CONTROL SYSTEMS ENGINEERS

AIT

Leveraging SCADA and PLCs

in industrial automation systems

INTRODUCTION

Automation has quickly become an integral part of the overall operations of many industries – including oil and gas facilities, mineral processing, chemical, factory automation, and water and sewage treatment plants – with the importance of supervisory control and data acquisition (SCADA) software and programmable logic controller (PLC) hardware becoming more apparent and necessary.

These technologies are partners for safe, reliable and efficient plant operation. SCADA can be seen as the broad software structure that supports the system, while PLCs are a part of the system that monitors and operates the plant which the SCADA 'oversees'. PLCs utilise SCADA to monitor and control the system functions while SCADA relies on data from the PLCs to provide a visual overview of the plant systems.

Together they can provide flexibility, modularity and reliability in operations, and are the preferred choice for industries that rely on these systems because they can be programmed for specific tasks and operations via a unified programming environment, collect robust data and can be used for predictive maintenance.

However, in order to get the most out of SCADA and PLCs, they need to be adapted to their specific application and its requirements – whether that means meeting a certain level of security, adjusting to the network architecture, converged networks and switch technology, and having data reporting or redundancy.

In some industries, PLC redundancy is necessary to keep equipment operating uninterrupted. Some processes require very little intervention, while others cannot tolerate delays and need a higher level of redundancy where any disruptions could cause significant safety issues to plant or personnel. With a wide range of PLC vendors available, it's crucial to keep this consideration in mind when selecting the right PLC for your application and network.

This white paper looks at the key considerations when designing an automation system with SCADA and PLCs to ensure that it operates efficiently and correctly so that you get the most out of it.

NETWORKS: WHAT YOU NEED TO KNOW

Communication networks and associated network switches are key components in SCADA systems. Communication networks can vary in complexity, size, the type and number of equipment being monitored, the level of security required, the network architecture, latency and bandwidth, along with data reporting requirements.

Industrial networks vs corporate networks

There are two main types of networks: industrial and corporate.

Industrial networks are typically controller level communications and are usually only accessed occasionally for maintenance. These communications are critical as network failure can result in critical equipment damage, loss of power supply, process issues or damage to the environment or personnel.

Industrial networks are specified and designed specifically for the type of connected devices and are sophisticated and complex in nature. Deterministic network behavior is important in industrial networks to ensure reliable communications necessary for application redundancy.

On the other hand, corporate networks require some redundancy at their core to keep critical servers online if a network fails such as an Ethernet switch or router. Typically, redundancy takes place in a matter of seconds and is usually transparent to the end users. They usually use mesh arrangements and interconnecting switches with these topographies supported by protocols to provide loop-free redundant paths to devices.

Corporate networks are designed for the asynchronous exchange of files, email and business intelligence system access as they do not require deterministic message delivery and are not typically affected by network failure.

Converged networks

In the past, operational technology and information technology remained separate and distinct from each other, however this has been changing over recent decades as the disconnect between networks has generated unreliable outputs, and the benefits of enhanced ` and performance have not been realised. This has led to an increase in converged networks.

In many industries there is an increased integration of wired and wireless communications between a growing number of intelligent devices with information technology entering the operational space through smart meters, automated asset distribution systems and self-monitoring transformers to name a few examples.

These converged networks are increasing asset owners' ability to proactively manage their assets, optimise their systems, provide their workforce with greater insight and actionable information, and reduce service disruption frequency and duration.

Communication network architecture

Communication networks encompass both hardware and software, from a basic unmanaged switch with a small number of ports and basic configuration ability, to large-scale mission critical systems that require extensive knowledge of networks including protocols, layering, bandwidth, cabling (copper and/or fibre-optic), security, redundancy and reliability. The network arrangement and architecture requirements are typically covered off at the early design stages of a project to ensure the network system will function as intended, with consideration for integration into a wider network if required.

