, compact, BLE connectivity and click™ board compatibility.
There has been a significant transition towards industrial Ethernet networks over the past few years with large vendors making an aggressive push to swap existing fieldbus infrastructure for Ethernet-based technologies. The promise of Industry 4.0 and the IIoT is that they can harness this shift, along with the global connectivity platform of the Internet, and recent IP stack extensions such as Time Sensitive Networking (TSN), to enable organisations to establish operational efficiencies and supply chain optimisations not previously achievable.

However, many industry pundits acknowledge that fulfilment of this promise will take time and considerable investment and understanding of the myriad of dynamic interdependencies that make implementation complex. The disparate levels of digital maturity of people and processes further exacerbate the challenge. There is still a need to identify and address the issues that cripple continuous improvement – often there is a simple answer waiting to be unravelled. Yes, the 80/20 rule still applies, so identify the low hanging fruit and take advantage of the same underlying technology improvements that will support Industry 4.0.

Rather than try and get ‘there’ in a single leap of optimism, there are many intermediate steps and knowledge acquisition and preparation that can be undertaken to enable the transition to take place with value being realised each step of the way.

Let’s consider just two of these:

**Disparate systems: phased migration, the blending of modern and legacy systems**

Vendors, wanting customers to adopt their latest offering, often motivate for a complete upgrade – out with the old and in with the new. While the cost of installing a new industrial Ethernet system does not vary greatly from installing a modern fieldbus network, the cost of replacing a fully functional fieldbus with a newer technology is a significant cost. This comes as both an upfront capital cost (purchase modern technology, system design, installation and commissioning time) and operational cost (extensive initial downtime and production loss, and the need for training). Improved operations over time hopefully mitigate this investment.

Operators of manufacturing facilities, while desiring improved operations, also need to sweat their existing assets and try to reach their design life of 20 to 50 years, without being drawn into making such major changes that introduce capital cost and impact production availability. The ability to migrate slowly over time, blending modern technology with legacy components should be an attractive compromise. Rather than, as networks reach end of life, and budget is made available, plants could opt to upgrade small portions of the entire network and maintain communication between the different systems with the use of gateways and protocol converters. This allows a more manageable transition with the advantage of keeping operations largely unaffected.

**Upgrading I/O: keep the existing control system**

Consider the case where the actuators and sensors are the first to be upgraded on a network and the existing PLC/DCS system is to remain running the plant. Without having to migrate or renew the controller’s logic, users can integrate a gateway device to transfer I/O from upgraded sensors and actuators. In this scenario, the gateway acts as an Ethernet/IP scanner and cyclically transfers data from connect I/O to the Profibus PLC.

A second scenario is where the control system can be upgraded to a newer technology while the existing field infrastructure remains intact, especially expensive components like drives and process analysers. For example, Profinet and Profibus, the gateway in this scenario will act as a Profibus master, scan the configured I/O from each of the devices connected and in turn make this available for the ‘new’ Profinet PLC system.

**Remote assistance, asset optimisation and permanent monitoring**

It is certainly no secret that there is an engineering skills shortage across all industries, and this is especially true with respect to automation systems based on modern communication technologies. It is becoming more and more challenging to have staff at remote facilities all trained and experienced on both legacy and modern technology.
While it remains true that relevant and effective training on these technologies by site staff is still a key operational component, it is now possible to supplement these local skills with insight and expertise from elsewhere. It is possible to establish secure remote access to site information that provides real-time performance metrics for networks, equipment, production output and quality, such that a pool of human expertise, along with machine learning and other artificial intelligent tools can be applied against similar plants geographically dispersed around the world. Proactive and reactive intervention can be triggered almost immediately without the time delay, health/safety risks and costs of travel to these locations.

The use of IIoT edge devices, OPC-UA, MQTT, FDI/FDT and other software tools enables a geographically-displaced community to effectively collaborate and share information and experience and further justify the continuing adoption of tools and methodologies that bring Industry 4.0 closer to realisation.

**Industry 4.0 is real and promising but be prepared to grow into it gracefully and pragmatically**

Every organisation has its unique pain-points and opportunities for improvements. Here in South Africa, we believe that two useful stepping stones to Industry 4.0 adoption are:

- Keep sweating plant assets and blend legacy automation components with modern industrial Ethernet systems at a pace that makes sense.
- Make use of secure remote access and site monitoring tools to allow rapid response by outside expertise to site issues that affect equipment availability, production efficiency, product quality and personal safety.

For more information contact Industrial Data Xchange, +27 (0)11 548 9960, info@idx.co.za, www.idx.co.za
Sensorik 4.0 provides added value for intra-logistics

Networked logistics systems as well as digitised processes and applications require future-proof sensors and communication solutions.

Experts agree, Industry 4.0 and the smart factory of the future have arrived. The drivers behind the development, even in logistics, are the best possible levels of flexibility, transparency, plant availability and increases in productivity. The digitisation of intra-logistics and supply chain requires high-performance bidirectional communication and data security, even at field level. Pepperl+Fuchs is tackling these challenges with its Sensorik 4.0 portfolio, which includes sensors for detection and measurement tasks, as well as identification and infrastructure.

Comprehensive communication capability is achieved with the IO-Link interface and thus fulfils a crucial requirement for Industry 4.0 components. IO-Link allows a standardised data exchange between field devices and control systems. In addition to sensor measurement values or setpoints for actuators, information on the identity and status of components can be exchanged, while adjustment parameters can be transmitted from the controller to the sensor or actuator.

Components such as the optical sensors of the R100, R101 and R103 series, can be adapted and optimised for various use cases with a wide range of parameter settings. IO-Link enables various process-relevant sensor parameter sets to be stored in the automation system. During operation, these can then be loaded into the sensor on the conveyor line or in the rack storage without losing any time. Any number of sensors can be adjusted flexibly and simultaneously directly from the controller by downloading parameters such as sensing range, hysteresis, and switching threshold. This saves time, avoids errors, and can be documented at any time.

Tools such as SmartBridge are available for visualisation, testing, and optimisation of parameter settings. The SmartBridge adaptor can be used as a smart data-logger for recording sensor data over extended periods of time. It can also be mounted in a plant temporarily to spot intermittent faults.

Self-diagnosis optimises availability

Smart sensors such as the R2100 multi-beam 2-D LiDAR sensor, are robust and are used in warehousing and material handling to check for occupied spaces, among other things. They also calculate diagnostic information internally, such as a functional reserve value, which can be evaluated as a measure of reliable sensor operation. This makes it possible to record environmental influences such as dust, cardboard abrasion, moisture and vibration, which automation components are exposed to continuously in intra-logistical systems.

