

PROCESS

TECHNOLOGY

AUTOMATION + CONTROL + INSTRUMENTATION

August 2021 vol.35 no.3

PP100007403



ICONICS Suite™

By  MITSUBISHI ELECTRIC

YOKOGAWA 



Sushi Sensor

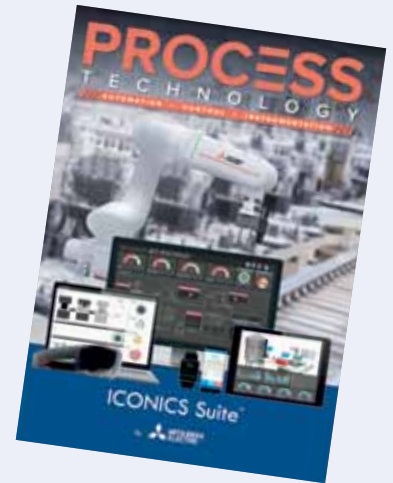
RESILIENT TRANSFORMATION

Digital transformation without compromise

IoT sensing for industrial processes
from the benchmark for quality and reliability

insight
focus
action
practice
ideas
analysis
vision





Operations, production and quality managers often struggle with a lack of real-time visibility into their equipment and disparate data sources. For discrete and process manufacturing companies, obtaining actionable insight into multiple production lines and a full view of the production life cycle helps managers visualise and improve the process for better results and smoother operations.

ICONICS Suite delivers real-time insight for operational excellence and features advanced visualisation technology to run on any desktop or mobile device, along with the ability to connect to a wide variety of industry standard communication protocols. ICONICS Suite helps users transform manufacturing from a complex process with siloed systems to a smooth operation with a clear, contextual view of production from start to finish. The platform tracks and traces products from raw materials, lines and equipment to a specific output batch, helping to find and drive impactful optimisation.

ICONICS, a group company of Mitsubishi Electric Corporation, serves as the software centre of excellence for Mitsubishi Electric's Factory Automation Systems Group. Its visualisation, analytics, mobile, IoT and cloud solutions improve productivity, reduce integration time and operating costs, and optimise asset utilisation. ICONICS solutions, combined with the knowledge and industry expertise of Mitsubishi Electric, maximise value to the customer by monitoring and controlling automation processes. ICONICS's award-winning software has achieved over 375,000 installations for factory automation, process automation and building automation customers in over 100 countries worldwide.

Learn more and schedule a demo at iconics.com.



Mitsubishi Electric Australia
www.mitsubishielectric.com.au

CONTENTS

- 4 The roles of DCS and SCADA in digital transformation
- 18 Machine safety myths
- 30 Can a solution provider handle industrial cybersecurity? Eight questions to ask
- 37 National operations in a COVID-19 environment
- 42 The craft of digital brewing



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

THE ROLES OF DCS AND SCADA IN DIGITAL TRANSFORMATION

Kevin Finnan and Wataru Nakagawa, Yokogawa Electric Corporation



Both DCS and SCADA systems are undergoing transformations in line with broader digital transformation trends, such as the IIoT.

For decades, industrial control systems have played an important role in industrial automation by allowing process manufacturers to collect, process and act on data from the production floor. Currently, these systems are in transition. Ongoing technological and industry developments have paved the way for DCS and SCADA systems to support digital transformation.

Background

Process manufacturers typically employ DCS and SCADA technologies to monitor and control the operations in their facilities. The DCS was designed to replace individual analog and pneumatic loop controllers, which were cumbersome when applied to very large processes such as refineries. SCADA originated as a solution for operations that span broad geographical areas, for example, pipelines and utilities. Later, a variant that uses an HMI in conjunction with PLCs evolved for plant automation applications.

However, DCS and SCADA systems are now doing much more than simply monitoring and controlling. They are integrating with additional intelligence at every level of the industrial automation architecture to facilitate predictive asset lifecycle management and value chain optimisation while advancing the stakeholder experience and improving security and safety. Although this particular industrial control system transition is already underway, the larger transformation of industrial automation systems has only recently begun.

Distributed control systems

At its core, a DCS is a platform for the automated control and operation of an industrial process or plant. A DCS uses local area networks (LANs) to interconnect sensors, actuators, controllers and operator terminals for process control. While it originally served the need to control large continuous processes such as refining and petrochemicals, it was subsequently extended to batch processes.

SCADA systems

Although SCADA systems originated by serving applications that require broad geographical area coverage, the concept evolved with the inception of PC-based HMIs, which replaced more expensive minicomputers in the 1980s. Instead of a wide area network that interfaces with remote terminal units (RTUs) at locations such as pump stations, a typical in-plant SCADA system uses Ethernet for communication between the HMI and PLCs. In the in-plant category, the SCADA system architecture shares many similarities with DCS architecture. In the remote scenario, a SCADA system can connect corporate operations with multiple plants, each of which uses a DCS. Process manufacturers can use these enterprise-wide systems for data communications without facing geographical restrictions.

Essentially, DCSs and SCADA systems both play important roles in plant automation. Despite this similarity, however, key differences separate these two types of systems.

The differences between DCS and SCADA

The differences extend far beyond the fact that a traditional SCADA system can work with a wide area network whose bandwidth is much lower than in a DCS LAN.

A key distinction is that a DCS uses distributed workstations for operator HMI. Each workstation can communicate directly with controllers on the DCS LAN. In a SCADA system, all communications between HMI workstations and PLCs will funnel through a server. Thus, the server is a single point of failure, the failure of which could render the entire process essentially invisible to all users.

While the architecture of a DCS and a SCADA system might otherwise appear identical, the DCS includes numerous, often subtle features such as redundant electronic circuits, which increase the system availability and minimise downtime. Redundancy extends to remote I/O: all remote I/O electronics and the communication networks between them



ONGOING TECHNOLOGICAL AND INDUSTRY DEVELOPMENTS HAVE PAVED THE WAY FOR DCS AND SCADA SYSTEMS TO SUPPORT DIGITAL TRANSFORMATION.

and the DCS controllers are, or at least could optionally be, redundant.

While SCADA HMI and servers are typically commercial off-the-shelf (COTS) PCs, a DCS uses non-COTS components that are optimised to the task. In addition, in a DCS, the Windows operating system is kept isolated from the process, which enhances cybersecurity. A deterministic DCS LAN guarantees that a critical message such as a high-priority alarm, will indeed arrive at its destination. The SCADA system typically relies instead on the high bandwidth of the LAN.

Since a single DCS vendor typically supplies the entire system, components such as controllers and workstations are more tightly integrated than they are in a SCADA system. Common benefits include simplicity or reduced engineering costs. Still, for a given process, a DCS will be more expensive than a SCADA system, but in processes for which unplanned shutdowns are very costly, the price difference is justified. While SCADA suppliers could deploy redundant servers or high-availability computing platforms to make those systems more reliable, their availability will not be as high as a DCS.

PLC versus DCS

One advantage of a PLC over a DCS is the processing speed. A PLC typically offers significantly shorter cycle times to scan I/O points and execute control and logic operations. Although DCS and PLC technologies have largely converged, their origins are completely different. While the DCS evolved from analog and pneumatic PID loop controllers, the PLC was originally a replacement for hard-wired relay logic panels. In discrete logic processing, speed is of the essence, and a PLC will perform such logic processing much faster than a DCS would.

The DCS was designed for continuous PID loop control in process industry applications, in which the PLC provides much less of an advantage in cycle processing time. An application with a combination of continuous control and discrete logic control will typically use a DCS for the former and a PLC for the latter. Often, the DCS will integrate with a PLC, which has been supplied on a skid-mounted process unit such as a turbine-driven centrifugal compressor. Some DCS vendors

have developed very efficient interfaces for such situations.

DCS, SCADA and the automation pyramid

DCS and SCADA systems both comply with the ISA95 Purdue reference model architecture. The first level — the field level — of the automation pyramid includes devices, actuators and sensors on the production floor. The second level — the control level — uses PLCs and proportional integral derivative (PID) controllers that interface to field-level devices. SCADA systems traditionally act as data funnels, transporting a broad variety of information for process control, asset management, historical analysis and IT applications. A DCS will often use multiple servers — which could be part of, or considered to be, a SCADA system — to communicate with corporate and IT systems.

A modern DCS or SCADA system will interact with several software and hardware components. Each resides in the first and second levels of a manufacturing control operation and pulls together all five levels of the automation pyramid. Because of this, it acts as the glue for digitalisation, quickly facilitating a flow of information through processes from the plant floor to the boardroom.

The evolving role of DCS and SCADA with digital transformation

Both DCS and SCADA systems are undergoing transformations in line with broader digital transformation trends, such as the Industrial Internet of Things (IIoT). This transformation comes with the promise of improved industrial automation capabilities and value for process manufacturers.

New challenges that end users have brought to light have prompted vendors to consider

how it would be possible to reimagine operational technology (OT) automation systems using COTS and information technology (IT) components. End users require that vendors incorporate best-in-class COTS hardware and software to create automation systems that surpass the reliability, security and end-user value of today's DCSs.

They also desire a system that enables them to preserve their control strategies by porting them into upgraded or new systems. In addition, end users have requested modularised hardware elements — computing, networking, storage and I/O terminations, for example — to allow for incremental upgrades. Finally, they would like software that has been decoupled from the hardware and I/O to allow execution anywhere in the system.

How is digital transformation changing DCS and SCADA?

Forward-looking process manufacturers are investing in digital transformation, and DCS and SCADA are ultimately part of such efforts. As a result, they are evolving alongside all other process manufacturing technologies. Changes to DCS and SCADA systems fit within the ongoing transformation of the automation pyramid, which is also evolving. IT/OT convergence and virtualisation technologies, for example, are blurring the distinctions between the pyramid's levels and enabling the migration of some engineering and software applications to the cloud.

With the integration of cloud technologies, process control systems can perform edge computing and serve as robust data sources for the IIoT. Cloud-based environments facilitate the convergence of data across multiple sources and improve data availability to support insightful decision-making and application interoperability.

What are the requirements for SCADA and DCS in digital transformation?

To take advantage of cloud technologies, the IIoT and edge computing, process manufacturers need to modernise their ageing automation systems. On the whole, the drive towards digital transformation has created a need for a more open and secure system architecture and design.

Figure 1: The automation pyramid.

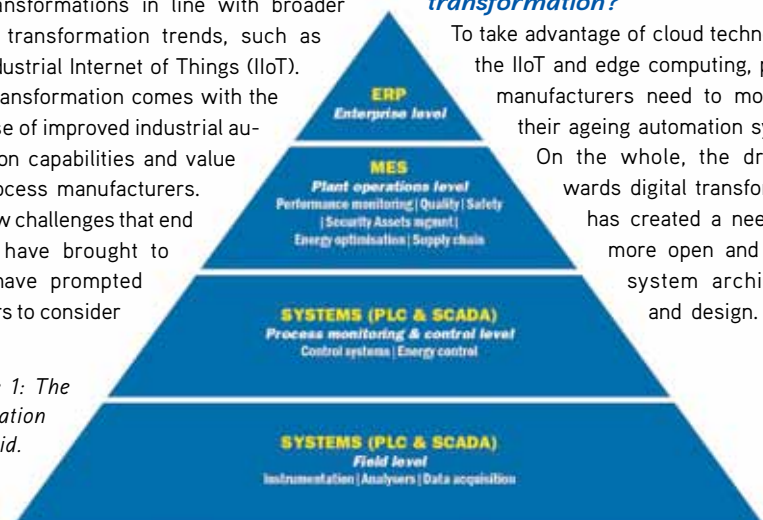
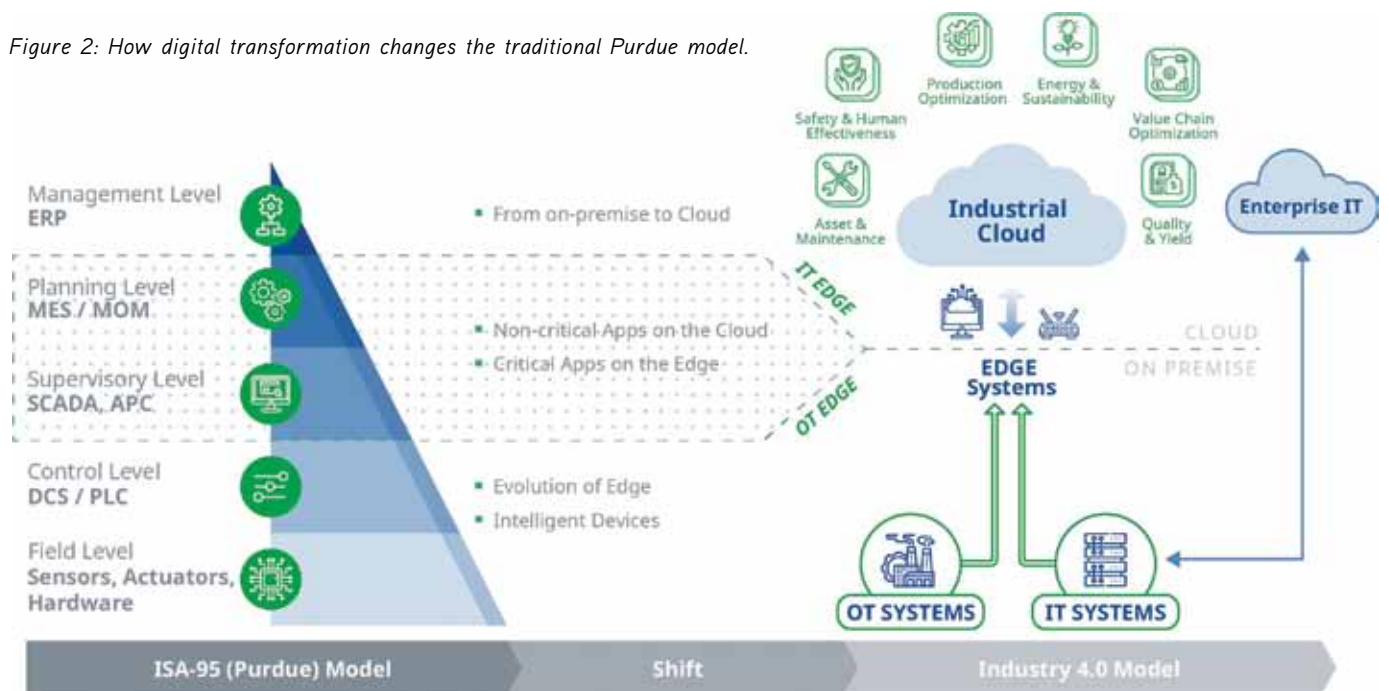


Figure 2: How digital transformation changes the traditional Purdue model.



Increasingly open systems

The NAMUR Open Architecture (NOA) and Open Process Automation Forum (OPAF) are driving major open architecture initiatives in industrial automation and prompting a shift away from proprietary architectures. Both initiatives describe vendor-neutral systems that allow the use of state-of-the-art equipment and functions at all times and the continued use of proprietary software applications in the future.

A key OPAF objective is to transition away from vendor lock-in, which has historically been an issue with large DCSs. The requirements for the architecture currently being considered by OPAF are interoperability, modularity, standards conformity, compliance with security standards, scalability and portability.