Basic network architecture may include a single or multiple switches, structured cabling, a connection to the field devices and, for smaller segregated systems, a PC or server. For larger systems it is not uncommon to have multiple switches connected via a ring, star and/or bus topologies, some of which may incorporate layer 3 functionality such as routing, combinations of fibre and copper segments, various protocol capability and even wireless segments to remote or difficult to reach devices.

SELECTING THE RIGHT CABLING

Having the right type of cabling is crucial to reducing direct and indirect costs of a particular system failure. Fibre optic (FO) and copper are the main types of cabling media used and they differ in two key aspects — the physical length of the network cabling segments and the rate of data transmission (bandwidth).

Fibre optic cabling

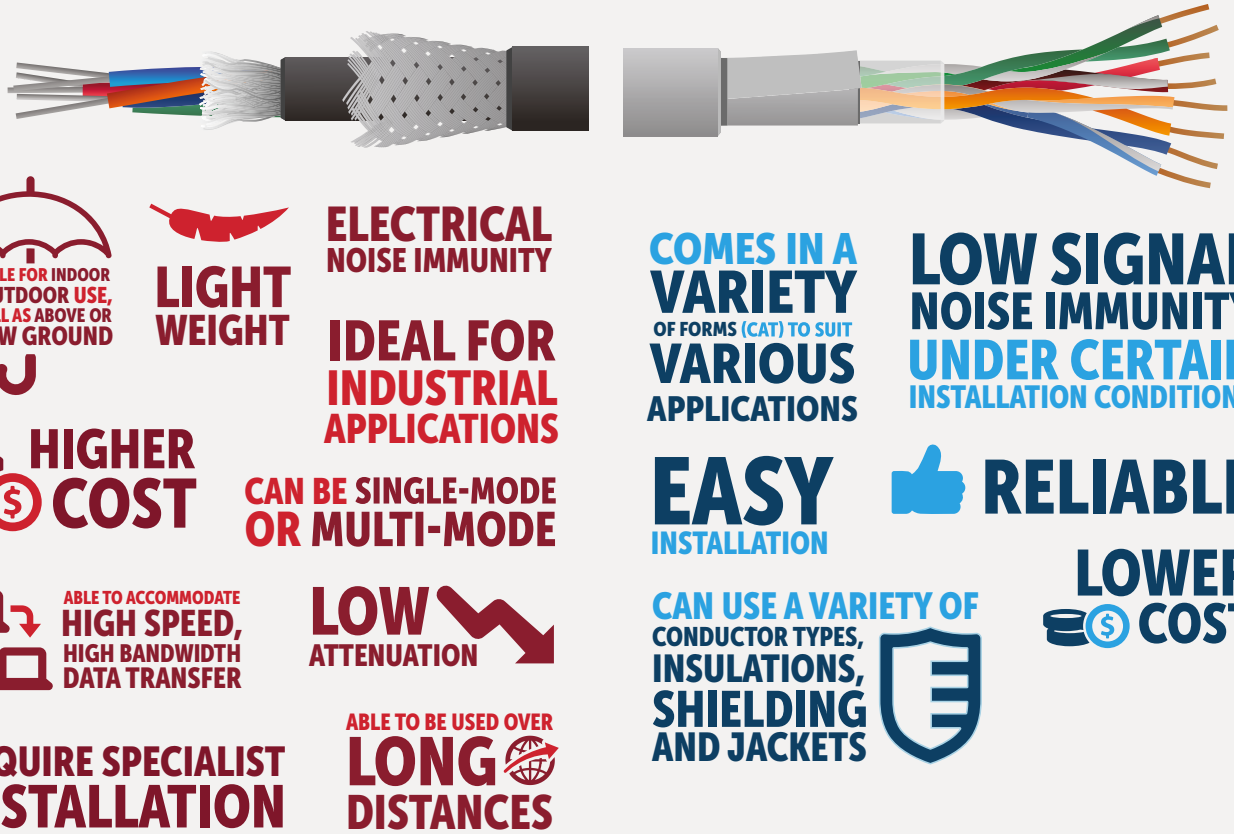
Fibre optic cabling is ideal for industrial applications where high-speed, high-bandwidth data transfer is required. FO cabling typically has advantages over copper cabling including superior bandwidth (more data flow), low attenuation (low signal loss) and very high electrical noise immunity (optical signals are typically not affected by electrically generated magnetic fields), so more data can be transmitted without disruption. Compared to copper cabling, fibre is also lighter, safer and can be used over much longer distances (typically 10-40km however up to 100km are possible before repeaters are required).