If one of these smart sensors indicates that the automation system is experiencing, or will experience, a functional impairment, remedial measures such as cleaning or readjustment can be initiated promptly before plant downtime occurs.

If sensor replacement is required, this can be carried out quickly and easily through the IO-Link communication: after connecting the replacement sensor, this is tested and confirmed by the automation system. Then, the last valid application-specific data from the previous sensor is taken from its digital twin and transferred directly into the new device. Additional manual settings are not required, meaning the conveyor or buffer section is available again with little or no downtime.

Smart sensors relieve automation systems

Through increased use of digitised and decentralised sensor information, functional local control loops can be established. In doing so, Sensorik 4.0 is pioneering technology for the self-organising factory. In conjunction with other communication-capable and intelligent sensors or actuators, self-contained functions can be carried out. For example, if a smart 3-D camera sensor like the PickFinder from VMT Bildverarbeitungssysteme detects the position and orientation of picking items in a storage container, it can send this information directly to an intelligent gripper, which picks up the parts individually and puts them in a picking container or shipping carton. Alternatively, in the context of human/machine collaboration, it could pass this information to the picker. Once this is done, the automation system simply receives an OK signal, meaning that the next process step can be started. This means the automation system itself is no longer burdened with directly controlling the autonomous detection and gripping function.

RFID – pioneering the digitisation of logistics processes

In hindsight, RFID technology in particular can be seen as the pioneer of digitised business processes in intra-logistics and the supply chain. Long before standard sensors were capable of bidirectional communication, RFID tags were able to exchange information with material flow computers and plant control systems, as well as carrying and updating process-relevant data on the object.

Write heads and control interfaces, such as IDENTControl, are available for all industry-standard frequency ranges (LF/HF/UHF), mixed operation in a range of frequencies is also possible. This allows a variety of identification tasks to be completed in an individual and intelligent manner. The RFID solutions from Pepperl+Fuchs offer additional future-proofing through their ability to be networked with higher-level information systems and thus also effectively support the digitisation of logistics processes in the implementation of Industry 4.0.

Added value with sensor data in the cloud

The programmable logic units typically used on the controller level are optimised for reliable...
control of processes with hard real-time requirements. They are not suitable for storing and processing large amounts of data recorded over long periods of time, due to their storage and computing capacity. Such tasks are the domain of IT systems with database-based structures.

With the multi-protocol enabled IO-Link master module ICE1-8IOL and an edge gateway, sensor data can be provided to higher-level IT systems, both local and in the cloud, as well as being transferred to the controller.

This is heralding a paradigm shift in the design of intra-logistics systems, since essential information is now available to generate digital twins of products and processes, allowing the mapping of logistical processes in a transparent and consistent manner. Digitised logistics is dependent on added communicative value, such as that provided by the Sensorik 4.0 portfolio.

A wide variety of applications can be implemented in IT systems using the parallel data provision. Asset management, condition monitoring, and predictive maintenance are examples of this.

Asset management based on end-to-end communication documents the components installed in an intra-logistical plant and keeps itself up to date. Differences between 'as planned,' 'as installed,' or 'as maintained' are thus eliminated.

Diagnostic data supplied by sensors can be used in analysis apps in order to detect possible faults, and avoid them through predictive maintenance. Service intervals can be optimised on per-cycle basis, for example by making use of pre-planned downtime on a material flow system or industrial truck for cleaning, maintenance, or component replacement. In this way, condition monitoring can have a direct impact on the availability of the entire intra-logistics plant.

Another obvious application in higher-level IT systems is visualisation of sensor status data and settings on HMI terminals. At a glance, a machine operator can recognise how a sensor is currently working, which switching thresholds are configured, and how a sensor is operating with respect to any critical tolerance values.

Sensorik 4.0 opens up disruptive perspectives

The potential benefits of smart sensors and communication modules are of an incremental nature – focused on step-by-step efficiency gains in existing tasks. As an example, with their communication capability and distributed intelligence, they are able to perform individual intra-logistical functions autonomously and thus generate important added value for the material flow itself as well as the accompanying data flow. At the same time, Sensorik 4.0 opens up disruptive perspectives because it makes data available centrally in the Internet of Things, as well as the Internet of Services, supporting the concepts of intelligent objects and networked logistical systems and processes.

The rise of Industry 4.0 and industrial connected working

With wireless connectivity becoming more widely used in the workplace, the potential use of Bluetooth, LTE and other systems in industrial environments is growing significantly.

With the rise of Industry 4.0 and the Internet of Things throughout many offshore locations, big companies like Shell and BP have found ways to share data wirelessly while on the move. Sharing digital data and information as well as communicating with others in real-time is one of the key advantages to this new way of working. Field Mobile Workers no longer need to go back to control centres to inform their colleagues on temperature, pressure and other field conditions. They just need their mobile device, like a tablet or smartphone, and can synchronise the required information immediately. This enables engineers to continuously monitor production and make quick decisions on how to best extract oil and spot any problems, such as blockages.

Today, Smart Field Technology is helping to improve and increase the efficiency and productivity of operations, thus reducing the costs and the expenditure of time. With the help of real-time communication technology, problems and incidents could be solved right at the spot, significantly cutting down on the amount of man-hours that are spent onsite.

In addition to these benefits, mobile technology enables solutions to provide accurate information about the workers in case of emergency and accidents. Lone Worker Protection Solutions, whether included as hardware or as an app solution, are a key factor to maintain the highest possible safety levels for mobile workers.

Whether for intra-logistics or the supply chain, the paradigm shift triggered by intelligent and communication-ready sensors is in full swing.

For more information contact Pepperl+Fuchs, +27 (0)87 985 0797, info@za.pepperl-fuchs.com, www.pepperl-fuchs.co.za

Application Examples

Voice of the Machine

Connected Factory
Compressed Air
Electro Hydraulic
Control Asset Tracking

Engineering your success.

www.parker.com/iot
As Industry 4.0 morphs from concepts and ideas into working, real world applications, factory and production equipment is utilising industrial networks to become more connected and intelligent. This is largely driven by the need for better performance, efficiency and productivity. The selection of a communication protocol, from both a hardware and software perspective, will also need to factor in considerations such as redundancy, flexibility, expansion and ease of implementation.

Importantly, adding intelligence to machines also gives the opportunity to implement a predictive maintenance strategy. The ability to foresee issues and then plan rather than react to maintenance needs minimises downtime and its associated costs and is extremely valuable to operators.