In the case of NOA, an independent domain called M+O (monitoring and optimisation) is prepared separately from the existing system, and data is directly collected from robots, drones and new sensors, for example, for corrosion, sound and vibration. Furthermore, data in the existing system is imported by OPC UA, and advanced control, analysis and diagnosis can be realised even in the field. From the viewpoint of security measures, compatibility with zone design recommended by IEC62443 is enhanced, and system design and maintenance can be easily performed.

More problematic is a lack of continuous upgrades from some DCS vendors. If their vendor ceases to provide upgrades, manufacturers are compelled to resort to a rip-and-replace approach, in which the old system is completely replaced by an entirely new one. In this scenario, the production

loss and costs incurred while transitioning to the new system often far outweigh the system cost. By creating an open, interoperable specification, OPAF aims to foster the development of less expensive and improved process control systems.

Increased security

Digital transformation has created a need for secure network architecture and design in addition to increased openness. Security is especially important as IT/OT convergence and new technologies, such as cloud computing, introduce new security risks.

Since exposing data to the internet presents security risks, it is vital that process manufacturers keep their SCADA systems up to date using contemporary cybersecurity resources. The International Society of Automation's (ISA) 62443 series of standards — which the International Electrotechnical Commission (IEC) has adopted — and the National Institute of Standards (NIST) 800-16 offer helpful resources and guidelines for network administrators and cybersecurity engineers.

Since their data exchanges typically rely on radio or public communication infrastructure, SCADA systems are more vulnerable to cyber attacks. As they oversee wide area networks, there are more points of entry. Meanwhile, a DCS is also not completely secure from cyber attacks and requires comprehensive measures, particularly on entry points into LANs.

A new standards-based approach to cybersecurity has been designed to encompass IT and OT systems. While OT typically uses the NIST cybersecurity framework, IT requirements and interactions with third parties could

involve additional standards, such as ISA/IEC 62443 and ISO 27001.

While integrating IIoT technology, IT/OT convergence implementation teams will continue making decisions regarding the segregation of OT networks from corporate networks, OT network isolation from the internet, least privilege access controls at site and process levels, and cross-site communication restrictions. Meanwhile, cybersecurity domain expertise is evolving to encompass the formerly disparate OT and IT domains.

What does the future look like for DCS and SCADA?

Requirements for open architectures and enhanced cybersecurity, driven by digital transformation, are likely to continue shaping future DCS and SCADA developments. As a result, these systems are currently in transition, but the digital transformation journey for industrial automation systems has only just begun. This journey comes with challenges for process manufacturers — for example, upgrading a legacy system can seem incredibly daunting at the outset. But the potential benefits of digital transformation make addressing such challenges more than worthwhile.

Digital transformation promises to bring a new era in industrial automation. In this era, machines will execute complex control functions with self-learning capabilities and minimal operator intervention. That will allow process manufacturers to reduce accidents and production downtime resulting from human error and achieve optimal plant operation.

Yokogawa Australia Pty Ltd
www.yokogawa.com/au

HOT PRODUCTS

ON WWW.PROCESSONLINE.COM.AU THIS MONTH



MODULAR AUTOMATION SYSTEM

MOVI-C is a modular automation system composed of the four necessary elements: drive technology, inverters, control technology and engineering software.

SEW-Eurodrive Pty Ltd

<https://bit.ly/2VjXqf1>



EXPLOSION PROOF ENCLOSURES

With over 30 enclosure sizes that can be used both horizontally and vertically, the SR series offers various dimensions for a wide range of applications.

Pepperl+Fuchs (Aust) Pty Ltd

<https://bit.ly/2VvkfvK>



COMPACT EMBEDDED COMPUTER

The Neusys POC-400 is a compact fanless embedded computer for industrial applications.

Backplane Systems Technology Pty Ltd

<https://bit.ly/3fpGaf9>

LINEAR BEARING

The drylin W polymer bearing weighs up to 84% less than classic linear bearings with their metallic housings.

Treotham Automation Pty Ltd

<https://bit.ly/3jg4VM3>



CONTROL DEVICES

DELIVERING YOU
EXCELLENCE IN **ENGINEERING**

INTRODUCING New Product



'Quality solutions for motion control'

Presenting TER to our extensive Control Devices product range. TER products are designed for reliability, ergonomics and are intuitively safe to use. Accommodates switching and control for a wide range of industrial applications, including hoisting, winch controls, conveyor systems and more.

PENDANT CONTROL STATIONS



JOYSTICK CONTROL STATIONS



RADIO REMOTE CONTROLS



JOYSTICKS - SLIP RING COLLECTORS - LIMIT SWITCHES - ENCODERS



ATEX SERIES EXPLOSION PROOF RANGE



LIMITEX AG
Rotary Limit Switch



LIMITEX AP
Position Limit Switch



MIKE-X
Pendant Control Station



SPA
Pendant Control Station

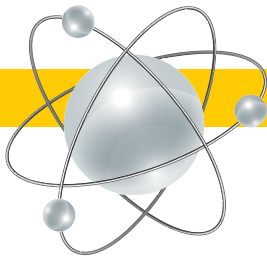


CONTACT US FOR A QUOTE

Unit 17, 69 O'Riordan Street, ALEXANDRIA NSW 2015
02 9330 1700 sales@controldevices.net



www.controldevices.com.au



Web-based design tool for better cobot safety



Users can combine different robots, hazard situations and tools with the design tool, thus compiling and continuously expanding a catalogue.

© Fraunhofer IFF

The safety of people interacting with robots has top priority, especially when humans and robots are working side by side instead of being separated from each other by safety fencing. The Fraunhofer Institute for Factory Operation and Automation has created a free web-based design tool that helps companies design their cobot implementations. The Cobot Designer helps minimise the risk of accidents and increases employee safety.

Humans and robots are sharing workspace in more and more sectors, whether they be manufacturing, logistics or medicine. Safety plays a major role in this. Up to now, range-finders on robots have prevented severe impacts or crushing when collisions occur but these sensors do not function when humans and machines have to stand close to each other, for example in subassembly — this requires other solutions. The Fraunhofer IFF web-based application, Cobot Designer, ascertains the robot speeds that ensure safe collaboration. The design tool helps programmers design cobot workstations safely. The project was contracted by the German Social Accident Insurance Institution for the Woodworking and Metalworking Industries (BGHM).

Anyone acquiring cobots for their business must perform a legally required risk assessment: companies must identify specific potential hazards and foreseeable misuse by employees beforehand. The maximum speed a robot is permitted to reach is measured when it is certified for safety — a special device measures impact forces and pressures that act on anyone who comes into contact with the robot. The limits set in the ISO/TS 15066 standard may not be exceeded, otherwise, the robot's speed would have to be reduced to prevent injuries to employees caused by clamping or impact.

However such measurement is costly and requires expertise, and the robot must then be programmed accordingly.

"Small businesses in particular can't afford this," said Dr Roland Behrens, research scientist at the Fraunhofer IFF. "What's more, measurements are taken too late since the robot has already been purchased. This is where

our Cobot Designer for digital hazard prevention comes into play."

Companies can use the interactive tool before a making a purchase to assess whether the robot's speed suffices to perform a particular job productively and, above all, safely.

"The amount of force is contingent on the robot's speed," said Behrens. If limits are exceeded, productivity subsequently suffers. "Let us assume the robot has to pre-sort a pallet in one minute. If the speed has to be reduced by 50% for safety reasons, the cycle time increases to two minutes, reducing the robot's economic efficiency 50%. That's why being able to perform an economic feasibility analysis before purchasing a robot would be desirable."

The Cobot Designer is intended to prevent bad purchases and more potentially necessary measurements. Using the design tool will enable businesses to reduce their engineering work significantly when they implement future HRC applications.

"The goal is to use computer simulation, as the Cobot Designer does, to dispense with measurements entirely in the future," said Behrens.

The tool is available for free online to anyone designing an HRC workstation, and runs on all browsers. The user merely has to enter the parameters for the robot, the hazard and the tool used, eg, a gripper. The Cobot Designer automatically computes the effect of contact between a human and the robot as well as the robot's maximum permissible speed. The tool also provides the option of loading proprietary, custom robot models.

Various biomechanical robot and hazard models constitute the technological basis. The user can combine different robots, hazard situations and tools, thus compiling and continuously expanding a catalogue. All the data entered can be downloaded and reused at a later time, and inputs are not stored on the Cobot Designer's server to protect data.

The biomechanical model precisely simulates the extent to which clamping and impact stress a person. It comprises all 29 relevant body parts where a person can feel pain, including the head, for instance. This model draws from the results of the one and only human subject study in the world to ascertain biomechanical limits, which was conducted by the Fraunhofer IFF and contracted by the German Social Accident Insurance DGUV and the BGHM. The Fraunhofer IFF validated the results of the Cobot Designer's simulation experimentally in stress tests with human subjects together with physicians from Otto von Guericke University Hospital's Traumatology Clinic and with the involvement of the appropriate ethics commission. The tests ran from 2015 to 2019.

Fraunhofer Institute for Factory Operation and Automation IFF
www.iff.fraunhofer.de

LEADER IN CABLE AND CONNECTIVITY SOLUTIONS

LAPP's comprehensive range of German-engineered cables, connectors, and accessories for process automation, manufacturing and advanced machinery delivers uncompromising product quality, and robust solutions that can withstand even the toughest conditions, backed by local customer and technical expertise.

ETHERLINE® PN CAT .5E Y

Resilient ethernet cables, 100MHZ, compliance with international standards (PROFINET®, UL) available in fixed to highly flexible, indoor & outdoor use

LAPP KABEL STUTTGART ETHERLINE® PN Cat.5e Y 2x2xAWG22/1



ETHERLINE® CAT.7 FLEX

Increased bandwidth - 600MHZ high speed, compliance with international standards (PROFINET®, UL) available in fixed to highly flexible, indoor & outdoor use


STUTTGART ETHERLINE® Cat.7 FLEX 4x2x26/7AWG



UNITRONIC® LIYCY (TP)

Multifunctional data transmission cables, for fixed, flexible & continuous flexing, available in combinations of overall screened, individually screened & twisted pairs

LAPP KABEL STUTTGART UNITRONIC® LIYCY (TP)



UNITRONIC® ST - SERIAL

RS232, RS422 & RS485 flexible cables with 100% foil screen coverage, available in single or multiple pairs, or three core

LAPP KABEL STUTTGART UNITRONIC® ST 1x2x24AWG



UNITRONIC® BUS

PROFIBUS®, CANBUS, DeviceNet™, Foundation Fieldbus and ISOBUS cables for indoor & outdoor, fixed to highly flexible applications

LAPP KABEL STUTTGART UNITRONIC® BUS PB FC



ETHERLINE® ACCESS SERIES

Fast network switches for ethernet based solutions in smart factories



ETHERLINE® DATA RJ45 SERIES

Robust ethernet connectors with a wide variety of applications



TOSIBOX®

Remote access solutions with locks and keys for your IOT infrastructure



 lappaustralia.com.au

 sales@lappaustralia.com.au

 1800 931 559

 **LAPP**

Make the right connection with LAPP Australia

BLUETOOTH LOW ENERGY LOCALISATION BEACON

The ecom Loc-Ex 01 is a Bluetooth Low Energy localisation beacon that is compatible with currently popular smartphones and tablets and can be used in Zone 1/21 (ATEX/IECEX) and Division 1 (NEC/CEC) areas. Due to the UV-resistant housing material it can be used both indoors and outdoors.

The beacons can be mounted directly on a suitable surface or easily adapted on the optional available mounting plate (which facilitates the battery exchange of the beacons). The

Bluetooth 4.0 standard makes the beacons compatible with currently popular mobile devices and they can be recognised by such devices over a distance of up to 200 m. The beacon signals can be evaluated by the mobile device via individual applications and, in this way, interact with the user or other programs.



Pepperl+Fuchs (Aust) Pty Ltd
www.pepperl-fuchs.com



PROCESS METERS

Precision Digital's process meters can be used to optimise operations in various water and wastewater applications.

The Helios PD2-6000 and ProVu PD6000 are used for pump level monitoring,

pump alternation and lead-lag pump alternation control applications. Both the Helios and ProVu process meters have built-in 24 VDC power supply to drive instrument transmitters. This feature not only saves the cost of an external power supply, but also simplifies wiring. In addition, there is a second 40 mA power supply provided with the 4–20 mA output option.

The Helios PD2-6000-6H7 powers the level transmitter and performs pump alternation, and the red light/horn provides high-/low-level alarm indication. The Helios large display process meter is beneficial for monitoring from a distance due to its large and bright 46 mm 6-digit dual-line LED display that is readable from up to 30 m away even in bright sunlight.

The ProVu PD6000-6R4 pump controller provides a solution for lead-lag pump alternation control with high and low alarm monitoring. Due to a NEMA 4X rated front panel, ProVu can be installed in panels exposed to moisture, dust and other adverse conditions. ProVu's 6-digit dual-line display can display numbers on the upper line and show either a tag or input in a different scale on the lower line. Other key features include four relays and a 4–20 mA output, advanced signal input conditioning such as automatic round horizontal tank linearisation and Modbus RTU serial communications.

Slentech Pty Ltd
www.slentech.com.au

EDGE COMPUTER

The ARK-1220F is a DIN-rail capable, fanless edge computer featuring isolated I/O for diverse industrial automation applications. It is powered by an Intel Atom E3940 QC processor and features front accessible I/O ports on a single bezel. This compact hardware and software integrated solution meets machine automation, in-cabinet equipment integration and outdoor equipment application challenges.

Utilising the Advantech DeviceOn/iEdge industrial app, the ARK-1220F is designed to optimise equipment management and productivity. DeviceOn/iEdge supports varied equipment data integrations using standard industrial protocols, including Modbus, OPC-UA and ODBC. This app also enables real-time equipment reactivity and preventative maintenance via equipment status management, a reaction rule engine, a pre-installed dashboard UI for data visualisation and abnormality notification functions. The ARK-1220F leverages Trusted Platform Module (TPM) 2.0, BitLocker under Windows 10 IoT and is secured using WISE-DeviceOn integrated McAfee and Acronis.

Featuring a vibration and shock-resistant mechanical design, the ARK-1220F accepts power input of 12–28 VDC and supports operation in broad temperature ranges (-30 to 60°C) with 0.7 m/s air flow. It has isolated COM and LAN with up to 2.5 kV isolation protection, is IEC 61000 certified and complies with heavy EN 61000-6-2 industrial standards. In addition, it provides advanced electromagnetic interference resistance via EN 55022 certification and meets industrial environment emission standards via EN 61000-6-4 certification. The ARK-1220F is suitable for applications in cramped, harsh industrial environments that necessitate stable data acquisition and high-voltage isolation.

Advantech Australia Pty Ltd
www.advantech.net.au





Mouser has something other sources don't -

Everything your BOM requires

au.mouser.com/selection

Mouser is an authorized distributor
of semiconductors and electronic components



australia@mouser.com

BARCODE AND SYMBOL SCANNER



The Cognex DataMan 374 presentation scanner is a high-speed machine vision barcode and symbol reader intended to be used in industrial applications where a fixed device can be mounted to accurately read product passing under it that is branded or tagged with identifiable text and or graphics.