FO cables are either single-mode (SM) or multi-mode (MM) and available for both indoor and outdoor use along with above and below ground options. SM FO cables are used where longer distances between the data transmit and receive points are required, examples include telecommunications infrastructure, cable TV companies, universities and mine sites. MM FO cables allow more data to pass and are used in shorter distance applications (<1km) where signal immunity is paramount, such as in an industrial process or automation plant which has a typically noisy electrical environment.

Copper cabling

Copper cabling has traditionally been used in industrial applications due to its low cost, ease of installation, reliability and low signal noise immunity (when using twisted pair/shielded cabling and segregated from power cables or other sources of electrical noise). FO cables are higher in cost than copper cables and also require specialist installation techniques including splicing/test equipment, so the trade-off between signal immunity and speed requires careful consideration.

Copper cabling comes in a variety of forms known as a Category, or CAT, examples include 5e, 6 and 6A twisted-pair cables, with the application requirements determining which form of cable would be best suited. CAT5a has been widely used for general data transfer requirements in the 10-100MB/s data transfer range; CAT6 is favoured for new installations to meet the increasing need for Gigabit data transfer rates; CAT6A can be used for futureproofing, minimising the lack of bandwidth and headroom. Copper cabling uses a variety of conductor types, insulations, shielding and jackets, including armoured sheaths for harsh environments.



Accessing data from devices

Industrial process plants utilise a wide range of field devices to monitor and control systems, with the device data being transmitted via the communication backbone to the associated control station or main data centre. In many cases, the physical backbone is made up of a FO ring, or multiple rings for added redundancy capabilities, to ensure any attached devices are able to transmit their data continuously with no disruption in the event of a single point of failure to the network.