Smarter manufacturing plants with a predictive maintenance approach can only be achieved by collecting significant amounts of sensor data in real-time. Production line versatility, which is a key benefit of smart manufacturing for companies making a number of different products, needs data to support decisions and then adjust and re-balance lines.

**IO-Link emerging from the crowd**

IO-Link, also known as SDCI (single-drop digital communication) is an open communications protocol that has emerged from the crowd of longer established alternatives as being a cost effective yet powerful platform that is well aligned with Industry 4.0. It enables simple, scalable, point-to-point communications between sensors or actuators and the controller, in very simple terms it is like having an industrial USB. Parker Hannifin is one of more than 130 companies in the IO-Link community which can boast over 3.5 million nodes achieved in the field to date. This is a degree of market penetration that demonstrates not only relevance to market needs, but also reliability.

Automated factory environments typically include large controller cabinets housing PLCs along with I/O cards and many I/O terminations. These provide the interface for all machine-to-machine communications. IO-Link’s low cost IP67 master blocks allow much of this to be moved out onto the machine, significantly reducing cabinet space. This is achieved by establishing communication via an IO-Link master situated closer to the point of sensing and therefore simplifying the communications and cabling arrangement. This is at a significantly reduced cost versus using IP67 Ethernet blocks for on-machine I/O. Compared to discrete wiring, IO-Link significantly reduces the extent of wiring needed between manifolds and sensors as is the number of interconnections. This enhances overall reliability as every interconnection represents a potential point of failure or compromise in system reliability. In addition, the standard non-shielded M12 cables and connectors used in IO-Link have just three or five wires and offer many design, implementation and reliability benefits when compared to traditional 25-pin/ D-sub connectors commonly used in machine and production automation and control systems.

**IO-Link and predictive maintenance**

Current trends are towards predictive/preventative rather than reactive maintenance. Predictive maintenance is widely recognised as the ‘way to go’ in many sectors – not just industrial automation. A study by Accenture and GE found that predictive maintenance can generate a 30% reduction in maintenance costs and an up to 70% cut in production line downtime caused by equipment breakdowns. IO-Link is especially well-suited to such an approach and philosophy.

**At point of installation**

While the main cost and downtime reduction benefits can be reaped during the long working life of a production process and system, there are also important pluses to IO-Link at the installation stage. Due to its simpler point-to-point topology, IO-Link is faster and easier to install than other monitoring and control approaches, including Ethernet. It allows for rapid troubleshooting at the commissioning stage that can be performed either locally or remotely. The detection and resolution of false sensor settings and other snagging issues are also much more straightforward to detect, isolate and resolve.

Versus a centralised, proprietary arrangement, IO-Link’s decentralised model also delivers cost benefits, this is both in terms of the actual cost of the required hardware, and the labour cost to install and interconnect hardware.
During working life

The major and ongoing benefits of employing IO-Link are to be enjoyed during the regular working life of the installation. With multiple, and easily extendable sensing points IO-Link gives extensive, precision data points on the machine and then communicates that data in real time allowing processes to be closely monitored.

Sensor detected excursions (beyond adjustable pre-set parameters) trigger alarms and can be quickly addressed before costly, unplanned interruptions to production or compromised quality of the products being made by the process become a risk. In many cases, early sensor notification of issues can allow system operators to investigate, consider, plan and schedule the required corrective maintenance for a time when production throughput is either low or can be stopped. This could be overnight, or during a larger planned plant maintenance shutdown. Cost and disruption of unavoidable downtime are reduced and replacement components can be sourced and repairs carried out with utmost control and efficiency.

Flexibility and robustness

Due its decentralised, plug-and-play topology, IO-Link is inherently flexible and this is enhanced by its vendor neutrality with modules and devices from different suppliers able to be easily combined. This can allow the extension or modification of existing implementations by adding more sensors and actuators to give enhanced diagnostics, monitoring and control. This means that reconfiguration of production environments is quick, easy and low risk versus other more complicated and vendor-tied industrial Ethernet approaches.

Not all production environments are clean, dry and free from vibration and other environmental challenges. These can threaten the reliability of communications infrastructures installed to sense, monitor and control processes. This is especially true where there are a large number of interconnects with each representing a potential point of failure. The standard, non-shielded, five-pin proximity switch cables and connectors used in IO-Link, are designed specifically for industrial applications and are robust with either IP65 or IP67 ratings underlining their resilience to the challenges of most operating environments. As all IO-Link data transfer is based on a 24-volt signal, susceptibility to electrical interference is not an issue and screened cables and grounding seen in other approaches is not necessary.

Conclusion

With widespread implementation of smart factories a positive inevitability, it is important to have a dedicated communications infrastructure that maximises the easing of implementation and then the versatility to adjust to changing needs and configurations. In addition, with the benefits of predictive maintenance well understood, many manufacturing organisations are keen to adopt the strategy and begin enjoying the business and continuity benefits. IO-Link is well positioned and equipped to deliver on these needs, and backed by its inherent robustness and vendor neutrality, become the industrial communications approach of choice for many sectors.

For more information contact Lisa de Beer,
Parker Hannifin SA, +27 (0)11 961 0700,lisa.debeer@parker.com, www.parker.com/za
Connected hydraulics: ready for Industry 4.0

Prejudices last for a long time, even when reality has long since disproved them. One of these prejudices is that hydraulics have no place in Industry 4.0 because they are not intelligent – but they have actually been ready for the future for some time.

For decades, hydraulics have been equipped with electronics, sensors, appropriate accessories and autonomous controls. In terms of automation technology, they have been at the same level as electromechanical drives for some time – partly thanks to the numerous system modules from Bosch Rexroth. Black and white valves have already disappeared from many applications, replaced by autarkic servo-hydraulic axes. The question is no longer whether hydraulic valve technology will benefit from networking capability, but simply when.

We are currently experiencing the transition from classic, analog hydraulics to largely digital networked fluid technology. European machine manufacturers are increasingly digitalising their machines and expect the hydraulics to integrate seamlessly into these networked environments. The challenge now is extending networking beyond the machine itself and handling the wealth of data obtained. It has to be bundled and evaluated meaningfully and securely.