It is used worldwide within airports to route luggage or freight, and within warehousing to ensure that product is true and correct. It is popular within the freighting industry as a source of information for track-and-trace applications.

Built as a robust industrial device, the DataMan 374 utilises the latest in communication technology to report and alert.

The DataMan 374 features non-obtrusive constant illumination and the ability to efficiently read at various distances and angles. It is compatible with all Cognex communication platforms, and is simple to set up due to its wide depth of field parameters and its ability to enhance low-contrast images due to its High Dynamic Range (HDR) imaging technology. It enhances image quality and contrast, resulting in greater depth-of-field and improved handling of low contrast codes.

The DataMan Setup Tool software simplifies installation and operation of Cognex barcode readers, capturing images in real time for user review and tracks read result history. Intelligent auto-tuning and application assistants guide the user to quickly optimise complex parameters. The Setup Tool also provides process control metrics and performance feedback.

Applications include pick-and-place, zone routing, scan tunnels, traceability scenarios, multi sided applications and multi-symbol applications.

Automation Systems and Controls Pty Ltd
www.asconline.com.au

DO YOU KNOW THE WEAR CONDITION OF YOUR BEARINGS AND GEARS?



STEEL PARTICLE ANALYSER SDM-72/SDM-73

SDM-72/SDM-73 units can diagnose the bearing and gear condition, even long before wear-induced vibration becomes detectable, by measuring the amount of abrasive steel particles in the grease/oil around the bearings or gears.

- Designed for ultra low to high speed rotating machinery including variable speed rotating machinery
- Battery operated
- Easy to use
- Auto-zero function
- Able to diagnose with small amount of grease/oil sample

For more information contact SafeGas
info@safegas.net.au | www.safegas.net.au



**NEW
PRODUCTS**



EDGE ETHERNET DAQ DEVICES

Adlink Technology has added the MCM-216 and MCM-218 models to its MCM-210 standalone Ethernet DAQ series. MCM-216/218 Ethernet DAQ, based on ARM Cortex-A9 processors with built-in 16 or eight channels, provide voltage or current input and can function as a standalone edge device without a host PC. The standalone Ethernet DAQ supports edge computing and includes a built-in web console and RESTful API for periodic machine condition polling.

The models are said to represent a simple, scalable, sustainable edge device to overcome the challenge of mass deployment in IIoT applications. Dual daisy-chainable Ethernet ports eliminate additional networking equipment and extend the usable distance, reducing TCO and boosting overall ROI. Successful applications include semiconductor factory digitisation, petrochemical plant monitoring and wafer feeder vacuum pump monitoring.

ADLINK Technology Inc
www.adlinktech.com



SIGNAL SPLITTER

The Acromag SP233 is a signal splitter that converts 1 mV or thermocouple sensor input into two proportional isolated 4–20 mA control signals. Power is received from one or both output loop currents.

Set-up is fast and easy with a USB connection to a PC using Acromag Windows software.

Acromag's Agility mobile app enables configuration on an Android smartphone or tablet. The software simplifies I/O range scaling, calibration and advanced signal processing capabilities.

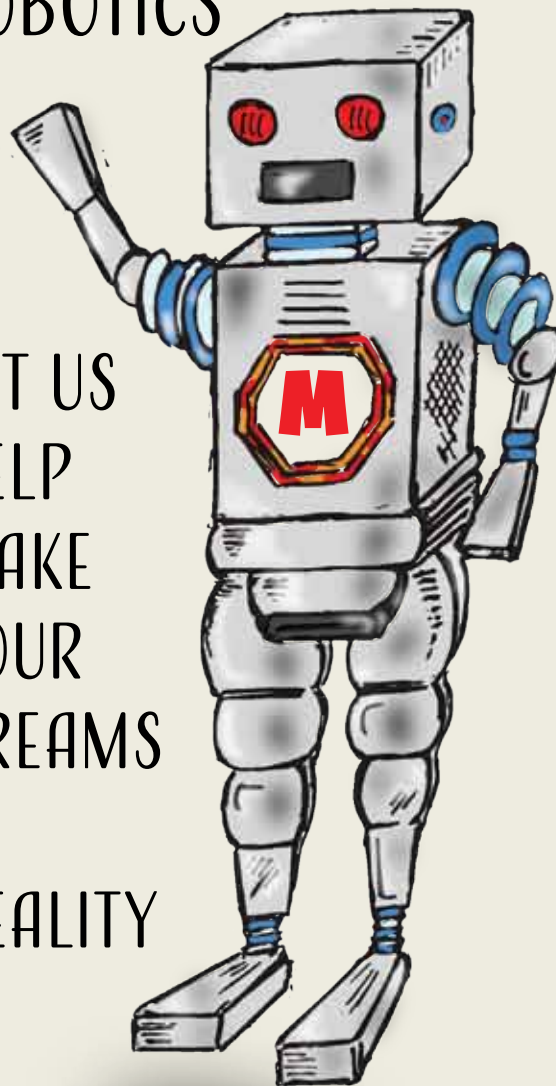
High-voltage isolation separates the input and between the output circuits. The isolation protects from surges, reduces noise and eliminates ground loop errors.

These rugged instruments withstand harsh industrial environments to operate across a wide temperature range with very low drift. They feature high immunity to RFI, EMI, ESD and EFT, plus low radiated emissions.

Metromotion Pty Ltd
www.metromotion.com.au



INDUSTRIAL COLLABORATIVE ROBOTICS



LET US
HELP
MAKE
YOUR
DREAMS
A
REALITY



**Automation
Systems &
Controls**

PH: 0407 553 103

**NEW
PRODUCTS**



MODULAR INDUSTRIAL PATCH PANELS

Hirschmann's Modular Industrial Patch Panel (MIPP) is designed to be a robust and versatile termination panel for both fibre and copper cables that need to be connected from the operating environment to active equipment. Easily installed on a standard 35 mm DIN rail, the panel features high port density to meet expanding network connectivity needs within limited space.

The panels are constructed of lightweight, high-strength aluminium, securely protecting copper and optical fibre connections under harsh industrial conditions. The housing can withstand temperatures from -20 to +70°C and is resistant to shocks and vibrations. The patch panel's industrial quality offers a secure termination point for industrial Ethernet connectivity.

As network designs may change over time, the product allows for modifications by simply swapping modules to meet the new design required. Installing a panel with blank modules readies the solution for any extensions or modifications to come. The importance of cabinet space in industrial sites has been considered with its narrow housing design. With three cable entry points (top and bottom), there is no need for special cabinet design or positioning.

Control Logic Pty Ltd
www.controllogic.com.au

RUGGED TABLET

Getac has announced its next-generation F110 rugged tablet for mobile professionals in the manufacturing, automotive, defence, public safety, utilities, and transportation and logistics sectors.

It includes a quad-core 11th Generation Intel Core i5/i7 processor and integrated Intel Iris Xe graphics as well as a broad range of connectivity options, including WLAN Wi-Fi 6, Bluetooth 5. WWAN 4G LTE/GPS and an integrated Thunderbolt 4 port. It also features an improved 11.6" LumiBond 2.0 touchscreen with up to 1000 nits of brightness.

The F110 has MIL-STD-810H and MIL-STD-461G certifications for reliability and is IP66 rated so that it offers full protection against dust ingress and water from powerful jets. Drop resistance is now up to 1.8 m when in use and the operating temperature range is now -29 to +63°C.

A redesigned dual hot-swappable battery system allows for quick battery changeover without powering down, and relocated expansion and SIM card slots (from rear to side) offer easier accessibility. There is also now a camera shutter for better privacy, and a user-removable SSD.

A full range of compatible accessories is also available, including a detachable backlit keyboard, featuring 88 full-size keys and integrated touchpad for laptop-like operation when performing data-intensive tasks. Additional accessories include a shoulder strap, rotating hand strap and kickstand, hard handle and secure office/vehicle docks.

Getac Technology Corp
www.getac.com/apac



COMPRESSED AIR POWER

CROLL OX.T AIR COMPRESSOR TANK MOUNTED ORBITAL TECHNOLOGY

Revolutionary Scroll compressor in a new, fully integrated, tank mounted system

The advanced alternative to noisy, piston type air compressors. Simply plug in for high efficiency, low maintenance, low noise power.

KAISHAN
Engineering the Future

KAISHAN AUSTRALIA

WORLD CLASS ■ EFFICIENCY ■ RELIABILITY ■ PERFORMANCE



DIGITAL POWER AMPLIFIER

The HYDAC EHCD-AM005XXXU universal digital power amplifier has been designed for actuating hydraulic proportional valves: a directional control valve with two solenoids, or one/two independent pressure or needle valves with one solenoid each.

This unit can be adapted to a wide range of proportional valves by employing user-defined parameter configuration in the power output stage. Making the configuration settings via the USB interface is easy (table-oriented) and is done using HYDAC's parameterisation software, which features an integrated oscilloscope.

Typical applications include control of directional, pressure and needle valves, which need a flexible adaptation of the solenoid control.

HYDAC International

www.hydac.com.au

SMARTPHONE FOR HAZARDOUS AREAS

The ecom Ex-Handy 10 from Pepperl+Fuchs is the company's next generation of feature phone for a broad range of applications. The Ex-Handy 10 is suitable for global 4G communication, supports 21 LTE bands, and offers both keypad and touch screen operation. The display is made of durable, scratch-resistant Gorilla Glass (IP68-rated) and can even be operated with gloves.

The Ex-Handy 10 is designed for harsh environments — it is operable in temperatures from -20 to +60°C and has good readability in direct sunlight. The feature phone has an optional 8 MP camera, which includes autofocus, LED flash and flashlight. An advanced rechargeable battery and energy management enable long operating times and it has global Ex certifications.

Pepperl+Fuchs (Aust) Pty Ltd

www.pepperl-fuchs.com



SINGLE-PAIR ETHERNET CABLE

Single-pair Ethernet (SPE) is a key technology on the way to the smart factory and Industry 4.0. It enables consistent and efficient industrial Ethernet networks and only needs one pair of cores to transmit data. This saving enables smart components to be integrated into the network, which were previously not networked via industrial Ethernet.



The ETHERLINE T1 Y Flex 1x2x22/7 AWG from LAPP is a UL-certified, two-core data cable for high-speed information exchange that maintains the same high data rates while reducing the set-up required. Due to its small bending radius and small outer diameter, it is lightweight and easy to install.

The Power-over-Data-Line compatible cable complies with IEEE 802.3bu and has been specially designed for transmitting digital signals in the frequency range up to 600 MHz over distances of up to 40 m. It enables a simultaneous power and data supply to SPE terminals with low energy consumption (up to 50 W). With an aluminium-laminated foil and copper braid screening with a high degree of coverage (SF/UTP), it is double shielded. In addition, the PVC outer sheath is resistant to acids and alkalis and is partially oil resistant. As a UL/CSA-certified Power Limited Tray Cable (PLTC), the single-pair Ethernet cable can also be installed openly on cable trays.

Treotham Automation Pty Ltd

www.treotham.com.au

PLANTS FOR INDUSTRY

k|r|s|t TANK MOUNTED ROTARY SCREW EFFICIENCY

High performance and efficiency in a low cost, compact rotary screw package

A totally integrated plug in, power plant that delivers high performance and outstanding reliability with the lowest possible energy input.



Backed by our fleet of expert mobile technicians, 24/7

kaishan.com.au

National Sales & Service: 1300 098 901



MACHINE SAFETY MYTHS

TEN COMMON MISCONCEPTIONS TO WATCH OUT FOR

Many machine safety-related misconceptions continue to be widespread in manufacturing.

Although the consequences of inadequate or misplaced machine safety practices can be severe, there are, nonetheless, a number of misunderstandings in existence that put many facilities — and their employees — at risk of accidents. Lack of safety knowledge and proper training can lead to poorly functioning safety systems. This article examines the causes of machine safety misconceptions to help manufacturers better understand this important topic.

What trends are currently causing a deficit in machine safety knowledge?

Misconceptions about machine safety are currently on the rise — in part because older workers are retiring in large numbers with few mid-career workers to inherit their expertise. This trend is causing many industrial facilities to lack the engineering expertise required to ensure that their machines meet modern safety standards.

In addition, an increase in the prevalence of newer, fully automated solutions may in some cases lead to complacency, as manufacturers believe (mistakenly) that their new systems must be compliant. This brings us to our first machine safety myth.

Myth 1: If a machine is brand new, then it must be compliant

This is false. Generally, OEMs have no legal obligation to include safety measures on their machines. This is usually due to cost considerations, as safety products and compliant solutions may make the OEMs less competitive in the market. Furthermore, safety usually isn't a core competency of these companies, so they avoid designing safety solutions that they have little expertise in. All of this means that safety measures have become the responsibility of the end user.

End users, of course, also face the need to minimise costs. This can unfortunately lead to a tendency to cut corners on a safety system. In some cases, manufacturers worry that safety measures hamper productivity and make processes less efficient.



©stock.adobe.com/au/TML5PhotoG

Although it's true that safety systems can slow down some processes, their benefits far outweigh the costs. Poorly designed systems can lead to serious injuries or even death, and there's no excuse for knowingly putting someone's life in danger. Furthermore, when it comes to costs, safety measures actually save money in the long run by helping to avoid expensive, traumatic incidents. Although the upfront investment is always a consideration, it shouldn't deter facility leaders from implementing a solid solution. In fact, if there's one important myth to debunk in this article, it would be that the cost of safety measures is too high.

Myth 2: Safety is too expensive, and it reduces productivity and efficiency by adding extra steps to key processes

The costs of an accident — which could be several times the initial investment in safety infrastructure — immediately demonstrates the falsehood of the above statement. These costs include not only fines and workers compensation, but also lost productivity due to poor

morale. An on-the-job injury affects not only the injured person, but also the employees who witnessed the accident or learned of it after the fact. The stress of the event and the resentment towards an employer that failed to protect its people — particularly if the employer is found to have knowingly ignored safety standards — is likely to lead to apathy and higher turnover.

To address the effect of safety measures on overall productivity, it's important for manufacturers to note that safety measures can be designed in ways that don't impact the efficiency of the machine. An example of this would be an application that uses a safety laser scanner to minimise downtime in areas with collaborative robots. In this scenario, if a worker enters the robot work area, the safety laser scanner will trigger the robot's reduced speed mode and cause it to slow down to a safe operating level. When the employee steps out of the area, the robot will go back to its faster speed.

Misconceptions about administrative controls and training vs good engineering

Some manufacturers mistakenly believe that they can substitute engineered safety solutions with enhanced training and the implementation of strict guidelines for employee behaviour around dangerous machinery. Although thorough training is obviously beneficial and necessary, the presence of administrative controls alone doesn't constitute a true safety solution. It's not enough to simply change the way employees work; there must also be safeguarding measures in place to physically prevent them from entering the hazard zone. This brings us to our third major misconception.

Myth 3: Good administrative controls and comprehensive employee safety training can replace good engineering

Thinking along these terms can put employees in harm's way. In the US, for example, the foundation of machine safety consists of a hierarchy of controls published by the National Institute for Occupational Safety and Health (NIOSH), which lists administrative controls and personal protective equipment (PPE) as the least effective ways to mitigate risk. Physically removing the hazard and replacing the hazard are the most effective measures, but these can be impractical. Engineering controls form the middle ground for protecting operators from hazardous machine motion (see Figure 1).