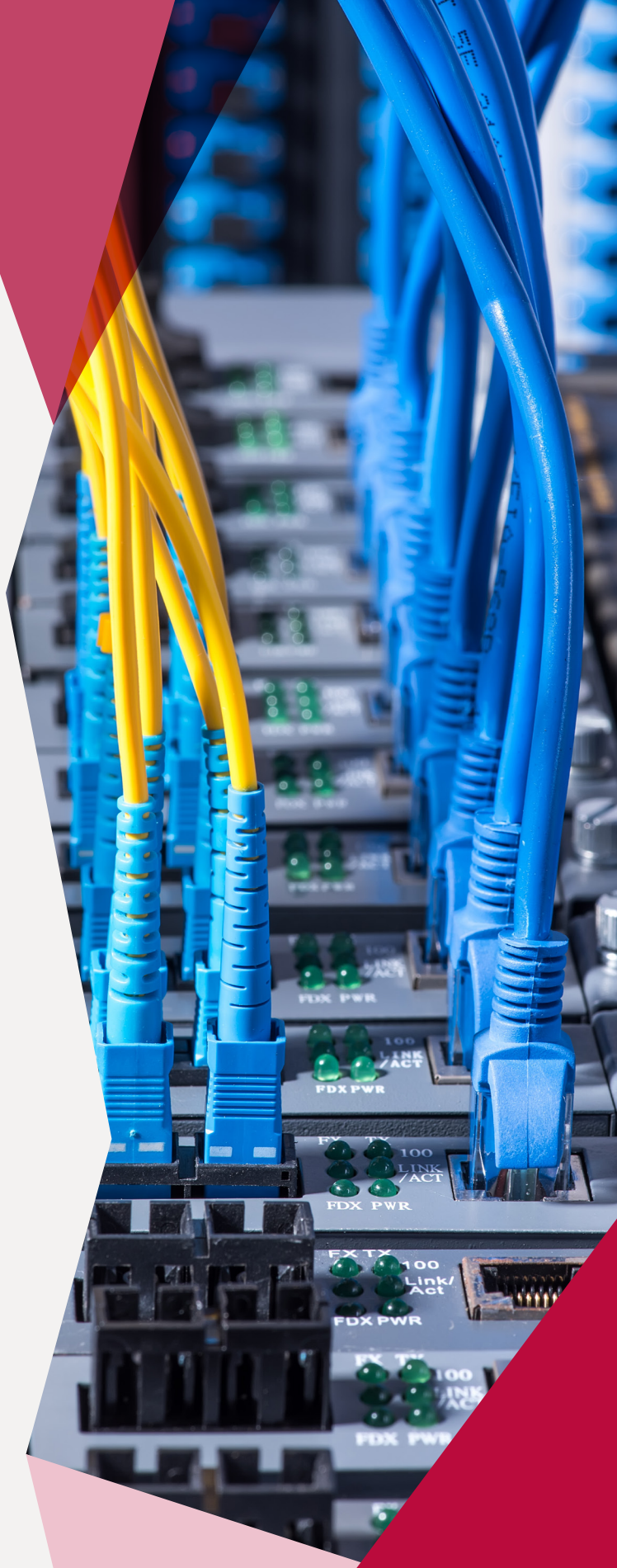
Most field devices or sensors are hardwired using a copper cable and don't typically have the ability to connect directly to FO networks, they require some form of converter. For segregated individual devices this can be in the form of a standalone gateway, or for multiple devices in larger systems connected into network switches. Network switches come in different hardware configurations and many can be specified with copper only ports, or a combination of copper and fixed FO ports or with SFP transceivers.

Another useful technology that has been developed is Power over Ethernet, or PoE. The PoE standard can be used to leverage an Ethernet network, it is designed to deliver low power over the same CAT5 or CAT6 copper cable that transmits data, so components such as CCTV cameras, sensors, field devices, wireless access points (WAP) or other low power devices can be connected to the network without having to install a separate power feed to each device. This can save considerable installation costs and also improve reliability as there are less points of failure to take into account.

There are two relevant standards for PoE: IEEE 802.3af for applications such as VoIP phone or WiFi access points, with a delivery rate up to 15.4W; and IEEE 802.3at PoE + which delivers up to 25.5W while remaining backward compatible with IEEE 802.3af.

The mix of cabling technology allows for robust designs to be implemented at relatively low cost when taking into consideration the total cost of ownership over the expected design life of the system. Having the ability to connect a wide range of devices to a site SCADA system ensures the plant owners and operators have clear visibility of the processes, including the ability to monitor individual communication and cable connections, and to take swift and appropriate action to resolve any issues before they cause a major disruption.

Leveraging off the network infrastructure via SCADA is a great way to improve system process efficiency, improve reporting capabilities, increase the process visibility, reduce plant downtime, reduce safety incidents and reduce overall operating costs.



CORE AND EDGE SWITCHES: WHICH ONE IS RIGHT FOR YOU?

There are two basic types of network switches – core and edge – both require careful consideration when it comes to the design and implementation, including the number and types of devices they will be connecting to, the amount and type of traffic and if management capabilities are required.

A core switch, or backbone switch, is used for connection to equipment such as servers, routers, firewalls and associated lower level network switches. Core switches are designed to be high capacity, have built in redundancy and should always have management capabilities, and they typically connect to equipment that cannot experience downtime.

Compared to an edge switch, core switches have greater features such as higher backplane speed, layer 3 with routing protocols and physical redundancy, and will typically have deeper buffers.

On the other hand, edge switches – or an access node or service node – are used to connect individual devices to a network segment that can access the main network core. Client devices including PLCs, RTUs, laptops, desktops, CCTV and wireless access points are typically connected to edge switches.