Intelligent interplay is the key
Tasks that were previously performed by steel and iron valve controls are now being carried out by decentralised intelligence in an electronic drive control unit. It adjusts the speed of the pump drive as required when power is needed at the consumer, or reduces it to almost zero. In many processes, this is a considerable energy advantage. The variable speed hydraulics consume up to 80% less energy than constant systems. Current discussions about Industry 4.0 show how important it is that all necessary functions and functionalities are defined. Active networking and communication is only possible if the mechanics, electronics, and sensors are standardised across different manufacturers.

In the future, not every hydraulic-mechanical pressure valve will have on-board digital electronics and connect to a control or other valves. This will only be the case when it makes sense.

Smart solutions with decentralised intelligence
Decentralised intelligence and open interfaces are the crucial requirements for future automation solutions. As a result, Bosch Rexroth uses multi-Ethernet interfaces that support all standard protocols in its electrics and hydraulics. The next step is to integrate sensors into the existing valve housing. This opens up a range of possibilities. Let’s consider condition monitoring for example. Here, sensors can record information about everything from oil quality to temperature, vibrations and completed switching cycles. Deep learning algorithms enable users to identify wear before it leads to a failure – a key step on the road to preventive maintenance.

Intelligent single-axis controllers are already responsible for decentralised hydraulic motion in a closed control loop. To achieve this, a powerful motion control is integrated into the valve’s on-board electronics. It carries out the target/actual comparison locally and makes adjustments to an accuracy of a few micrometers. The control quality of the system depends solely on the resolution of the measuring systems. These control cabinet-free motion controls are being used increasingly frequently in a wide range of markets.

With its IAC control valve, Rexroth also offers a control cabinet-free motion control that is completely integrated into the valve electronics. It can be fully networked using open interfaces, as can servo-hydraulic axes with a dedicated decentralised fluid circuit. In these ready to install axes, the pump, valves and cylinders make up a single assembly, which the machine manufacturer only has to connect to the power supply and control communication.

Plug-and-play for hydraulics
In the future, best-in-class controllers will replace valves that were previously necessary for motion. The electric drive positions the hydraulic cylinder based on the speed of the pump drive alone. Thus, the hydraulic gears essentially do the same as an electromechanical linear drive – they convert the rotary motion of electric drives into linear motion, but with all the advantages of hydraulics.

In the next development stage – autarkic linear axes – the advancement is particularly apparent. These are ready to install cylinder assemblies with a dedicated, highly-integrated fluid circuit. To operate these axes, machines therefore require no central hydraulic unit. The autarkic axes are connected in the same way as electric drives – all that is needed is a power cable and a data connection to the machine control. The same software tools are used for commissioning as for electric drives. Commissioning engineers require no in-depth knowledge of hydraulics, because they simply configure the preprogrammed functions for the machine conditions.

For more information contact
Willem Gijzelaar, Hytec Holdings,
+27 (0)11 979 4630,
info@hyhold.co.za,
www.hytecgroupl.co.za
The effects of the Internet of Things (IoT) is something we experience in our everyday lives through the proliferation of smart phones, cars, thermostats, and even smart refrigerators entering our homes. These smart devices provide us with a rich source of sensor data that can be networked, gathered and analysed by software to detect potential issues, allowing us to work more productively and save more energy.

A less frequently talked about phenomenon, the Industrial IoT (IIoT), is the application of these same principles to a wide range of industrial plants and processes. The IIoT has been developing in parallel to the more consumer-focused IoT, and it promises to revolutionise industrial prowess by improving efficiency at manufacturing plants, mining operations, oil refineries and off-shore oil platforms, and more.

Schneider Electric's EcoStruxure

Looking for opportunities to expand its digital offering through the application of the IoT to industrial environments, plants and factories, Schneider Electric's EcoStruxure promises to change South Africa's mining, food, beverage, and water industries.

“Gathering technical data, tracking equipment and monitoring maintenance activity would help to reduce downtime, process energy usage, maintenance costs and time-to-market,” says Marc Ramsay, vice president of Schneider Electric South Africa’s Industry Business Unit. “This smart IIoT software ultimately serves to make plants more efficient, safe and reliable.”

Information security

IIoT technology has continued to develop at a steady rate, and a number of trends are expected to guide these developments for 2018. Adoption of the IIoT has increased significantly as more and more industrial devices get connected to the Internet. As the networks have expanded, volumes of data have increased and more information is now at risk, therefore it comes as no surprise that the focus on creating applications and data storage solutions capable of providing the necessary security has intensified.

“We understand that robust cybersecurity protection is a must, and Schneider Electric’s solutions apply rigorous policies and methodologies to ensure the protection of critical infrastructure,” adds Ramsay. “We also assess risk, implement cyber-specific solutions and maintain onsite defences over time. Cybersecurity solutions are applied from the operations perspective while making sure all appropriate IT policies and requirements are implemented. I think this is what sets Schneider Electric’s EcoStruxure apart.”

While early IIoT implementations were generally focused on improving asset utilisation through better monitoring and predictive analytics, such as predictive maintenance, many industries are now taking advantage of increased connectivity in order to implement more autonomous systems.

“Schneider Electric is a leader in the digital transformation of energy management and industrial automation in South Africa, and the rest of the globe,” explains Ramsay. “Our EcoStruxure solutions offer a new level of efficiency and performance, and specific products such as Edge Control allow for remote automation, process automation and machine automation.”

Maintaining plant equipment can be a daunting and costly task, and creating efficiencies and using predictive maintenance has become a top priority in the future of the IIoT. Here, sensors and real-time monitoring could help organisations understand precisely where and when equipment needs to be adjusted or replaced.

“This connected ‘smart’ technology is capable of automatically measuring, monitoring and controlling energy consumption and demands,” concludes Ramsay. “When automation and energy is coupled with software and analytics, an unprecedented level of operational intelligence can be delivered, leading to better, and more predictive decision making in real-time.”

For more information contact Jason Ullbricht, Schneider Electric SA, +27 (0)11 254 6400, jason.ullbricht@schneider-electric.com, www.schneider-electric.co.za
The changes resulting from future-oriented Industrie 4.0 projects demand new concepts for machine operation and monitoring. This also has an impact on the hardware, as the corresponding devices not only need to be adapted to the framework conditions, but must also fulfill the increased safety requirements.

Which hardware enables users to operate their machines easily and to monitor them according to circumstances? The decisive factor here is whether the application is for the automotive industry, a wind turbine generator, a water treatment plant or an oil platform. Each of these areas of application is subjected to special ambient conditions, thus having its own particular demands on the devices installed. These need to be considered when selecting the required visualisation hardware.