Misconceptions about exemptions for older equipment and smaller companies

Retrofitting a safety system onto legacy equipment can be a challenge, and some manufacturers are under the impression that older equipment doesn't fall under the same standards as new equipment. They cite the fact that these machines were built before certain safeguarding standards came into existence as justification for their decision not to implement engineering controls. However, the idea that older machines are exempt from safeguarding requirements is a myth that can easily lead to a standards violation and possibly a serious accident.

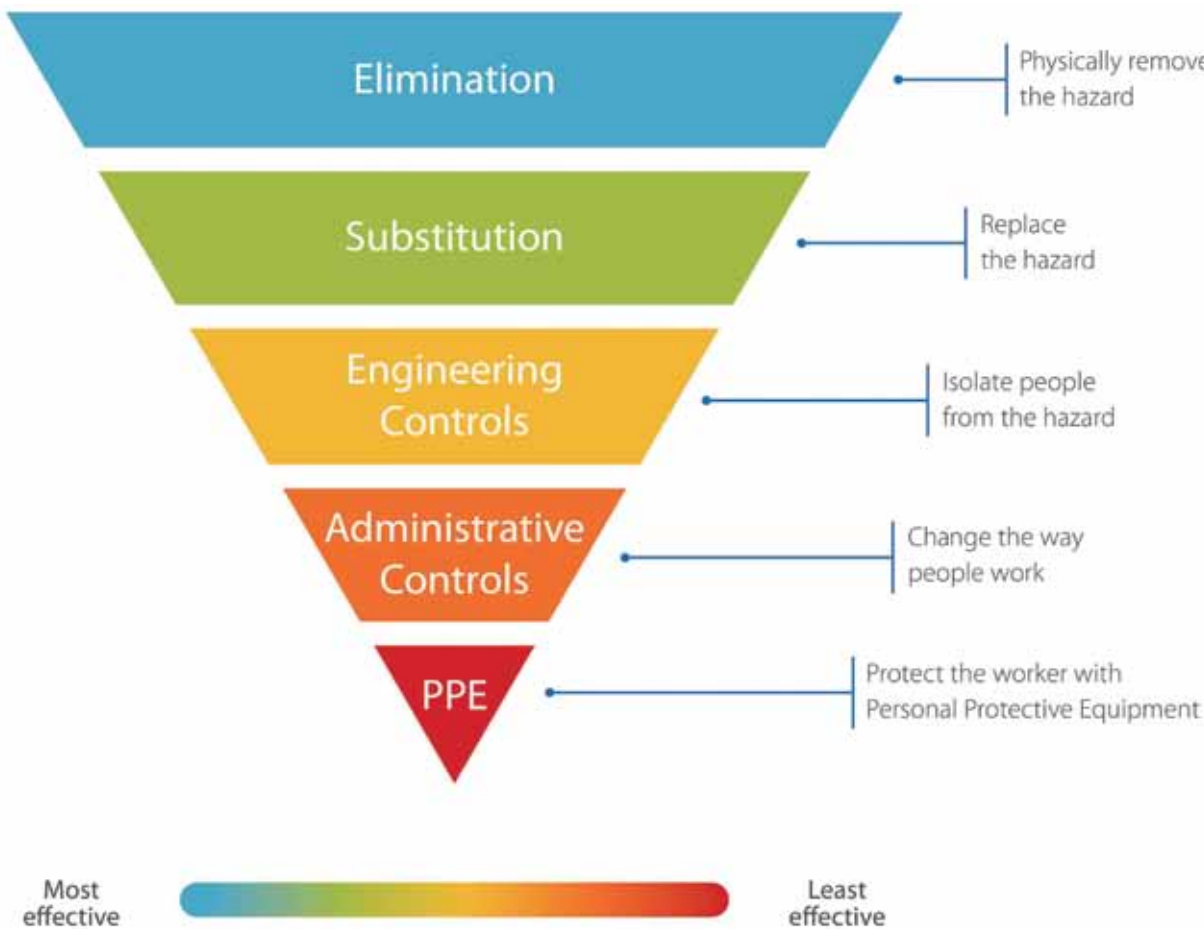


Figure 1: Hierarchy of safety controls.

Myth 4: Older machines can be 'grandfathered in', so they don't need safeguarding

No equipment is exempt from current machine guarding standards, and so-called 'grandfather clauses' simply do not exist for machine safeguarding. An exemption does exist under some robot standards, and it applies to a robot's safety circuit integration. This very narrow exemption has led to some confusion as manufacturers mistakenly interpret it to apply more generally.

The underlying reason for the resistance to retrofitting legacy equipment with current standards-compliant safeguarding is the cost. This concern also relates to another misconception that exemptions exist when there are none, this time with regards to smaller companies. Smaller manufacturers have much less cash on hand than larger manufacturers, so there's a tendency to believe that the rules don't apply in the same way.

Myth 5: There are machine safeguarding exemptions for smaller companies

This is false. All companies are required to safeguard their machines properly and protect the lives and safety of their employees. What may depend on company size is the amount a company is required to pay in case of a safety violation. In general, regulatory agencies see enforcement actions as a way to motivate compliance, rather than simply functioning as punitive measures. Regulatory bodies often have discretion in the nature and size of an enforcement actions. They can issue a warning or a fine, or — in extreme cases — lock out non-compliant equipment. In determining the appropriate level

of enforcement, the agencies will look not only at the seriousness of the infraction and whether it's a repeat violation, but also what would be necessary (within statutory limitations) to motivate the offending company to bring its equipment into compliance.

Misconceptions about identical machines and machines that have been moved

Another way that some companies seek to cut corners is to avoid performing risk assessments on machines that are very similar or that have been moved or modified slightly. This brings us to machine safety myths 6 and 7.

Myth 6: When several machines are identical, it's only necessary to do a risk assessment for one of them

This is not necessarily true; it depends on the complexity of the machine. Even seemingly insignificant differences between machines and their positioning relative to one another could change the outcome of a risk assessment. For instance, the addition of a small step to one of several otherwise identical machines could be sufficient to place a worker in harm's way.

Myth 7: If a machine was assessed for risk before it was moved to a new location, there's no need to do another risk assessment

As with the previous myth, this depends on the complexity of the machine. Moving it to a new location could create a requirement



for a new risk assessment. When assessing access to a hazard on a machine, safety assessors should determine whether an employee can reach around, under, through or over a safeguarding measure to reach a hazard area. When a machine is first assessed in its original location, there may have been a wall or another structure blocking access to part of it. Once it's placed in a new location, the immediate surroundings may not block access in the same way, giving employees unrestricted access to the hazard. Similarly, the new location may include nearby steps that allow someone to reach over a guard in a way that they couldn't have done previously.

Engineering-specific machine safety misconceptions

The more technical aspects of a safety system can also be rife with misunderstandings. Here are a couple of the more frequent ones that have been found during our risk assessments.

Myth 8: A gate using a padlock to prevent access is an acceptable and sufficient safety measure

This is false. Movable guards providing protection against hazards need to be interlocked to signal the apparatus to stop. Fixed guards should be securely held in place either permanently (by welding, for example) or by means of tamper-resistant fasteners that make it impossible to open the guards without using tools that aren't readily available to operators on the manufacturing floor. Since the guards must never remain closed without their fasteners, a gate must be fastened shut or interlocked.

Myth 9: Performance requirements for safety measures stop at the wire

This misconception has to do with the ways in which various energy sources must be safeguarded. Many manufacturers believe that safeguarding is only necessary when the energy source is electrical. As it turns out, all hazardous energy sources need to be 'single-fault tolerant', including hydraulic and pneumatic sources.

What to look for in an assessment service provider

Given the sheer number of misconceptions that exist with regard to machine safety, it's more important than ever for manufacturers to have thorough risk assessments performed on their equipment by a trusted provider. When selecting an assessment service, companies should make sure that the team is composed of safety experts and engineers rather than sales professionals. The provider needs to have a thorough understanding of machinery control systems and should hold relevant industry certifications from a professional certification organisation (such as TÜV Rheinland) and, in some circumstances, professional engineering credentials. They should also have professional liability insurance.

In addition, these risk assessments should be performed on a regular basis, not just with the acquisition of new equipment but also in accordance with any modification to or relocating of existing equipment. This brings us to our final myth, the debunking of which should come as no surprise given the conclusions of the previous ones.

Myth 10: Safety is something you can just take care of once and then forget about

This is completely false. Safety is an ongoing requirement, and companies must have regular risk assessments performed on their machines to ensure that they meet the most recent safety standards. Standards evolve with the purpose of making workplaces safer, and it's imperative for manufacturers to stay up to date and protect their employees.

Summary

This article should clarify not only the need for regular risk assessments, but also the importance of seeing past the common safety misconceptions to understand what's actually needed to protect workers in manufacturing environments. When it's not feasible to completely remove a hazard, manufacturers must put the appropriate engineering controls in place to isolate the danger source from the operator. There's no justification for cutting corners in this situation, and it's not worth the risk (and financial penalties) of a serious on-the-job accident. A robust and frequently updated safety solution is always a worthwhile investment.

References

1. Mason-Darnell T and Joaquin M 2018, "Machine safety myths: 13 workplace misconceptions, debunked", *Manufacturing Automation*, <<<https://www.automationmag.com/machine-safety-myths-13-workplace-misconceptions-debunked-8691/>>>
2. National Institute for Occupational Safety and Health (NIOSH) 2015, *Hierarchy of Controls*, <<<https://www.cdc.gov/niosh/topics/hierarchy/default.html>>>

Omron Electronics Pty Ltd
store.omron.com.au

LASER DISTANCE SENSOR

The Acuity AR1000 measures targets from 0.1 up to 30 m without the use of reflective targets. It can work with opaque targets, even glowing steel at temperatures up to 1000°C. The accuracy is typically ±3 mm, depending on the reflectivity of target surface, ambient light and temperature conditions.

In simple sampling modes, the AR1000 automatically determines the optimal sampling speed, waiting until it collects enough light to make an accurate measurement. Typical sampling output rates are 6 Hz, but 50 Hz sampling is possible for short ranges and white targets. For long-distance measurements, a larger target with a retroreflective target



material can be used to increase the maximum measurement range to 150 m. The AR1000 has a Class 2, red visible laser diode for simple aiming and setup. The spot size is 5 mm as the light leaves the laser, and the beam has a divergence of 0.6 milliradians.

A standard RS232 or optional RS422 serial interface is available for communication with a computer or PLC. The AR1000 also comes with a standard 4–20 mA analog output. The analog output can be programmed to have a custom measurement span,

and the minimum and maximum currents can be set to any points in the laser's range. The AR1000 has a single limit output for indicating alarms that can be useful for triggering an external device when a target reaches a set position.

Slentech Pty Ltd

www.slentech.com.au

IoT SOFTWARE PLATFORM

PACEdge is an IoT software platform package from Emerson that provides all aspects of edge processing to simplify IIoT application development, deployment and administration. It helps to maximise the value of data to generate real insights and improve operation in safety and energy optimisation.

All components necessary in the IIoT application life cycle are brought together to provide a unified and secure interface to decrease development time and increase deployable footprint. With drag-and-drop programming, preparing software and hardware interfaces is simplified, to allow the connection of systems from the shop floor to user dashboards using a single centralised application platform. The software includes web interfaces for device administration, application development and scalability, with no need for command line configuration.

The platform has been built for a dynamically evolving, cloud-agnostic development strategy and allows easy connection to multiple cloud vendors. Data can be pulled from a cloud vendor, combined with control system data and pushed to a different cloud vendor.

The product is available on Emerson's range of Industrial RXi2 PCs, including its CPL410 programmable automation controller.

Control Logic Pty Ltd

www.controllogic.com.au



TABLET HOLDER WITH E-STOP

IDEC Corporation has developed the HT3P Safety Commander to address a growing need for users who want to incorporate modern tablets into their industrial automation systems, but also need to include a hardwired e-stop and associated functionality. The product is designed to make it easy to hold a tablet securely in an industrial setting, for applications like machinery, robotics, automatic guided vehicles (AGVs) and production lines.

Traditionally, industrial operations personnel have needed to stand in front of fixed control panels, or use dedicated handheld touch panels or teaching pendants. IIoT initiatives are now prompting designers to select mobile tablets as visualisation and control devices because of their convenience and productivity benefits. Tablets can offer many more capabilities than dedicated industrial teaching pendants, which are expensive and can be difficult to use.

The Safety Commander is a handheld device with a slider and adjustable grippers to accommodate tablets ranging from 8–11" diagonal size. It provides key-locking provisions to keep the tablet secure in the device, as well as a sturdy and ergonomic hand grip and strap, for both right- and left-handed users, and an optional neck strap. It also provides a hardwired e-stop button with LED indicator and a hardwired three-position enable switch. The tablet can be rotated to any vertical/portrait or horizontal/landscape orientation.

A 5 m cable is provided along with a USB Type-C port for tablet charging. The unit also offers IP54 protection from water splashes and dirt, and drop resistance tested to 1.2 m.

IDEC Australia Pty Ltd

www.idec.com/australia



POWERFLO
SOLUTIONS

ASHCROFT[®]
Trust the shield.[®]



***ASHCROFT are the CRITICAL APPLICATION SOLUTION EXPERTS[®] in
PRESSURE and TEMPERATURE INSTRUMENTATION.***

When Failure Is Not An Option, consider ASHCROFT Instruments for unrivalled performance, ruggedness and quality. ASHCROFT offer thousands of Product configurations for pressure and temperature gauging, switching and transmitting, with IEC and SIL Certification where required.

Through the recreation of process and environmental conditions, along with in-house metallurgical expertise, ASHCROFT Product Proving can be undertaken to verify Product Quality and Optimal Performance in the most harshest of environments.

Don't take a risk... ASHCROFT have been protecting Plant and People since 1852.

Contact us at POWERFLO SOLUTIONS for local technical support and all aspects of After-Market service.

***Proudly Distributed, Assembled, Stocked, Tested and
Serviced by your Instrumentation Partner***

1300 658 701
sales@powerflo.com.au
www.powerflo.com.au



WIRELESS CAN ADAPTER

Use cases for the Anybus Wireless Bolt from HMS Industrial Networks vary from warehouse installations and AGVs to manufacturing of food, underground mining or rough outdoor applications. HMS has now launched the Anybus Wireless Bolt CAN, featuring CAN-based communication to the host equipment.

The Anybus Wireless Bolt for CAN enables CAN-based, heavy-duty machinery and applications to transfer CAN data over a robust wireless link. Wireless communication is established either over a fast Wi-Fi connection or a Bluetooth link. The CAN data is transported over a TCP/IP link, which enables other standard Wi-Fi infrastructure to also connect to the wireless link if desired.

A typical use case is wireless access to CAN data from an industrial vehicle, such as a bulk material transport truck. For example, J1939 CAN data can be easily communicated to a handheld tablet, which gives the operator full control and visibility of the ongoing bulk material filling process.