Edge switches can be routers, routing switches, integrated access devices (IADs), multiplexers or WAN devices. Edge switches are not usually as critical in operation as the core switches, however if downtime of these devices cannot be tolerated, then redundancy of the entire network can be achieved with managed switches and implementing ring topologies.

REDUNDANCY: COLD, WARM AND HOT

Redundancy comes in many forms depending on the application, however for all situations it is about providing reliability and a process alternative to a failing condition.

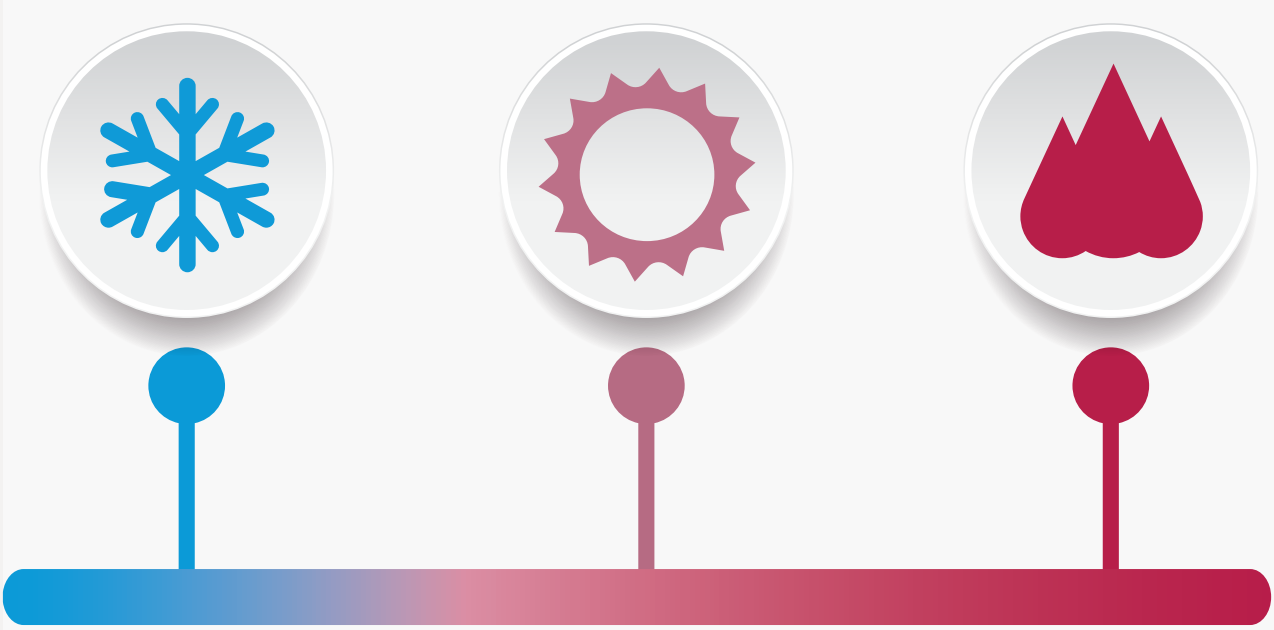
An alternative response can be designed into a process control system at either the component or process level.

Critical systems typically require redundancy at some level in order to keep critical servers or devices online, and keep gathering information and data if a network failure were to occur.

Network redundancy is needed for critical operations where a loss of network connectivity can result in processes stopping or the control system not working as intended, or where the associated costs of such an event occurring are unacceptable. Adding network redundancy in a system can involve device wiring, various types of switches, a ring network or other network infrastructure, as well as network interface cards (NICs) in the computer, PLC, RTU or other devices.

While most PLC vendors provide units with built-in redundancy for processor control and power supplies, extra control hardware and software can be installed to further reduce the risk of damage and inconvenience if a controller should fail. Depending on the consequences of failure, increasing reliability through redundancy can be an easy decision. The tricky part is that not all vendor solutions are equal.