Combination of mounted and mobile devices
In the four typical applications listed above, the user would like to receive application data and information at any location. The values should not only be shown within the system, but also be viewable in the plant environment. To this end, a tablet PC can be used. In practice, however, it’s all too often the case that the tablet PC is not available when it is most needed. In contrast, a permanently installed HMI device enables the user to operate and monitor the application at any time. In a larger system, it is advisable to use both the tablet PC and the HMI device.

There is a similar situation in a wind turbine generator system. A combined HMI hardware solution allows for the seamless monitoring and maintenance of the application. As is the case with the renewable energy production, extreme ambient conditions may also occur in a water treatment plant which can differ significantly from one location to the next. Temperatures, for example, may vary strongly. Humidity, seawater and aggressive gases will adversely affect devices used for operation and monitoring. Oil and gas, process industry and maritime applications are to be considered as a special case. In these fields of application, the hardware offered for visualisation purposes is restricted due to safety regulations and approvals. As a result, there are only a few manufacturers offering these devices. This is especially the case in the mobile sector.

Closed systems in addition to HTML5-based systems
It is easy to see why visualisation for the scenarios described above cannot be based on only one platform. Various cross compilers are available, but there are some restrictions with regard to platforms. Furthermore, there are often problems on platforms that need a tailored solution. In this case, the web technology and, in particular, the HTML5 language, allows for cross-platform visualisation. HTML5, however, should not be viewed as a universal solution because there are always incompatibilities between the different browsers used on the different platforms. In general, the problems – often less significant visual problems – are easily rectified.

Distinguishing features are needed to
respond to the strongly growing competition. This may, for example, be an optimally designed user interface as the plant’s calling card. The portfolio around the open HTML5-based devices is complemented by HMI hardware for closed systems. This includes the ‘PC Worx Engineer’ engineering environment developed by Phoenix Contact for its PLCnext Technology control platform. Using the HTML5-based visualisation editor integrated in PC Worx Engineer, it is possible to create a closed and safe production chain. Phoenix Contact offers both HMI hardware for PLCnext Technology and open HTML5-based systems.

**User interface reduced to the functions and actions necessary**

PC Worx Engineer has not only been designed as programming software, but can also be used for creating modern visualisations. This offers the user numerous benefits: the techniques already known from programming noticeably simplify the creation of visualisations. Additional software tools are no longer necessary. Programming and visualisation work together reliably since they are perfectly adapted to each other. Furthermore, PC Worx Engineer allows for a web-based display based on open standards, such as HTML5 and JavaScript. Thanks to the scalability and adaptability of visualisations, any device with a web browser can be used as an HMI client without any additional software. The performance of the controller is available for core tasks, thus saving resources of operation and monitoring devices. Reusability of visualisation templates, pre-configured objects, as well as self-created icons, lead to a shortened development time.

**Portfolio for every application**

With its comprehensive product portfolio, Phoenix Contact always offers the right hardware for the respective visualisation. Using a new processor generation, the devices are characterised by fast reaction and screen change times. Various touch technologies – such as analog resistive foil touch, projected capacitive glass touch (PCAP) and robust glass-film-glass-touch (GFG) – bring about advantages in all application areas.

The front plate made of brushed aluminium impresses not only with its slim design but also with robustness and durability. HMI devices designed for an operating temperature from -32 to 70°C can be operated with work gloves. The IP67 protection class enables the use without control cabinet, directly in the application. The display is resistant to UV and IR radiation and can be read easily even in direct sunlight.

HMI which are used, for example, in production plants and the fields of process industry, machine building and building automation, perform important functions in indoor and outdoor applications. Further applications can be found in wastewater treatment and water treatment plants as well as in the fields of renewable energy production and automation of traffic tunnels and snowmaking systems. The HazLoc certification related to extreme conditions of use places virtually no limitations. Shock-proof, splash-proof and dimmable devices that are certified and approved according to GL, LR, BV, DNV, ABS, and EN 60945 are available especially to cope with the demands of shipping.

All HMI devices can be configured individually with regard to application software, operating system, memory and design. Display sizes from 110 mm to 470 mm permit flexible system planning.

For more information contact
Kevin Preston, Phoenix Contact, +27 (0)11 801 8200, kevinp@phoenixcontact.co.za, www.phoenixcontact.co.za
Human-robot collaboration (HRC) describes a work scenario in which humans and automated machines share the same workspace and work within it simultaneously. Driven by Industry 4.0, this model promises the interaction of highly flexible work processes, maximum plant availability and productivity, as well as economic efficiency. But HRC will only be able to live up to this promise when appropriate application-specific safety technology is assured.

**Human-robot interaction: a question of space and time**

Industrial automation focused on interaction between humans and machines long before the initiation of Industry 4.0. Until now, two interaction scenarios – coexistence and cooperation – have dominated, representing about 90 percent of such situations. Space and time are the important interaction parameters here.

Coexistence describes a work situation in which the human and the machine are in neighbouring areas at the same time during the interaction. Cooperation, on the other hand, is an interaction during which the human and the machine share the same work area but work within it at different times.

A third form of interaction is increasingly being focused on within the framework of Industry 4.0: collaboration between the human and the robot during which they share the same workspace at the same time. In such collaborative scenarios, the standard industrial robot with safe kinematics is no longer sufficiently safe, so collaborative robots must be used. In this case the forces, speeds and travel paths of the robot must be monitored, and limited, depending on the actual degree of risk. If necessary, the robot is stopped or switched off. The distance between the human and the robot thus becomes a decisive safety-relevant parameter.

**Risk assessment is always the starting point – even with ‘coboters’**

Since no two human-robot collaborations are the same, an individual risk assessment of the HRC is necessary even if the robot used has been especially developed for this collaboration with humans. Such a ‘coboter’ will already have several of the features of an inherently safe design right from the initial considerations. At the same time, however, the collaboration space must also meet fundamental requirements, e.g. regarding minimum distances to neighbouring accessible areas that present crushing or trapping risks. The standards basis for the functional safety of HRC applications consists of general standards, such as IEC 61508, IEC 62061 and ISO 13849-1/-2. In addition, ISO 10218-1/-2 on the safety of industrial systems, or an inherently safe design of the robot, must be taken into account.

Developers and integrators of robot systems must not only carefully examine the functionalities and compliance with standards of the design-related protective measures undertaken by the robot’s producer, but also take into account any residual hazards and risks. It is therefore necessary to carry out a risk assessment on the robot system according to ISO 12100 in order to derive appropriate safety measures for risk reduction, e.g. safety light curtains or safety laser scanners.