The product is said to be fully transparent when it comes to transporting CAN data, meaning that it works with any CAN-based protocol, including CANopen. This opens the possibility to create mobile automation islands in any manufacturing process.

The Wireless Bolt product family also includes other versions that can connect to host equipment using serial and industrial Ethernet connectivity. On the wireless side of the Wireless Bolt, the Wi-Fi and Bluetooth options were recently complemented with a version that supports the LTE standards NB-IoT and CAT-M1, targeting IoT applications.

Global M2M

www.globalm2m.com.au



PORTABLE EMBEDDED COMPUTER SYSTEM

The Crystal Group RE2512 is a portable embedded computer system with advanced thermal management and an all-aluminium chassis.

Features include an 8th/9th generation Xeon D Intel processor, a flexible configuration option with up to six removable drives (SSD). It has a standard 2950 battery, a 43.94 cm TFT LCD wide screen, keyboard and trackpad, and supports 3840 x 2160 resolution. The rugged embedded computer/display is integrated into a protected water-resistant case for transportation.

Field-tested to withstand shock and vibration, extended temperature ranges, harsh elements and harsh environments, the system follows the Intel Roadmap to ensure access to the latest Intel chipsets and processors.

Compact construction provides a footprint of 22.5 x 40.13 x 49.53 cm.

Metromatics Pty Ltd

www.metromatics.com.au



FieldLab Hydrostatic Test Kits

10X as accurate, extremely light weight, and none of the paper and pen hassles of chart recorders

- **Log pressure** up to 70 MPa at 0.1% of reading
- **Log temperature wirelessly** from up to 100 meters away
- **Customize tests** for any length of time and automatically shut down when finished
- **Download data via wireless or USB** to your PC with included FieldLab Desktop Software
- **View test data live** on the FieldLab display
- **Create and customize reports** to include all reference info, graphs of pressure and temperature readings, DUT data, customer info, and more
- **Record pressure and temperature** per AS 2885 or international standards



To learn more visit ralstoninst.com/wnipt-htk or scan the QR code

sales@ralstoninst.com



ISO 9001:2015 Certified • Made in the U.S.A.



ULTRASONIC SAFETY SENSOR SYSTEM

The Pepperl+Fuchs USi-safety ultrasonic sensor system is designed to work in challenging, dusty environments or in outdoor areas. The company says that regardless of material, surface structure and colours, reliable detection is always ensured.

Up to two ultrasonic sensor units can be connected to the evaluation unit of the USi-safety ultrasonic sensor system. They each have a single-fault tolerance, two-channel structure. Reliable protection is therefore possible via each of the two independent sensor channels: a safe sensor system is provided even when only one sensor unit is connected.

One signal output and safe OSSD outputs in accordance with category 3 PL d are available for signal output to a safety controller for each connected sensor unit. Due to the 'wide and shallow' shape of the detection field, the system can be successfully used just above the floor or close to a wall.

Designed for monitoring in three-dimensional space, the optimal protection of machines, vehicles and persons is made possible by the shape of the sound beam: while conventional ultrasonic sensors emit acoustic signals in the form of a radially symmetrical sound beam, the USi-safety does so in an elliptical sound field. Due to the opening angle of $\pm 17^\circ \pm 5^\circ$, a particularly wide detection range is generated in one plane and a narrow detection range in the other plane.

Pepperl+Fuchs (Aust) Pty Ltd
www.pepperl-fuchs.com



Process Automation Solutions for Pressure, Level, Flow and Temperature



**INSERTION
ELECTROMAGNETIC
FLOW TRANSMITTER
SERIES IEF**



**PADDLEWHEEL
FLOW
SENSOR
SERIES PFT**



**SUBMERSIBLE
LEVEL
TRANSMITTER
SERIES PBLT2**



**WET/WET DIFFERENTIAL
PRESSURE
TRANSMITTER
SERIES 629HLP**



**INDUSTRIAL
PRESSURE
TRANSMITTER
SERIES 628**

+61 (0) 2 4272 2055 | dwyer-inst.com.au





Water plant drive upgrade eliminates electrical disturbances

AlburyCity Council in New South Wales operates two water supply systems to manage and treat raw water to provide clear, potable water. The raw water scheme uses three pump stations to deliver raw water to the water filtration plant, where it is treated into safe and secure drinking water for 55,000 residents in Albury and the surrounding region.

One section of the clear water reticulation system features a water-boosting pump station responsible for pumping to water storage tanks on a nearby hill. From here, the system uses gravity to distribute the treated water to nearby communities. It is on standby 24 hours a day, seven days a week, with actual pumping operations of between six hours per day in winter months and up to 16 hours per day during the summer months.

A result of many decades of steady development, the pumping station area now sits among various dwellings including a public school, as close as 20 m.

A problem was recognised in the power system each time the station's pumps would start: it was causing an intrusive electrical disturbance whereby the lights in nearby buildings would dim each time the pumps were started or stopped.

In response, AlburyCity Council engaged ABB Channel Partner Remtron to conduct an analysis of the problem and provide a solution with long-term resolve. Remtron identified that the power quality disturbance was caused by the system's installed soft starter motor controller.

"When the soft starter would activate, the associated soft starting action created unwanted distortion on the power network," said Anthony Merrett, Automation Support Engineer – Drives and Power Quality for Remtron.

The electrical stress caused by harmonics and high starting currents pollute electrical networks with dirty power that can make connected equipment behave erratically. In severe cases they can cause damage to sensitive electronic equipment and interference in communication equipment, and give false readings on measurement devices.

It became Remtron's goal to not only solve the network disturbances, but also assist the council in optimising its system's overall infrastructure to reduce the risk of operational failure, extend equipment lifetime and increase energy efficiency.

Analysis of the existing soft starter and motor pumping system indicated that efficiency gains could be realised by using variable speed drive (VSD) control. A more efficient method to pump water is by using variable flow control and operating at the pump's best efficiency point (BEP).

After installing a VSD, it was observed that when operating at a motor frequency of 45 Hz, water was pumping at 176 L/s, with a current consumption of 135 A. As a comparison, when the motor frequency was increased to 50 Hz, water was pumping at a higher flow rate of 210 L/s with a current consumption of 194 A. Remtron determined that although 50 Hz achieves a greater flow rate, because it's not at the BEP it costs



Anthony Merrett from Remtron and Mitchell Palmer from AlburyCity Council beside ABB's M2BAX IE3 high-efficiency motor.

significantly more to pump. Decreasing the motor speed frequency from 50 to 45 Hz therefore results in higher pumping energy efficiency per litre of water pumped.

A drive and motor package was identified to be the best solution for AlburyCity Council. It featured ABB's ACQ580 ultralow harmonic (ULH) variable speed drives and ABB's M2BAX IE3 premium efficiency motor.

With a typical THD of less than 3%, the ACQ580 water-dedicated drives are engineered to reduce harmonics in the power network. By using this technology, the need for any additional filters or power quality equipment is eliminated.

"We knew we would be saving energy by knocking a couple of Hz off the speed of a motor by installing a VSD, but through this project we now understand how to choose the best motor speed and more importantly all of the other benefits achieved by installing a VSD," said Mitch Palmer, Electrical Supervisor for Construction and Maintenance at AlburyCity Council.

"It's essentially optimising the demands of the process with less wear and tear, lower pump cavitation and hydraulic stress through the pipes, just by being able to reduce motor speed by 10% via the drive," said Merrett. "But first and foremost, it solves the original problem: there's no more light flickering for any building in the area."

As a result of the upgrade, the council has already gained 20–30% in energy savings, which has resulted in reduced electricity running costs.

"I really enjoyed working alongside Remtron and A1 Motors," said Palmer. "Not only did they share their knowledge of equipment solutions and all things electrical, their mechanical comprehension was invaluable. The effects mechanical and electrical components can have on one another when there is a problem is profound, but equally so when all factors have been considered and aligned. The results are genuinely impressive."

ABB Australia Pty Ltd
www.abbaustralia.com.au

NEW
PRODUCTS



COMPACT COMPUTER

Powered by the latest 8th generation Intel Core i processor, the UNO-238 is said to be a high-performance computer in an optimised, compact form factor. To ensure available system resources for diverse applications, the mechanical design of the UNO-238 system has been optimised for easy RAM swapping.

To satisfy most factory usage requirements, the UNO-238 offers multiple I/O including two GbE ports, four USB 3.2 ports, two RS-232/422/485 ports, eight GPIO ports and one HDMI and DisplayPort. The provision of USB 3.2 Gen 2 enables twice as fast data transfer rates compared with USB Gen 1, delivering optimal efficiency for high computing performance. Additionally, to facilitate IoT applications, the UNO-238 can be integrated with additional LTE/Wi-Fi modules for enhanced connectivity and communication via the M.2 2230 (E-key) and M.2 3042/3052 (B-key) slots. The system's versatile I/O ensures the UNO-238 can support diverse factory applications, such as factory automation, process automation and manufacturing execution system (MES) operations.

To accelerate the deployment of IoT applications and integrated solutions from the sensor node to the edge and the cloud, the UNO-238 is equipped with Advantech's WISE-DeviceOn IoT device management software. This allows users to not only rapidly implement applications, but also maximise operational optimisation and transformation. With the built-in EdgeX architecture and container technology, the UNO-238 can be used to manage devices remotely to facilitate centralised management and OTA updates. This enables users to prevent failures and improve maintenance efficiency.

Advantech Australia Pty Ltd

www.advantech.net.au

ONE GIANT LEAP IN BURST DISC TECHNOLOGY...THE **SAFETY CARTRIDGE**

oseco pressure
intelligence



- ONE PIECE ASSEMBLY
 - NO SPECIAL HOLDERS REQUIRED
 - INSTALL BETWEEN EXISTING FLANGES
- FORWARD ACTING DISC TYPE 1"–8" Ø
- REVERSE OPTI-GARD DISC TYPE 1"–12" Ø
- SUITABLE FOR FULL VACUUM

MODEL **HPSR**
HIGH PRESSURE
CARTRIDGE
2500 – 6000psi



AUSTRALIAN AGENT & TECHNICAL SUPPORT

WE HANDLE PRESSURE®



PRESSURE & SAFETY SYSTEMS

Tel: (03) 9699 7355

www.pressureandsafety.com.au

9301 P&SS-VN/NPT



COMPRESSORS WITH INTEGRATED REFRIGERANT DRYERS

The oil-lubricated Boge screw compressors in the S-4 series between 55 and 110 kW now come with an optional integrated dryer. The refrigerant compressed air dryer is characterised by low pressure losses and has been fitted into the housing to ensure its compact design and flat surfaces with sharp lines could be maintained. The refrigerant dryer's electronics and control systems are integrated directly into the device, which is only 400 mm longer than the non-dryer version.

Boge says the S-4 screw compressor provides high delivery volumes with low power consumption. The core element of every individual compressor is the compression pump designed and produced in-house, and the integrated power transmission or direct drive with speed control. The optimally designed cooling air duct and the vertical oil separator, which has been isolated from any mechanical vibration, are designed to provide quiet operation.

The compressed air has a pressure dew point of 3°C and is suitable for use across a wide range of applications. One advantage of the S-4 devices is their reduced footprint in comparison with similar compressors with separate downstream refrigeration — having a different unit to dry the compressed air means increased installation costs for both the electrics and pipework.

Boge Compressors Ltd
www.boge.net.au

DEWESoft®

MEASUREMENT | CONTROL | MONITORING

IOLITE LX
Embedded data acquisition system based on a low power Linux based ARM processor with open architecture being able to act like a standalone data logger, real-time system, and signal conditioning fronted, all at the same time.

IOLITEr
Standard IOLITE aluminium chassis is compatible and can be mounted in any 19-inch rack cabinet. This is perfect for the test-bed installations. The IOLITEr chassis height is 4U and can host up to 12 IOLITE I/O modules.

IOLITEs
IOLITE DAQ system is also available in standalone rugged aluminium chassis compatible with SIRIUS data acquisition instruments. The IOLITEs chassis provides 8 slots for IOLITE input and output slices to be installed.

www.dewesoft.com

Available from Metromatics Pty Ltd | www.metromatics.com.au | sales@metromatics.com.au | +61 7 3868-4255



RUGGED TABLET PC

The Winmate M101S utilises an Intel Core i5-7200U processor at 2.5 GHz with an efficient cooling system to provide stable performance and low power consumption. The M101S supports the latest Windows 10 IoT Enterprise operating system for industrial application requirements and provides an alternative solution for those between general consumer-grade and rugged solutions.

The M101S rugged tablet is designed to be tough, withstanding shock, vibration and drops of up to 1.3 m to concrete according to military standard MIL-STD-810G. With all-around rubber edges and covered I/O ports, the M101S is dust-tight and waterproof.

The M101S offers GPS, GLONASS, Wi-Fi 802.11 a/b/g/n/ac, Bluetooth 5.0 and optional 4G LTE to enable mobile communications. With a built-in 8.0 MP camera on the rear side users can capture photos, videos and documents instantly or utilise the front 2.0 MP camera for applications such

as self-video recording or video communications.

Backplane Systems Technology Pty Ltd

www.backplane.com.au

VISION SENSORS

Different parameters can play an important role in vision applications. Pepperl+Fuchs VOS vision sensors are said to offer a simple solution for the majority of requirements. With integrated optics, lighting and electronic analysis, all the key components are housed in one compact device.

The lenses of the VOS vision sensors can be selected to suit the measurement distance, size of the measurement object and test criteria. Many models feature an integrated ring light, but external lighting is also available in the form of side or rear lighting or light and dark field illumination. Standard interferences and a comprehensive range of accessories allow the sensor to be optimally adapted to the application.

Pepperl+Fuchs provides three different housing designs with the VOS series to meet the challenges of different applications: the VOS1000, the VOS2000 and the VOS5000.

Pepperl+Fuchs (Aust) Pty Ltd

www.pepperl-fuchs.com



Improve Temperature Monitoring for Critical Quality Control Applications

Get more accurate temperature measurement of your media and ensure critical quality control with the new TS+. The TS+ temperature sensor from Turck is easy to program via an integrated multi-color display, ensuring your applications are up and running quickly. And with IO-Link, communicating key process data has never been easier.

Contact us to learn more.

www.turck.com.au

1300-132-566



CAN A SOLUTION PROVIDER HANDLE INDUSTRIAL CYBERSECURITY?

EIGHT QUESTIONS TO ASK

Felipe Sabino Costa, ISA cybersecurity instructor and Moxa LATAM Industrial Cybersecurity (IACS) Expert

The past few years have seen an increased demand for cybersecurity in industrial applications. As a result of this, many decision-makers involved with industrial applications are interacting with cybersecurity for the first time. While many companies hope to invest more in ramping up network security, it is essential they make informed decisions when selecting a suitable supplier or solution provider. Industrial cybersecurity is a complex topic that must include considerations about industrial operations. It is highly recommended that decision-makers do not just look at the specifications shown on fact sheets or datasheets, but also consider key questions that can help ensure they choose a qualified solution provider.

1. What are the indicators that I am selecting a company that has a mature industrial cybersecurity solution?

There are many important factors to consider depending on the industry and application. As the literature usually does not distinguish suppliers from users, the factors mentioned below can be used as a reference for both.