The form of redundancy is dependent on a number of factors and can be classed as cold, warm or hot redundancy.



- Best suited for non-critical processes
- Equipment and process downtime is acceptable
- Human intervention is possible if a problem occurs
- Applications usually have an identical spare PLC or parts thereof close by and access to the latest PLC code

- Momentary outage of processes and equipment is acceptable
- Usually operates in shadow mode where identical software connects the primary and standby processors
- The standby processor is only provided with periodic updates by the primary processor so it may take a few program scans for it to catch up after the switch over has occurred
- The hardware for both warm and hot redundancy systems are almost identical

- Best suited for critical processes where outage cannot occur
- Provides instant process correction when a failure is detected
- PLC programming software and hardware coordination is exact so messages are constantly relayed between processors so they can access common data for a smooth transition
- Provides a seamless transfer of the I/O during the changeover between processors

Cold redundancy

Cold redundancy is best suited to non-critical processes where downtime is not a big concern and human intervention is possible.

For example, if a belt press machine in a large wastewater treatment plant fails, the control system will set off an alarm to inform the operator of the problem. Typically, these plants have several belt presses working in parallel so the operator can then make a decision to take the unit out of service, or resume operation by starting another unit and requesting a service for the failed unit.

In this example, the plant has redundancy of equipment so a PLC failure is not a big deal. Cold redundancy would consist of having an identical spare PLC or parts thereof close by and access to the latest PLC code so that the CPU can be programmed easily. This design is acceptable as the loss of the press is unlikely to have a critical impact on operations and operator intervention is acceptable.

For processes which are more time critical, a warm or hot redundancy design is a better approach.

Warm redundancy

Warm redundancy design is suited to processes where time and response are important but a momentary outage is still acceptable.

Looking at a fluid transfer system as an example, if a valve fails to operate, the pump can be disabled and the system shut down. The length of acceptable time the system can be shut down can range from a few seconds or minutes, or even longer, and will be determined by the product and how long it takes to be damaged, contaminated or start to deteriorate. Generally, the process must be restored quickly and automatically to avoid any integrity issues.

Warm redundancy systems usually operate in shadow mode where identical software connects the primary and standby processors. The primary processor controls the system's input and outputs (I/O) while the standby processor will take control of the I/O if the primary processor goes offline, allowing the system to be maintained without losing process control.

During normal operation, the standby processor is only provided with periodic updates by the primary processor, usually at the end of each program scan and may only involve a portion of the data. This means it may take a few program scans for the secondary processor to catch up to the primary processor after the switch over has occurred. Most warm standby systems will halt the process for this period although they will typically hold the last state of the outputs while the changeover occurs.

The hardware for both warm and hot redundancy systems are almost identical, and care needs to be taken when examining the different types of system as the hardware can easily be confused. It is critical to talk to your system integrator about the hardware selection to ensure you know what sort of performance will be achieved from a system before specifying a certain brand or type of PLC system.