**Functional safety for HRC: expertise, product range and implementation from a single source**

Of the four different types of collaboration quoted in ISO/TS 15066, it is ‘speed and separation monitoring’ that offers the greatest future potential in HRC applications. Therefore, whilst not neglecting the still-dominant interaction scenarios of coexistence and cooperation, it is clear that safety-oriented sensor and control technology faces new challenges in enabling unhindered human-robot collaboration.

For more information contact Mark Madeley, SICK Automation Southern Africa, mark.madeley@sickautomation.co.za, www.sickautomation.co.za
Nimbus smart relay with built-in Cloud interface

Designed specifically to allow industrial companies using process machinery to control and connect their machines to the Cloud, the Nimbus provides the opportunity to improve efficiency and reduce costs by utilising machine data more accurately to plan maintenance, consumables replenishment, parts replacement and other ‘upkeep’ tasks.

There are literally hundreds of thousands of unconnected industrial machines on shop floors, factories and manufacturing plants. The Nimbus at last gives the owners of this hardware a way to evaluate the overall ‘health’ of their machines, and so avoid costly downtime or catastrophic failure. A dashboard app keeps users in the loop by displaying live machine measurements and data on a tablet, smartphone or desktop computer.

Described as an all-in-one solution for controlling small machines, the Nimbus is conveniently compact (101 x 23 x 120 mm) and provides 3 programmable relay outputs capable of switching mains powered equipment. It features industrial grade analog and digital I/O, with 4–20 mA and NTC temperature input options.

It supports a wide range of communication protocols including Modbus and MQTT with physical connections of WiFi, RS-485, RS-232 or external 3G/4G modem. For manufacturers that need machine health and production information at their fingertips, Nimbus offers a way to control small machines and send data to the Cloud to monitor equipment health.

For more information contact Charlene Oroschin, Define Instruments South Africa, +27 (0)83 384 9186, charlene@defineinstruments.co.za, www.defineinstruments.co.za

PowerTag: Schneider Electric’s smallest wireless energy sensor

Schneider Electric has introduced PowerTag, its smallest wireless energy sensor, designed to enhance the monitoring of electrical assets. PowerTag is built to connect to a miniature circuit breaker, to add connectivity, and to provide building owners and facility managers with precise, powerful, and real-time data to increase the health of a facility’s strategic assets.

Designed for any type of building, the energy sensor easily monitors and measures currents, voltages, power, power factor and energy. This first of its kind connection enables greater availability of electrical assets by providing the ability to manage critical loads, leading to higher reliability and efficiency of the electrical installation. Data is sent wirelessly to a concentrator for display via in-built web pages, or provide data for larger energy management systems or BMS. Data can also be leveraged to create customised e-mail alarms to assist facility managers with remote monitoring of their assets.

“Customers are demanding new solutions to meet the critical challenges of building asset and energy management,” said James Calmeyer, vice president for buildings, Schneider Electric South Africa. “PowerTag provides the innovation to make asset and energy management simpler. The majority of circuit breakers can now be tagged, bringing electrical distribution connectivity to a new era. The tag can easily be fitted without the need for complex wiring or additional space requirements – in reality it’s a five-minute installation to get connected.”

The compact, space-saving auxiliary fits easily in new and existing distribution boards and is natively integrated into Schneider Electric’s Acti 9 Communication System to provide customers an all-in-one monitoring and control solution.

For more information contact Jason Ullbricht, Schneider Electric SA, +27 (0)11 254 6400, jason.ullbricht@schneider-electric.com, www.schneider-electric.co.za
**PRODUCT SHOWCASE**

**Smart valve sensor provides continuous position feedback and diagnostics**

The intelligent valve sensor for pneumatic quarter-turn actuators from ifm electronic features 360° position monitoring to allow precise and continuous scrutiny of the valve condition. Problems such as wear or dogging are reliably detected and directly communicated to the user. This data supports maintenance planning and can also avoid production losses. Thanks to the integrated IO-Link communication interface and in combination with ifm IO-Link masters, the sensor can be networked via different bus systems, allowing connection to the ERP system.

**Flexible configuration**

The smart valve sensor matches settings to the application software (LR Device) or inductive teach button. Any end position of the valve and the size of the sensing range can be set. A third switch point can be selected, for example for three-way valves or for switching off the pump to avoid pressure peaks.

**Diagnostic functions**

The IO-Link communication interface allows the identification of different wear conditions. On the one hand, the sensor features seal monitoring indicating a change of the closed position, which can point to deposits or wear of the seal, for example. On the other, the different positions can be counted and the time taken can be measured.

Visit ifm at stand C2 at Electra Mining Africa 2018 for a demonstration or more technical information on this new product.

For more information contact ifm electronic SA, 086 143 6772, info.za@ifm.com, www.ifm.com

**Omniflex IoT enabled control and data acquisition**

Omniflex specialises in remote monitoring solutions based on years of plant networking experience from last mile networking to mainstream Ethernet backbones. The Teleterm range specifically addresses the remote outstation issue by providing a programmable platform based on IEC61131 languages for control and networking options from low grade cable to radio and GSM infrastructure. Wireless distributed PLCs with inherent data acquisition capability are an attractive proposition against cable-based systems.

HMI systems can link easily with SQL databases, Use MQTT and OPC UA to integrate into larger MES system with links to big data. Visualisation can also be wireless, through the use of Wi-Fi a tablet for a portable operator interface or management tool can be used for linking into the system without having to use fixed desktop computers. Remote site visualisation is achieved the same way using a tablet and remote Teleterm devices via the Internet and local integrated routers. Other features include:

- Flexible configurable I/O analog and digital.
- Ethernet and wireless ports.
- Programmable serial port.
- Local logging on SD cards.
- Small DIN rail mounting.
- 9-30 VDC powered.
- Modbus and Modbus TCP as standard.

**Wireless capabilities**

- Licence-free band RTUs.
- Licence-free band wireless PLC units.
- Wi-Fi and HMI solutions.
- GSM IoT RTUs.
- GSM IoT PLC units.
- Repeater solutions.
- Internet-based monitoring.
- SMS, email and data transmission.

For more information contact Ian Loudon, Omniflex Remote Monitoring Specialists, +27 (0)31 207 7466, sales@omniflex.com, www.omniflex.com
In the industrial automation world, business owners who follow the IIoT trend are able to optimise operational efficiency and maximise profits. In order to achieve this, one of the main goals that must be accomplished is to ensure reliable connectivity between operational technology (OT) and information technology (IT). Moxa offers comprehensive industrial edge-to-cloud connectivity solutions that accelerate convergence of the OT and IT worlds and allows users to make their IIoT dream a reality.