As a starting point, cybersecurity is not only a feature or product. In fact, it is a complex process that involves many different factors during different phases. It is fundamental to establish the pillars 'People', 'Processes' and 'Technologies' on both sides — supplier



©stock.adobe.com/au/sssun Bughdaryan

and end user — as they pass through the lifecycle of integration and maintenance of the cybersecurity solution.

While measuring the cybersecurity maturity of a company can be difficult, it is possible to identify some indicators that can be used to determine how mature the company is. These indicators are explored in more details in later questions and include topics such as threat intelligence processes, how quickly the company responds to incidents, whether its solutions are based on solid and internationally recognised frameworks, whether the company receives vulnerability notifications from external parties and its experience working on industrial applications, as well as services and support before and after purchase.

2. How do I measure the maturity of a cybersecurity solution provider?

It is quite difficult to define a maturity baseline for different companies that may have different frameworks and measurements. However, if we consider the ARC Cybersecurity Maturity Model, a mature company should have established a threat intelligence management process, including a full-time cybersecurity team to respond to any cyber threats. In addition, it should be able to detect anomalies and breaches. Finally, the company should also be able to anticipate potential threats instead of only responding to them, which is the most difficult to achieve. This maturity model considers some key aspects, which can be good indicators of the maturity of a cybersecurity solution provider.

In addition to the factors mentioned above, a company has a higher cybersecurity maturity level when it has implemented a solid threat intelligence process and the team effectively responds to any threats found and maps the vulnerabilities. Companies that are able to anticipate threats are able to offer better solutions.

There are also some additional methodologies, such as the 'Detection Maturity Level Model — DML' and 'The Cyber Threat Intelligence Model — CTI', which measure the maturity of a company based on how they handle threats (although they fall outside the scope of this article). In order for a company to be considered mature with regards to its approach to cybersecurity, it should have established threat intelligence processes and have a dedicated team to quickly respond to any potential threats detected internally or externally.

3. Are there any independent methods to compare solutions?

Inside specific industries there are some recognised frameworks such as NIST and IEC 62443, which give practical and impartial suggestions for product characteristics and general recommendations that businesses operating inside these industries should consider.

It is also important to consider the adoption of both vertical and horizontal standards. Horizontal standards tend to embrace a broader range of industrial applications such as ISA/IEC 62443, while vertical standards often represent a smaller sector, such as NERC CIP for the power sector. Depending on the requirements of each individual sector, there may be additional vertical industry standards that can be used for reference and guidance.

Last, another important indicator to determine the maturity of a provider's offering is whether it follows proven frameworks. The usage of recognised frameworks provides an independent method to compare solutions.

4. How can I calculate the ROI for a cybersecurity investment?

There is still an ongoing debate about how to measure a cybersecurity investment, usually termed return on investment (ROI) or return on security investment (ROSI). Although there is not a single agreed formula that can be easily shared, it is plausible to consider the correlation between cybersecurity investments and the benefits of enhanced safety, increased production stability and others.

As cybersecurity, in a simple manner, is a combination of availability, confidentiality and integrity (CIA triangle), it is possible to infer that investments in cybersecurity directly minimise potential threats to industrial control systems and, as a consequence, increase levels of production and enhance safety. In other words, cybersecurity is the balance between the financial cost you can afford and the risk you can accept.

5. Does the solution provider receive information regarding vulnerabilities from external parties?

Another important factor to consider when evaluating a potential offering is to verify if the solution provider has an open channel to receive information about potential vulnerabilities from external parties. Being receptive to this information is fundamental to developing a more mature solution as well as increasing the reliability of the solution being offered.

For industrial control systems, this capability is still relatively new, but this openness and willingness to improve is vital to ensure a supplier is able to provide reliable solutions. Those who have already embraced this approach are demonstrating that they are well on their way to offering a mature cybersecurity solution.

6. Does the solution provider have success stories for industrial applications that are similar to my own requirements?

The majority of the time, any given industrial application will have unique aspects. Therefore, it is important to understand if the supplier has already developed solutions for a relatively similar application. This minimises, or at least anticipates, potential operational problems because industrial solutions differ from enterprise solutions in many respects.

Whenever possible, decision-makers should request a proof of concept (PoC) in order to make sure that what is being requested can be delivered. It never hurts to emphasise, as recommended by important industrial frameworks such as NIST and ISA/IEC 62443, that any test should not be performed on a live system, but on an isolated external system first, in order to avoid disrupting live operations.

7. Does the solution provider have experience deploying solutions inside OT environments?

It is very important to determine whether the solution provider has enough knowledge of industrial environments so that it is able to support you. While it is true that enterprise and industrial cybersecurity solutions have a lot in common, it should not be forgotten that they are not 100% equal. In order to obtain a tailored industrial solution, different specific requirements have to be considered for each industrial application.

For industrial environments, data must be passed from one device to another very quickly. For the majority of industrial applications, latency is detrimental to the system and is therefore not acceptable. In contrast to this, some latency is acceptable for the majority of enterprise applications.

The environment also plays an important role. For products being developed for industrial environments, the hardware should be built to withstand wide temperature ranges, vibration, dust and other environmental factors. In contrast to this, an enterprise product is not normally required to go through such a rigorous testing process.

Another important capability is if the software has the ability to detect and filter industrial protocols such as Profinet, EtherNet/IP



or Modbus/TCP among others, which are widely used in industrial applications.

From all of the points that have been considered, it is apparent how complex it is to implement an industrial cybersecurity solution. Thus, it is essential that the companies that are providing the cybersecurity solutions really understand this demanding sector.

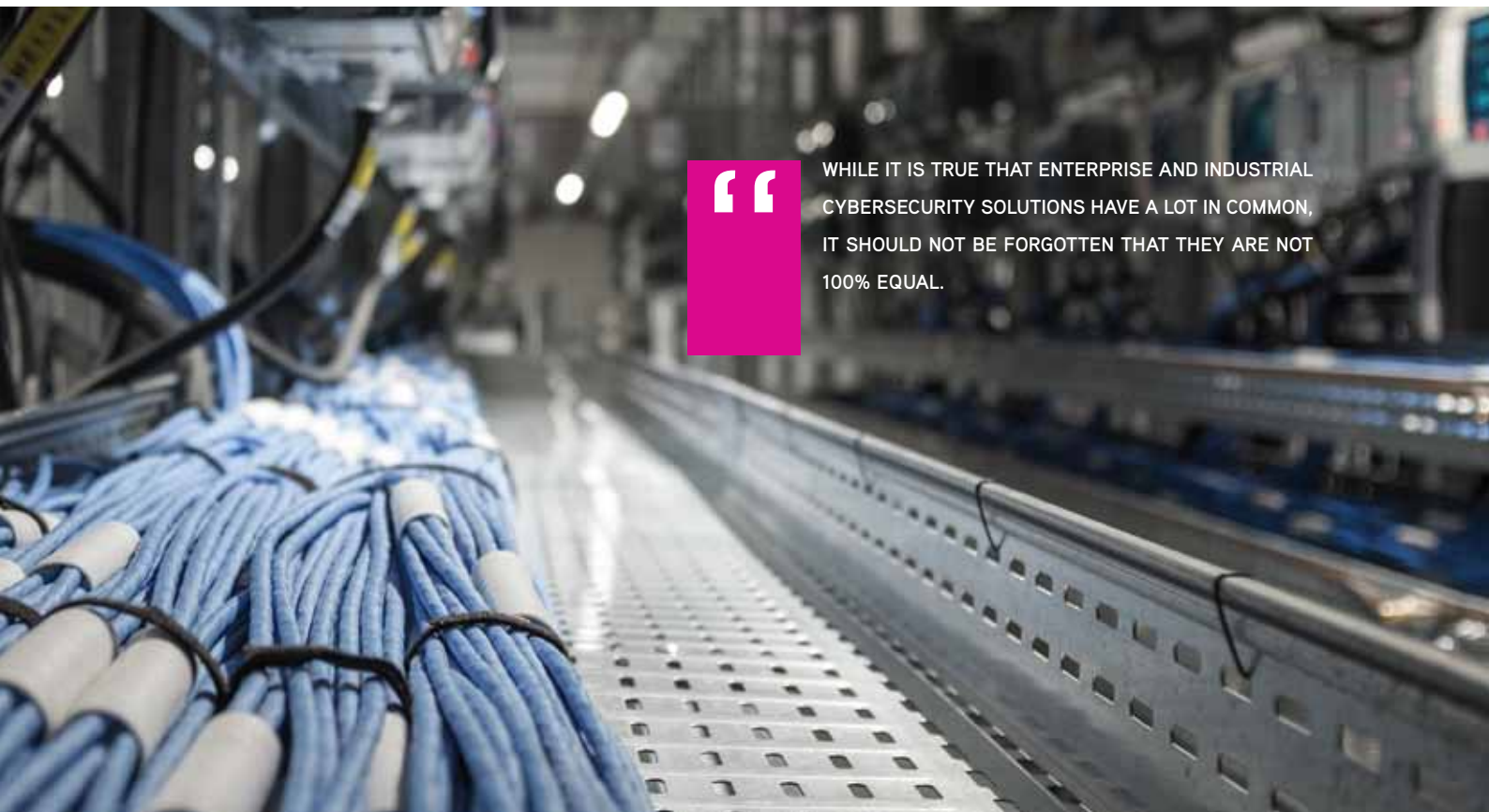
8. Will the solution provider be committed to my business?

When selecting a solution provider, it is important to not just consider the equipment datasheets. It is important to understand whether the security solutions are connected to an overall cybersecurity strategy and how much the solution provider understands your needs.

During the past few years, there has been an increased demand and appreciation for pre- and post-sales services for the majority of cybersecurity customers.

Before you purchase the solution, ensure that your solution provider is aware of your framework and that they have a good understanding of where the proposed solution fits in. The company offering the solution should act like a consultant, and be able to give you good advice for your solution. A vendor that is serious about cybersecurity needs to understand each application and suggest a specific solution for each case. The 'one solution fits all' model is definitely not recommended for industrial cybersecurity.

If your company does not have its own framework, a possible starting point is the Cybersecurity and Infrastructure Security Agency (CISA), which is based in the United States. It utilises solid industrial frameworks within its Cyber Security Evaluation Tool (CSET) and uses this as a foundation to evaluate industrial control systems, including frameworks such as NIST and ISA/IEC 62443 among others. As each country may have its own regulatory



WHILE IT IS TRUE THAT ENTERPRISE AND INDUSTRIAL CYBERSECURITY SOLUTIONS HAVE A LOT IN COMMON, IT SHOULD NOT BE FORGOTTEN THAT THEY ARE NOT 100% EQUAL.

agency, we suggest checking your country's agency framework recommendations if you live outside the United States.

Finally, you should list which services are available after you have purchased the solution such as warranty, troubleshooting, SLA and others. From here, you can decide which services are more important and consider the TCO based on the needs of your company.

Conclusion

In conclusion, it is worth remembering the following two points. The first is that there is an optimal point between the financial cost and level of protection required. Second, IT cybersecurity may not be suitable for an OT environment, so selecting an experienced solution provider should be a requirement.

Further reading

1. Kapellmann D and Washburn R 2019, "Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About vulnerabilities in Industrial Control Systems and Critical Infrastructure", *11th International Conference on Cyber Conflict (CyCon)*, IEEE.
2. ARC Advisory Group, 2019, *Cybersecurity Maturity Model*, <<https://www.arcweb.com/industry-concepts/cybersecurity-maturity-model>>
3. Tounsi W and Rais H 2018, "A survey on technical threat intelligence in the age of sophisticated cyber attacks", *Computers & Security*, vol. 27 pp. 212-233.
4. Mavroeidis V and Bromander S 2017, "Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence", *2017 European Intelligence and Security Informatics Conference (EISIC)*, IEEE.
5. NIST 2015, *NIST Special Publication 800-82 Revision 2: Guide to Industrial Control Systems (ICS) Security*.
6. International Electrotechnical Commission 2019, *IEC 62443-4-2:2019 Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components*.
7. Batard J and Ldovic L et. al. 2019, "Cybersecurity In Distribution Automation: Approach For Common Referential Leveraging Standardization", *25th International Conference on Electricity Distribution, CIRED*.
8. Onwubiko C and Onwubiko A 2019, "Cyber KPI for Return on Security Investment", *2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, IEEE.
9. Von Solms R and Van Niekirk J 2013, "From information security to cyber security", *Computers & Security*, vol. 38 pp. 97-102.
10. International Society of Automation 2018, *ANSI/ISA-62443-2-4 (99.02.04), Security for industrial automation and control systems: Part 2-4, Installation and maintenance requirements for IACS components*.
11. Sommestad T, Ericsson G and Nordlander E 2010, "SCADA system cyber security - A comparison of standards", *IEEE General Meeting Power & Energy Society*, IEEE.
12. Cheraghi SH, Dadashzadeh M and Subramanian M. 2011, "Critical success factors for supplier selection: an update", *Journal of Applied Business Research*.
13. Cybersecurity and Infrastructure Security Agency (CISA) 2019, *CSET 9.2.0 Release Notes*.

Colterlec Pty Ltd

<https://colterlec.com.au/build-secure-network-infrastructure/>

PROFINET CABLE

Profinet is the most widespread industrial Ethernet communication system in the world. Profinet cables are often used in combination with an RJ45 connector in machine tools, packaging technology or the field of handling. While many machine and plant operators already rely on ready-to-connect energy chain systems, users in the field need cables from the drum, which they adapt to the length and harness themselves. This may be the case, for example, if the cable has to be guided through a screw connection into the switch cabinet. Here, the only thing that fits through is the cable but not the connector. To quickly join the connector to the cable, igus has developed FastConnect technology for its chainflex Profinet cables. It means that the CF898.061.FC cable can be stripped and fitted with a connector in just a few steps.

All the electrician needs for the harnessing is the cable, a connector and a stripping tool. For this purpose, igus has designed the inner jacket, the shield and the outer jacket in such a way that the user only has to set the tool once, then remove the cable, insert the connector and close it. The company claims the whole process saves 46% of the time over conventional stripping of a classic cable with pliers and a knife.

Treotham Automation Pty Ltd
www.treotham.com.au



GAS DETECTION DATA LOGGER

The ICP DAS DL-300-WF-IP65 is a gas detection monitoring module with Wi-Fi, Ethernet and RS-485 interfaces. It can be used to record CO, CO₂, CH₂O (formaldehyde), TVOC (volatile organic compounds), NH₃, H₂S, temperature, humidity and dewpoint information, including date and time stamps, and can store up to 450,000 downloadable records.

Real-time data can be accessed from the device using the Windows software or an iOS or Android app, as long as they are connected to the same local network as the data logger. Support is provided for popular industrial protocols such as DCON, Modbus RTU and Modbus TCP. It also supports the emerging machine-to-machine (M2M)/IoT connectivity protocol MQTT.

The DL-300-WF-IP65 series data logger can be connected via widely used communication interfaces including RS-485, Ethernet, PoE and Wi-Fi, meaning that the device can be easily integrated into existing HMI or SCADA systems. The IP65 version of the DL300-WF-IP65 series is designed for industrial applications in harsh environments. A rugged RJ-45 port is said to ensure tight, robust connections for applications that are subject to high vibration and shock.