### Three considerations when developing connectivity for the IIoT

Make data actionable: to make your data actionable, it is essential to have a ready-to-run IIoT gateway to bridge OT and IT for data transmissions. Moxa’s intelligent IIoT gateway solutions include the ThingsPro platform, which makes data actionable through fast development, easy deployment, secure communication, and effortless maintenance.

Make data connected: connecting data to IIoT applications requires a secure network with high availability. Moxa provides industrial network infrastructure solutions that optimise network connectivity for IIoT applications.

Make data collectable: it is essential to have an easy-to-use and efficient solution. Moxa offers a variety of connectivity and computing solutions that make data collectable through interoperability and efficient data processing in order to consolidate edge connectivity for IIoT applications.

For more information contact RJ Connect, +27 (0)11 781 0777, info@rjconnect.co.za, www.rjconnect.co.za

---

### Siemens IoT2040 industrial intelligent gateway

The Simatic IOT2040 is a first ‘open’ intelligent gateway that standardises communication between various data sources and then analyses and forwards it to the corresponding recipients. It is a solution that can be easily integrated into existing machines or control systems which use legacy fieldbuses to communicate, thus enabling vital process performance data to be unlocked, shared and used to improve and optimise production.

The device is able to support industrial engineers, machine builders and designers. It is ideally suited as a gateway between the cloud, or the company IT level, and production.

The Simatic IOT2040 is designed for 24/7 operation and is the link between production and cloud based data analysis. It combines the tasks of interfacing to the ERP system and the corresponding communication of automation components, which therefore minimises errors and increases the efficiency of production process. The role as an intelligent gateway interface can be used in both directions i.e. transferring analysed data from the cloud to the production control. This continuous data communication closes the control loop for optimal of production.

This intelligent gateway for industrial IoT solutions has an Intel Quark x1020 (+Secure Boot), 1 GB RAM, microSD Card slot, 2 Ethernet Interfaces, and 2 x RS-232/485 interfaces. The IOT2040 supports Yocto Linux and comes with a battery buffered RTC and watchdog. This device is compatible with mPCIe cards, Arduino shields and Siemens IoT development kits.

For more information contact RS Components SA, +27 (0)11 691 9300, sales.za@rs-components.com, www.rsonline.co.za
RS Components has introduced the Intel Movidius Neural Compute Stick (NCS), the newest development tool for ultra-low-power deep-learning inference. The tool enables developers to develop and prototype artificial intelligence (AI) applications to a broad range of devices at the edge in a convenient USB form factor.

Targeting developers, corporate R&D and academic researchers working in machine-learning and data-science applications, the NCS integrates the Movidius Vision Processing Unit (VPU), which offers best-in-class power efficiency and is capable of running high-performance floating-point convolutional neural networks (CNNs).

Supporting the popular deep neural network (DNN) framework, the stick is ideal for use as a development tool for neural network prototyping and acceleration. The USB-form-factor inference engine enables developers and researchers to free their projects from the Cloud and allow them to learn quickly about the performance and accuracy of their neural network applications running in the real world. Neural network projects can be quickly ported via the Movidius Neural Compute Compiler to run real-time deep-learning inference on the compact USB stick.

Enabling the acceleration of existing compute-constrained platforms, the NCS enables deep-learning R&D and prototyping on a Linux laptop or any x86-based host device. In addition, the Neural Compute Platform API allows user applications to run on an embedded host, which can initialise the target platform, load a graph file and offload inferences. Support for the NCS will also be extended in the future to include other platforms such as the Raspberry Pi.

The complete list of software tools available in the Movidius Neural Compute Software Development Kit includes the Movidius Neural Compute toolkit and the Movidius Neural Compute API. These tools are available online on the developer.movidius.com website.