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

EMBEDDED PANEL COMPUTER

The MPL TRICOR15 is a rugged, embedded, 15" panel computer with Intel processors up to i7 9th Gen, as well as Atom and Xeon processors. It combines a built-in 15" screen with high optical specifications and a core functional module based on MPL's single-board computer.



The system is constructed from a military-grade, high-strength and lightweight HE30 aluminium alloy housing. Its modular architecture allows the system to be easily configurable with many options. The fanless design helps with the noiseless operation, giving the system a longer MTBF. The operating temperature is -20 to +60°C.

Operational accessories such as MIL connectors are available on the sides for easy access. The unit has console-mountable provisions and is suitable for any application that needs a rugged solution.

The product meets the MIL-STD-810F and MIL-STD-461E standards and is suitable for all applications.

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

TRAINING COLLABORATION BETWEEN INDUSTRY AND EDUCATION PAYS OFF



Training collaboration between industry and educational institutions is bearing fruit despite challenge.

Swinburne University of Technology and HYDAC share a history of training collaboration that has served both parties well.

Swinburne University of Technology Manager for Engineering and Industry 4.0 programs Lei Shi has worked with HYDAC Australia on the Associate Degree of Applied Technologies and a third-party agreement to jointly provide vocational education and training.

Integral role of Industry 4.0 when it comes to training

Shi highlights that it is challenging for universities and industries to keep abreast of the impact of Industry 4.0.

“As a result of globalisation and because we’re in a digitisation era we have to embrace Industry 4.0,” he said. “In line with this, Swinburne commenced an associate degree in 2017 to provide training in Industry 4.0.”

Associate degree promotes higher apprentices

Shi explained that Swinburne’s Associate Degree of Applied Technologies is a “unique” product that promotes the higher apprentices compared to the traditional apprentices from an educational perspective.

“The associate degree is a relatively new concept, with awareness and acceptance in industry not as high as a traditional apprentice or traditional location-based education,” he said. “The higher apprenticeships also come with much more flexibility and agility than the traditional training model that is bound by a restrictive training package, thereby limiting flexibility.”

Shi said that HYDAC’s collaboration with Swinburne over the hydraulic training part of the degree has been appreciated.

“HYDAC’s already been on this Industry 4.0 journey for about five years and has provided a lot of equipment for training purposes,” he said.

He cautions however that for the most part Industry 4.0 is still quite new to Australia, with many companies and individuals still predominantly concerned about how the training capabilities of HYDAC and a university will enable them to see concrete benefits on the ground.

From this aspect, he said, collaboration is required between government, universities, and industry to work together to create more tangible outcomes for industry — not only in providing training for Industry 4.0 knowledge and skills but also training that is “centred on working with industry in real life.”

Cyber-physical systems at core of Industry 4.0

Shi says that cyber-physical systems are at the core of Industry 4.0 because it centres on the “two most important factors” to Industry 4.0: sensors and cyber.

“The challenge for education is how a cyber-physical system can be incorporated into learning and training, and for industry it is how Industry 4.0 can be adopted, especially for companies that focus on return on investment and clear evidence as to how investments are benefitting the company.”

Online training a hot topic

According to Shi, online training has become a hot topic as a result of COVID-19 restrictions.

“It is promoted by industry and organisations, including universities, because of the nature of life today — only today I gave a class on artificial intelligence from home,” he said.

However, he emphasises that this form of learning provides challenges for engineering because the nature of engineering courses is to focus on hands-on skills and practical components that students need to master.

An opportunity, according to Shi, would be to extend the experience of virtual reality training as provided by HYDAC, as well as other technologies such as augmented reality to enable students to complete more practical work at home instead of attending lectures at the university or studying in a laboratory.

Swinburne’s Department of Trades and Engineering Technologies is also developing a remote learning cell system to enable students to “remote in” from their home by leaving their computers in the classroom.

Applied research

Shi also said that applied research, a popular concept in Europe, is not being fully utilised in vocational education in Australia.

“In applied research, vocational teachers work together with students and industry on real-life projects. This means that an educational institution’s income comes not only from the training of students but also from industry projects. This makes for good current-practice teaching,” he explained.

Collaboration challenges

Shi concedes that despite there being much good training collaboration between industries and companies there are also challenges to overcome in terms of optimising the strengths of both parties for a better experience for the learner and public.

“Universities such as Swinburne and industrial companies like HYDAC have their respective strengths,” he said. “HYDAC’s strength lies in real-life application and service to the customer whereas Swinburne’s lies in research and broader experience in providing training and education.”

HYDAC International
www.hydac.com.au





COMPACT EDGE INTELLIGENCE SYSTEM

The EI-52 is a compact edge intelligence system that leverages an 11th Gen Intel Core i5/i3/Celeron processor and plug-and-play system design. It features a broad range of I/O ports such as two Gigabit Ethernet, two COM ports and six USB ports, as well as 8 or 16 GB of DDR4 memory and a 64 GB SATA slim SSD. It also offers a broad operating temperature range of -10 to +50°C.

The EI-52 is also integrated with Advantech's WISE-DeviceOn software that supports zero-touch onboarding, remote device monitoring/management and visualised user interfaces.

Using the pre-installed Edge X on the EI-52 enables developers to avoid delving into different data formats and device APIs for connecting edge data to cloud services. Edge X supports over 15 types of protocols for sensing devices and has been tested on more than 20 heterogeneous devices. It further provides an open device SDK to ease device integration using proprietary protocols. This intelligent system enables edge data pre-processing and analysis and comes with preconfigured tools for quick connection to Ali/AWS/Azure cloud applications.

The EI-52 is compatible with a selection of optional packages that enable 5G, AI and quick-start AIoT applications. It is designed to accelerate AIoT smart application deployment, data acquisition application development and remote device management.

Advantech Australia Pty Ltd
www.advantech.net.au

SIGNAL LINE SURGE PROTECTORS

A high-energy pluggable device, the Novaris SL4 and SLC surge protection units offer 20 kA protection, making them suitable for PLCs, fire and security systems, telecommunications, telemetry, railway signalling and SCADA systems.

The SL4 is built with two balanced pair signal circuits while the SLC has a built-in 10 A power supply circuit rated at 24 VDC in the one device.

Protection is possible for up to 150 VDC, depending on the model chosen, including support for RS485 or RS422 serial communications for sensitive devices or where the location is susceptible to lightning strikes. In the event of excessive surge current, the signal line protectors are equipped with protection fuses and a fail-safe design with a red indicator to alert for replacement.

The pluggable design allows for easy removal and replacement, with gold-plated connectors to ensure low resistance between surge protector modules and the DIN rail base. Measuring 12 mm wide, the 20 kA surge protector is easy to install.

Control Logic Pty Ltd
www.controllogic.com.au



**A FULL RANGE
OF CABLES,
CONNECTORS
& ACCESSORIES
FOR ANY
APPLICATION**



Harnessed solutions
are also available

Treotham Automation Pty Ltd - Australian owned & managed
www.treotham.com.au | info@treotham.com.au | 1300 65 75 64

NATIONAL OPERATIONS IN A COVID-19 ENVIRONMENT



Whilst COVID has no doubt been disruptive, it has come with positives. The necessity of having the majority of staff working remotely has forced the evolution of our ISO9001 system to progress to online documentation wherever possible. AMS estimate that we've cut the amount of paper produced in documenting job file information by 75%. The associated on-costs in terms for running a printer have fallen in similar proportion. Prior to that, complex jobs could produce job files using substantial volumes of paper. An added benefit has been increased visibility of job-related data across the organisation. With the relevant supporting data on the server, anyone can access it, whereas previously staff had to go and get the job file from the office storage area and review physical copies. This is clearly a problem for interstate-based staff. Against that, now there are more printers as some of those working from home have had to purchase one to work off-site.

Another difference is the noticeable difficulty in getting access to various sites. Manufacturers in the food and beverage industry seem to be particularly reticent about letting external people on site. Given the potential requirement for deep cleans in the event an infected person is subsequently found to have visited a site, this is prudent and not surprising. There's also the fact that many technical staff are now at least partially working from home. Availability for the traditional face-to-face meeting has reduced accordingly. And now when you do get on site there is often the awkward moment of offering a handshake or not. At least the awkwardness is widespread enough that everyone has been there before and it's often something to laugh about and break the ice. Online meetings and product demonstrations have become more common and YouTube channels have become increas-

ingly important for both process equipment manufacturers and distributors alike. I feel most would agree, though, that these are substandard replacements for actual meetings. We just need to make do.

Planning for site visits has become almost academic. Even now as Victoria, SA and NSW are under lockdown, the idea of planning to visit a site is almost a waste of time: anything beyond a week ahead is a lottery. The only certainty right now is that you'll be working from home and trying to interact with your stakeholders as best you can. We and our suppliers run webinars on technical solutions and applications when we can, but over time it appears to become more difficult to attract an audience. For a while they had some novelty value but now I suspect that technical staff inboxes are inundated with invitations from various sources throughout the industrial sector up and down the supply chain. There is efficiency in being able to attend webinars without leaving your desk but it's also a bit impersonal. That said, television documentaries have found audiences for years and webinars can be very educational.

There has also been a lot of discussion about the security of supply chains and production over the last year or so. Many suppliers are based in countries that have had widespread COVID-19 exposure. In general, they have kept operations ticking over without obvious evidence of supply security difficulties. In our experience, some supplier schedules have drifted out by a couple of weeks and there are isolated incidences of real difficulty, but overall our experience has seen minimal hiccups. One of our suppliers has warned of rising concerns over securing microchips for board assemblies. This is an issue that has severely impacted production in some industries but doesn't seem to have had a broad effect among our suppliers; at least not yet.

Overall, I'd have to say the biggest change has been an increased awareness and focus on managing mental health and motivation among staff. Lockdowns are trying, and the isolation of working long stints from home can wear you down. But having polled most of our staff, the general feeling is that a mix of working from home and time in the office may be the most lasting change we see out of this experience. There are many advantages to working at least some of your time from home, and now it's been field tested to prove it can work.



After studying Electrical Engineering and Accountancy, Tom Kuiper joined AMS. Nearly 20 years later he is the National Sales Manager. As AMS sells a broad range of process equipment, he's been exposed to a wide of applications and industries.



ETHERNET REMOTE I/O MODULES

Acromag's BusWorks NT2000 series remote I/O modules provide an Ethernet interface for analog, discrete and temperature signals.

NTE Ethernet I/O models have dual RJ45 ports and a web server with Modbus TCP communication to monitor or control the internal I/O channels.

An integrated DIN rail bus allows connection of up to three NTX expansion I/O modules. Each I/O module adds up to 16 input or output signals allowing a mix of voltage, current, temperature, TTL and relay control signals networked on one IP address.

The space-saving design requires 25 mm of DIN rail per module. Ethernet I/O modules distribute 9–32 VDC power along the DIN rail bus to expansion modules. Additionally, hazardous location approvals, high noise immunity and -40 to 70°C operation make this I/O suitable for use in harsh environments.

The NT2000 Series offers a broad variety of I/O signal processing options.

Nine I/O configurations are available as either NTE Ethernet I/O or NTX expansion I/O models. Analog I/O models feature eight differential or 16 single-ended inputs, for monitoring current or voltage signals.

Discrete I/O models provide 16 tandem I/O channels with either active high/low input and sinking/sourcing output. A six-channel mechanical relay output model is also available. For temperature monitoring, a thermocouple input model supports many sensor types and also millivolt ranges.

Currently, the NTE I/O modules support only Modbus TCP communication, but will soon include EtherNet/IP and Profinet protocols. The modules typically function as a network slave, but also offer Acromag's i2o peer-to-peer communication technology.

Metromatics Pty Ltd

www.metromatics.com.au

ETHERCAT INCREMENTAL ENCODER

The ICP DAS ECAT-2092T is an EtherCAT slave incremental encoder counter that provides two independent high-speed counter channels. It reads the pulse train generated by an incremental encoder and can be used in positioning feedback applications. Each channel has two counters (A, B) and one index input (C). The inputs can either be single-ended or differential signals. Three counting modes are supported: clockwise/anticlockwise, pulse/direction and quadrant counting mode. Each 32-bit counter and the trigger level (falling/rising edge) can be configured and set by software.

In addition to the encoder inputs, latch input I for each encoder channel allows the latching and clearing of each encoder counter. Encoder position is latched at rising and falling input signal and recorded in two separate registers.

The product also supports position comparison: each encoder channel is equipped with one 32-bit compare register, which compares the counter position with the compare position and generates an output signal when the counter reaches or passes the compare position. The compare function supports single, auto-incremental and array position compare. The pulse width of the compare output can be set. Lastly, each channel has an adjustable input signal filter for filtering out electrical noise.

ICP Electronics Australia Pty Ltd

www.icp-australia.com.au



COMPACT CABINET COOLERS

EXAIR's cabinet cooler systems can be customised to provide cooling within electrical enclosures in NEMA 12, NEMA 4, NEMA 4X and hazardous location environments. These customisations include specific Btu/h values from 275–5600 Btu/h, adaptations for high temperature environments up to 93°C and a selection of materials including aluminium, and type 303 or 316 stainless steel, to combat corrosive environments. For dirty and dusty environments, a non-hazardous purge option will create a positive pressure inside the cabinet to keep dirt and debris from entering the control panel. All systems are UL Listed and CE compliant.

Additional customisations include settings to maintain a specific cabinet temperature, special coatings, high-temperature materials and cold air distribution kits. Cabinet cooler systems are a low-cost way to purge and cool electrical control panels. They convert an ordinary supply of compressed air to cold, -7°C air, without refrigerants. The cold air is circulated through the enclosure to eliminate heat damage and control shutdown.

The compact cabinet coolers can be installed in minutes through a standard electrical knockout hole. Optional thermostat control minimises compressed air use. There are no moving parts to wear out and no maintenance required. Applications include cooling PLCs, microprocessors, variable frequency drives and industrial computers.

Compressed Air Australia Pty Ltd

www.caasafety.com.au



THREE KEY CHALLENGES FACING THE UTILITIES SECTOR

The utilities sector is one of the most essential critical infrastructure industries. Power generation, distribution and supply, water supply and treatment, and natural gas are essential services for the smooth running of society. During a blackout or when the water is turned off, people can't go about their daily lives as normal. When these outages last for longer than a few hours, people find themselves unable to perform basic life functions like eating, drinking, and washing. This can quickly lead to widespread panic and, in the event of prolonged outages, can even cause civil unrest and antisocial behaviours such as looting.

A successful cyberattack on a utilities provider is likely to cause widespread disruption, making these critical infrastructure operators a prime target for cybercrime. Cyberattackers can use connected devices and control systems to disable or sabotage the operational technology (OT) that controls the operations of these organisations. The outcomes can include sustained power outages, toxins leaching into water supplies, or even explosions and equipment malfunction leading to injuries and even death.

SCADA systems, industrial control systems (ICS) and other OT used to be protected from cyberattackers because they were air-gapped. Now, these technologies have become increasingly connected to each other and to the internet, which delivers significant business and efficiency benefits but also opens up these systems to the risk of cyberattack.

Protecting OT from online attacks is not the same as protecting corporate information technology (IT) due to the specialised and often delicate nature of OT assets. Utilities operators usually run a variety of systems with differing age, performance, function, business criticality, and upgrade cycles. Put simply, gaining visibility into the OT network can be a challenging task.

New legislation is coming into force in Australia that will require critical infrastructure operators, such as utilities, to demonstrate how they are protecting their systems and networks against cyberattacks.

When it comes to securing their critical infrastructure assets, utilities are facing three key challenges.

1. Increased complexity

ICS and SCADA systems are being connected for remote monitoring and management, while new systems and capabilities are coming online all the time. This is creating increased complexity in the OT environment, making it harder to achieve full visibility and control over all the systems and critical assets.

2. New equipment and threats

Utilities operators regularly invest in new equipment to increase safety or performance. As new equipment is added to the environment and connected to the network, it creates another potential gateway for a cyberattack unless it is secured appropriately. This trend will continue as organisations in the utilities industry continue to find new ways to provide energy and water.

For example, in the future, micro-nuclear capabilities may create efficiencies as the energy industry looks to replace coal and gas in a bid to reduce CO₂ emissions. These micro-nuclear plants could potentially deliver relatively safe, clean power but could also create an environmental hazard if successfully breached by a cyberattacker.

3. Visibility and control

The long lifespan of OT and its mission-critical function makes it unviable to replace older systems before they reach end-of-life. However, protecting older systems is challenging because these systems were, in most cases, never designed to be connected to the internet. This means they weren't designed with cybersecurity in mind, so they can't be easily patched or protected. Moreover, the use of monitoring agents can disrupt the system's operations, making it an impractical way to gain visibility.

Adding to these challenges, utilities are also constrained by a lack of budget and resources for cybersecurity projects as well as the shortage of specialised cybersecurity skills.

Fortinet International Inc
www.fortinet.com

FORTINET.



Rapid robotics for safety: what a bottle picker can do

Dutch brewing company Heineken is one of the largest beer producers in the world, with more than 70 production facilities globally. From small breweries to mega-plants, its logistics and production processes are increasingly complex and its machinery evermore advanced. The global beer giant therefore began looking for robotics solutions to make its breweries safer and more attractive for employees while enabling a more flexible organisation.

Automatically adapting to the situation

“We are becoming a high-tech company and attracting more and more technically trained staff,” said Dennis van der Plas, Senior Global Lead Packaging Lines at Heineken. “Repetitive tasks — like picking up fallen bottles from the conveyor belt — will not provide them job satisfaction.”

As part of the SMITZH innovation program*, Heineken and RoboHouse fieldlab, with support from the Netherlands Organisation for Applied Scientific Research (TNO), have developed a solution on the basis of flexible manufacturing: automated handling of unexpected situations.

According to Shobhit Yadav of TNO, flexible manufacturing is one of the most important developments in smart industry. “Today, manufacturing companies mainly produce small series on demand. It means that manufacturers have to be able to make many different products. This can be achieved either with a large number of production lines or with a small number that are flexible enough to adapt,” he said.

The Heineken project fell into the second category and involved developing a robot that could recognise different kinds of beer bottles that had fallen over on the conveyor. The robot had to pick them up while the belt was still moving.

“The environment is constantly changing and the robot has to be able to respond immediately,” explained Yadav. “This is a typical example of a flexible production line that automatically adapts to the situation.”

Robotics for a safe and enjoyable working environment

“The automotive industry deploys robots for welding car parts, whereas our sector uses them for automatically palletising products,” said van der Plas. “But with this project we took a different approach. Our starting point was not a question of which robots exist and how they could be used. Instead, we focused on the needs and wishes of the people in the breweries, the operators who control and maintain the machines, and how robots could support them in their work.”

The solution, in other words, had to lead not only to process optimisation but also to improved safety and job satisfaction. In addition, it would result in Heineken becoming a better employer. It is why van der Plas and his colleague Wessel Reurslag, Global Lead Packaging Engineering & Robotics, asked the operators what they would need to



make their work safer and more interesting. One of the use cases that emerged was picking up bottles that had fallen over on the conveyor belt: repetitive but also unsafe as the glass bottles could break.

Experimenting without a business case

Heineken initially made contact with RoboHouse fieldlab through a sponsorship project with X!Delft, an initiative that strengthens corporate innovation and closes the gap between industry and Delft University of Technology. “The lab is the place to meet for anyone involved in robotics,” said Reurslag. “It is also linked to SMITZH and thus connected to TNO.”

The parties soon realised that their ambitions overlapped. Heineken was seeking independent advice and both TNO and RoboHouse were looking for an applied research project that focused on flexible manufacturing. “This kind of partnership is very valuable to all involved,” said Yadav. “SMITZH allows us at TNO to work with current issues in the industry and establish valuable contacts, which makes our research more relevant. In turn, manufacturers have somewhere to go with their questions and problems regarding smart technologies.”

A joint product by TNO and RoboHouse

TNO and RoboHouse distilled two research goals from the use cases presented by Heineken: enabling real-time robot control and using vision technology to direct the robots with cameras. The main challenge involved devising a solution that could be applied to Heineken’s high-speed packaging lines. TNO worked on the control and movements of the robot, while RoboHouse took on the vision technology aspect. This entailed recognising the fallen bottles, developing the system’s software-based control and building the ‘gripper’ to pick up the bottles.

“Communication between the robot and the computer is very important,” explained Bas van Mil, Mechanical Engineer at RoboHouse. “Our input and TNO’s work were complementary. For example, RoboHouse did not possess Yadav’s knowledge of control technology, which is

indispensable for controlling the robot. Through close cooperation, we really developed a joint product.”

Every millisecond counts

The biggest challenge in detecting and tracking fallen beer bottles is that they never stop moving. As van Mil explained, “They do not just move in the direction of the bottle conveyor but can also roll around on the belt itself. In many existing robotic systems, the camera takes a single photo that informs the movements of the robot. The robot will do a ‘blind pick’ with no way of knowing whether anything has changed since the photo was taken. This only works if the environment stays the same — but in this case, it doesn’t.”

The solution involves a system in which the camera and the movements of the robot are constantly connected to each other. “Every millisecond counts, as the bottle will disappear from view and the robot will still try to pick it up from the spot where it was half a second ago,” said van Mil. A RoboHouse programmer developed the camera software to be as fast and efficient as possible. The fieldlab even purchased a powerful computer running an advanced AI system especially for the project.

TNO and RoboHouse then wrote a program together that determines the speed of the robot from the moment a fallen bottle is detected. This enables the robot to move with the bottle based on its calculated speed. It is what makes this robot so different from existing ones. “The robot responds immediately to changes,” said Yadav. “In fact, it is 30% faster than the current top speed of Heineken’s bottle conveyors. As a result, it has a wide range of applications and can be used in a variety of environments with different production speeds.”

Smarter thanks to independent partners

Heineken valued not just the successful innovation but also the independent character of TNO and RoboHouse during the development process. “We now have a much better idea of what is technically feasible, what the challenges are and what we can realistically ask of

our technical suppliers,” said van der Plas. “Thanks to this project, we can act much more like a smart buyer and make smarter demands of our suppliers. This information is relevant to have, especially as we operate in such an innovative field where we do not just buy parts off the shelf. After all, if I ask too little, I will not get the best out of my project. But if I ask too much, it affects our relationship with the supplier.”

The project has also served as a source of inspiration for van der Plas’s colleagues worldwide. “We have been sharing videos and reports from SMITZH on the intranet, building a kind of community within Heineken. We are receiving feedback as well as requests for the new robotic systems from breweries all over the globe,” he said. To meet the demand, van der Plas and Ruurslag want to supply breweries with a ready-to-use version. “We are currently looking for parties that can make the technology available and provide support services.”

Wessel Reurslag, Global Lead Packaging Engineering & Robotics at Heineken, is already looking for the next step: “A robotic solution that is plug and play, flexible and easy to integrate in the brewery.”

Meanwhile, RoboHouse and TNO aim to continue optimising the robot. “This is only the pilot version”, said van Mil. “We can still improve its flexibility, for example by installing a different vision module, thereby making the technology even more widely applicable.” Both organisations are therefore looking for use cases in which they can use the same technology to solve other problems. “We are looking at the bigger picture,” explained Yadav. “This project could serve as a model for similar challenges in other industries.”

**SMITZH is an innovation program focused on smart manufacturing solutions in West Holland. It brings together supply and demand to stimulate the industrial application of smart manufacturing technologies and help regional companies innovate. Each SMITZH project consists of at least one manufacturing company and a fieldlab. RoboHouse served as the fieldlab in this project.*

Story originally published on RoboHouse: Original text by Joost van de Loo; photography by Daniel Verkijk.



MEDIUM-VOLTAGE DRIVES

Rockwell Automation has announced that its Allen-Bradley PowerFlex 6000T medium-voltage drives now include TotalFORCE technology, which is designed to provide precise control of speed and torque, diagnostic information for tracking system health, and automatic adjustments to keep operations running smoothly.

The drives follow speed or torque commands closely in both open- and closed-loop vector control modes to deliver the control required for high performance and large loads. The drives also continuously monitor operations to track the health of electrical components in the drive and motor, and provide real-time diagnostic information to the control system. With this information, users can better predict maintenance requirements well before component failures and take action to prevent unplanned downtime.

Additionally, adaptive control features within the drives are said to help isolate potentially harmful vibration and resonances, and automatically compensate for variances to help keep applications running. With load-observer technology, they also effectively reject disturbances when loads change suddenly, helping to keep operations running smoothly and increasing output.

Rockwell Automation Australia

www.rockwellautomation.com/en-au.html

**NEW
PRODUCTS**



THE CRAFT OF DIGITAL BREWING

As the head of our food and beverage portfolio in the region, I have a particular fondness for how automation and digitalisation have been helping our local craft brewers share their art with the world. There's no better example of technology making a difference to our everyday lives than its impact on the production of our much-loved beer.

Investing in good, scalable technology is vital for any industry, but more so for craft brewers as success could be overnight and production then needs to be ramped up quickly. There are a number of reasons why digitalisation is critical to craft brewing.

Firstly, high productivity and operational flexibility are important. Craft brewing is a highly competitive market and brewers rely heavily on high productivity and operational flexibility to succeed. According to the Independent Brewers Association (IBA), there are now over 600 independent brewers in Australia. New hops are hitting the market at never-before-seen speed and flavour profiles are changing almost weekly. Brewers must respond quickly to keep ahead. From a tech perspective, two critical factors make a big difference to speed to market: a) very precise cleaning between brews done quickly; and b) fine-tuning recipes and minimising brew times so brewers can focus on getting one brew through the cycle and then start a completely different style of beverage as soon as possible, enabling a variety of products despite a finite number of brewing vessels.

Digitalisation also improves the final product: today, data and algorithms can help craft the perfect brew. Artificial intelligence

and predictive analysis, combined with tools such as cloud-based industrial applications set up with the right algorithms, not only help save time but also impact cost, efficiency and the bottom line. Platforms like Fermecraft from Deacam are helping craft breweries in Australia use live data to detect the smallest of changes in critical factors such as temperature and humidity, as the smallest variance could make or break the perfect brew. For a brewer resting at home on the weekend, being able to look at their phone and tell if conditions are as they should be, without visiting the brewery, is technology worth its weight in gold.

Scalability is also a major factor for small breweries, in that they need to be able to start small but plan big. Craft brewers usually don't start with a lot of funding or investment, so having access to bite-sized versions of the same technology used by some of the biggest manufacturers worldwide is not just a benefit for the short term but also helps set them up for long-term growth. Investing in technology that can be scaled as the brewery grows or adapted as they shift from kegs to cans, as Wolf of the Willows did when the pandemic hit, sets brewers up for the long term.

I grew up in the Melbourne suburb of Mordialloc, home to a lovely beach and Wolf of the Willows brewery that uses technology from our company. I wear my T-shirt from the brewery with pride as my life, my passion for beer and technology all intertwine. It's a good day knowing the purpose of the technology you take to market has helped create the perfect sip of ale.



Justin Farrell is the Head of Factory Automation for Siemens Australia and New Zealand. This role covers various sectors such as food and beverage, transport and infrastructure, manufacturing and others.

40
CELEBRATING
YEARS

wfmedia
connecting industry

Westwick-Farrow Media
A.B.N. 22 152 305 336

www.wfmedia.com.au

Head Office

Unit 7, 6-8 Byfield Street, North Ryde
Locked Bag 2226, North Ryde BC NSW 1670

AUSTRALIA

ph: +61 2 9168 2500

Editor

Glenn Johnson

pt@wfmedia.com.au

Publishing Director/MD

Geoff Hird

Art Director/Production Manager

Julie Wright

Art/Production

Colleen Sam, Veronica King

Circulation

Dianna Alberry

circulation@wfmedia.com.au

Copy Control

Mitchie Mullins

copy@wfmedia.com.au

Advertising Sales

Industrial Group Sales Manager

Nicola Fender-Fox – 0414 703 780

nfender-fox@wfmedia.com.au

Sandra Romanin – 0414 558 464

sromanin@wfmedia.com.au

Tim Thompson – 0421 623 958

tthompson@wfmedia.com.au

Subscriptions

For unregistered readers price on application.

If you have any queries regarding our privacy

policy please email

privacy@wfmedia.com.au



Contact the editor

Printed and bound by Bluestar Print

Print Post Approved PP100007403

ISSN No. 0819-5447

All material published in this magazine is published in good faith and every care is taken to accurately relay information provided to us. Readers are advised by the publishers to ensure that all necessary safety devices and precautions are installed and safe working procedures adopted before the use of any equipment found or purchased through the information we provide. Further, all performance criteria was provided by the representative company concerned and any dispute should be referred to them.

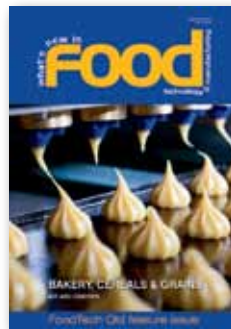
Information indicating that products are made in Australia or New Zealand is supplied by the source company. Westwick Farrow P/L does not quantify the amount of local content or the accuracy of the statement made by the source.

FREE

to industry and business professionals



The magazine you are reading is just one of 11 published by Westwick-Farrow Media. To receive your free subscription (magazine and eNewsletter), visit the link below.



www.WFMedia.com.au/subscribe

Beamex MC6-T

New revolutionary temperature calibrator



AMS

The Beamex MC6-T is an extremely versatile portable automated temperature calibration system. It combines a state-of-the-art temperature dry-block with Beamex MC6 multifunction process calibrator and communicator technology.

With the ability to generate temperature as well as measure and simulate temperature and electrical signals, it offers a really unique combination of functionality. In addition to temperature calibration abilities, the MC6-T also offers electrical and pressure calibration capability, all in one device.

It offers versatility, that no other temperature calibrator can match.

AMS INSTRUMENTATION & CALIBRATION PTY LTD
Unit 20, 51 Kalman drive
Boronia VIC 3155
AUSTRALIA

Phone: +61-3-9017 8225
Fax: +61-3-9729 9604
E-mail: sales@ams-ic.com.au
Internet: www.ams-ic.com.au