For more information contact
RS Components SA, +27 (0)11 691 9300, sales.za@rs-components.com, www.rsonline.co.za
<table>
<thead>
<tr>
<th>Company</th>
<th>Telephone</th>
<th>E-mail</th>
<th>Website</th>
<th>Pages</th>
</tr>
</thead>
<tbody>
<tr>
<td>1Worx</td>
<td>+27 (0)83 327 7069</td>
<td><a href="mailto:duan@1worx.co">duan@1worx.co</a></td>
<td><a href="http://www.1worx.co">www.1worx.co</a></td>
<td>26</td>
</tr>
<tr>
<td>ABB South Africa</td>
<td>+27 (0)10 202 5532</td>
<td><a href="mailto:john.mcintosh@za.abb.com">john.mcintosh@za.abb.com</a></td>
<td><a href="http://www.abb.com">www.abb.com</a></td>
<td>17*</td>
</tr>
<tr>
<td>Absolute Perspectives</td>
<td>+27 (0)83 274 7180</td>
<td><a href="mailto:gavin@gavinhalse.com">gavin@gavinhalse.com</a></td>
<td><a href="http://www.absoluteperspectives.com">www.absoluteperspectives.com</a></td>
<td>6,7</td>
</tr>
<tr>
<td>Beckhoff Automation</td>
<td>+27 (0)11 795 2898</td>
<td><a href="mailto:michellem@beckhoff.com">michellem@beckhoff.com</a></td>
<td><a href="http://www.beckhoff.co.za">www.beckhoff.co.za</a></td>
<td>OFC*,4,5</td>
</tr>
<tr>
<td>Define Instruments South Africa</td>
<td>+27 (0)83 384 9186</td>
<td><a href="mailto:charlene@defineinstruments.co.za">charlene@defineinstruments.co.za</a></td>
<td><a href="http://www.defineinstruments.co.za">www.defineinstruments.co.za</a></td>
<td>49</td>
</tr>
<tr>
<td>Endress+Hauser</td>
<td>+27 (0)11 262 8000</td>
<td><a href="mailto:info@za.endress.com">info@za.endress.com</a></td>
<td><a href="http://www.za.endress.com">www.za.endress.com</a></td>
<td>18,19,43*</td>
</tr>
<tr>
<td>EtherCAT Technology Group</td>
<td>+49 911 540 56 226</td>
<td><a href="mailto:press@ethercat.org">press@ethercat.org</a></td>
<td><a href="http://www.ethercat.org">www.ethercat.org</a></td>
<td>33</td>
</tr>
<tr>
<td>Festo</td>
<td>+27 (0)11 971 5509</td>
<td><a href="mailto:kersia.beharie@festo.com">kersia.beharie@festo.com</a></td>
<td><a href="http://www.festo.co.za">www.festo.co.za</a></td>
<td>24,29*,35</td>
</tr>
<tr>
<td>Hytec Holdings</td>
<td>+27 (0)11 979 4630</td>
<td><a href="mailto:info@hyhold.co.za">info@hyhold.co.za</a></td>
<td><a href="http://www.hytecgroup.co.za">www.hytecgroup.co.za</a></td>
<td>44</td>
</tr>
<tr>
<td>ifm electronic SA</td>
<td>086 143 6772</td>
<td><a href="mailto:info@ifm.com">info@ifm.com</a></td>
<td><a href="http://www.ifm.com">www.ifm.com</a></td>
<td>38,39*</td>
</tr>
<tr>
<td>Industrial Data Xchange</td>
<td>+27 (0)11 548 9960</td>
<td><a href="mailto:info@idx.co.za">info@idx.co.za</a></td>
<td><a href="http://www.idx.co.za">www.idx.co.za</a></td>
<td>3*</td>
</tr>
<tr>
<td>IoTnxt</td>
<td>+27 (0)12 880 0114</td>
<td><a href="mailto:daleen.vanwyk@iotnxt.com">daleen.vanwyk@iotnxt.com</a></td>
<td><a href="http://www.iotnxt.com">www.iotnxt.com</a></td>
<td></td>
</tr>
<tr>
<td>Lapp Group</td>
<td>+27 (0)11 201 3200</td>
<td><a href="mailto:info@lappgroup.co.za">info@lappgroup.co.za</a></td>
<td><a href="http://www.lappgroup.co.za">www.lappgroup.co.za</a></td>
<td>28,29</td>
</tr>
<tr>
<td>Omniflex Remote</td>
<td>+27 (0)31 207 7466</td>
<td><a href="mailto:sales@omniflex.com">sales@omniflex.com</a></td>
<td><a href="http://www.omniflex.com">www.omniflex.com</a></td>
<td>50</td>
</tr>
<tr>
<td>Monitoring Specialists</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Omron Electronics</td>
<td>+27 (0)11 579 2600</td>
<td><a href="mailto:info.sa@eu.omron.com">info.sa@eu.omron.com</a></td>
<td><a href="http://www.industrial.omron.co.za">www.industrial.omron.co.za</a></td>
<td>22,25*,52</td>
</tr>
<tr>
<td>Parker Hannifin (SA)</td>
<td>+27 (0)11 961 0700</td>
<td><a href="mailto:lisa.debeer@parker.com">lisa.debeer@parker.com</a></td>
<td><a href="http://www.parker.com/za">www.parker.com/za</a></td>
<td>41*</td>
</tr>
<tr>
<td>Pepperl+Fuchs</td>
<td>+27 (0)87 985 0797</td>
<td><a href="mailto:info@za.pepperl-fuchs.com">info@za.pepperl-fuchs.com</a></td>
<td><a href="http://www.pepperl-fuchs.co.za">www.pepperl-fuchs.co.za</a></td>
<td>IFC*,40,41</td>
</tr>
<tr>
<td>Phoenix Contact</td>
<td>+27 (0)11 801 8200</td>
<td><a href="mailto:kevin@phoenixcontact.co.za">kevin@phoenixcontact.co.za</a></td>
<td><a href="http://www.phoenixcontact.co.za">www.phoenixcontact.co.za</a></td>
<td>33*,46,47</td>
</tr>
<tr>
<td>RJ Connect</td>
<td>+27 (0)11 781 0777</td>
<td><a href="mailto:info@rjconnect.co.za">info@rjconnect.co.za</a></td>
<td><a href="http://www.rjconnect.co.za">www.rjconnect.co.za</a></td>
<td>12,13,14,</td>
</tr>
<tr>
<td>Rockwell Automation</td>
<td>+27 (0)11 654 9700</td>
<td><a href="mailto:cbuys@ra.rockwell.com">cbuys@ra.rockwell.com</a></td>
<td><a href="http://www.rockwellautomation.com">www.rockwellautomation.com</a></td>
<td>15,16,51, OBC*</td>
</tr>
<tr>
<td>RS Components SA</td>
<td>+27 (0)11 691 9300</td>
<td><a href="mailto:sales.za@rs-components.com">sales.za@rs-components.com</a></td>
<td><a href="http://www.rsone.co.za">www.rsone.co.za</a></td>
<td>30</td>
</tr>
<tr>
<td>Schneider Electric SA</td>
<td>+27 (0)11 254 6400</td>
<td><a href="mailto:jason.uilbricht@schneider-electric.com">jason.uilbricht@schneider-electric.com</a></td>
<td><a href="http://www.schneider-electric.co.za">www.schneider-electric.co.za</a></td>
<td>36*,37*,51,52</td>
</tr>
<tr>
<td>SICK Automation Southern Africa</td>
<td>+27 (0)11 472 3733</td>
<td><a href="mailto:mark.madeley@sickautomation.co.za">mark.madeley@sickautomation.co.za</a></td>
<td><a href="http://www.sickautomation.co.za">www.sickautomation.co.za</a></td>
<td>8,9,10,</td>
</tr>
<tr>
<td>Siemens Digital Factory and</td>
<td>+27 (0)11 652 2795</td>
<td><a href="mailto:jennifer.naidoo@siemens.com">jennifer.naidoo@siemens.com</a></td>
<td><a href="http://www.siemens.co.za">www.siemens.co.za</a></td>
<td>11*,45,49</td>
</tr>
<tr>
<td>Process Industries and Drives</td>
<td></td>
<td></td>
<td></td>
<td>32,48</td>
</tr>
<tr>
<td>Throughput Technologies</td>
<td>+27 (0)11 705 2497</td>
<td><a href="mailto:bob@throughput.co.za">bob@throughput.co.za</a></td>
<td><a href="http://www.throughput.co.za">www.throughput.co.za</a></td>
<td>21*,25,27,34</td>
</tr>
<tr>
<td>Yokogawa SA</td>
<td>+27 (0)11 831 6300</td>
<td><a href="mailto:christie.cronje@za.yokogawa.com">christie.cronje@za.yokogawa.com</a></td>
<td><a href="http://www.yokogawa.co/za">www.yokogawa.co/za</a></td>
<td>31,47*</td>
</tr>
</tbody>
</table>

For more information on these and other suppliers please see www.ibg.co.za
Accelerate OT and IT Integration with Moxa’s Industrial Edge-to-Cloud Connectivity Solutions