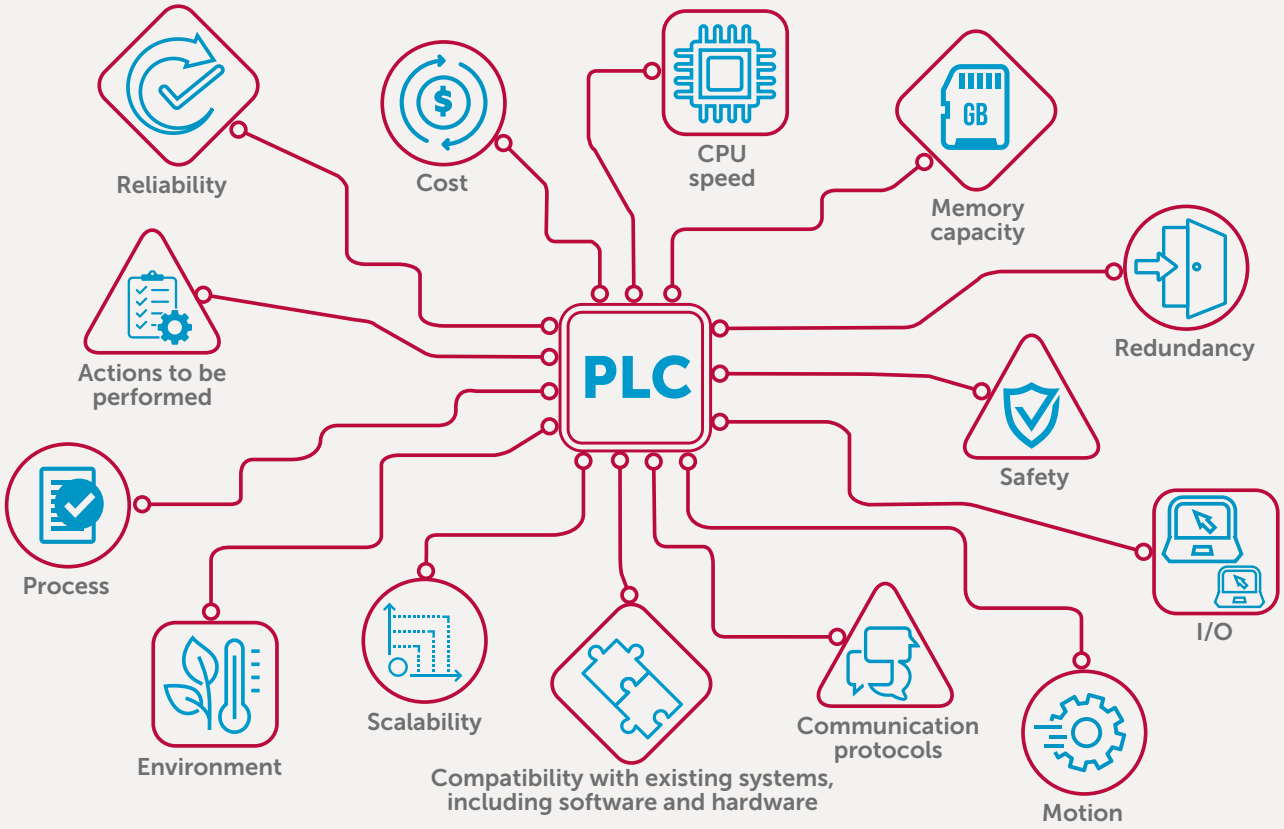
Hot redundancy

While the architecture of warm and hot redundancy systems are very similar, unlike warm systems, hot redundancy systems provide instant process correction when a failure is detected. This makes it the best solution for critical processes which cannot experience an outage for even a brief moment.

Examples of where a hot redundancy system is applicable would be a critical power system for a hospital, an air traffic control system or a process plant with large high-speed machinery. In such applications, if a primary controller fails, a backup one needs to assume control immediately so that there are no delays in the transfer. Any delays in transfer could result in critical equipment damage, supply breakers tripping or delays in generator transfers resulting in power glitches or complete momentary loss.

For hot redundancy systems, the PLC programming software and hardware coordination must be exact to allow processors to constantly relay messages between each other and so they can access common data for a smooth transition to take place. The most important thing is that the secondary processor has knowledge of every logic cycle of the primary processor to ensure data integrity. Some of the best systems available today provide data transfer speeds in nanoseconds and ensure that the data tables of both processors are updated throughout the scan cycle so that when a failure occurs control is transferred to the secondary within a single scan and the process does not experience even the slightest glitch.

Unlike warm redundancy systems, hot systems provide a seamless transfer of the I/O during the changeover between processors.



CONSIDERATIONS WHEN SELECTING AN INDUSTRIAL NETWORKING PRODUCT

There are a wide range of PLCs available for almost any application, so which brand or type would be 'best suited' for a particular project?

There are many considerations that should be taken into account to help narrow down the options for a particular application:

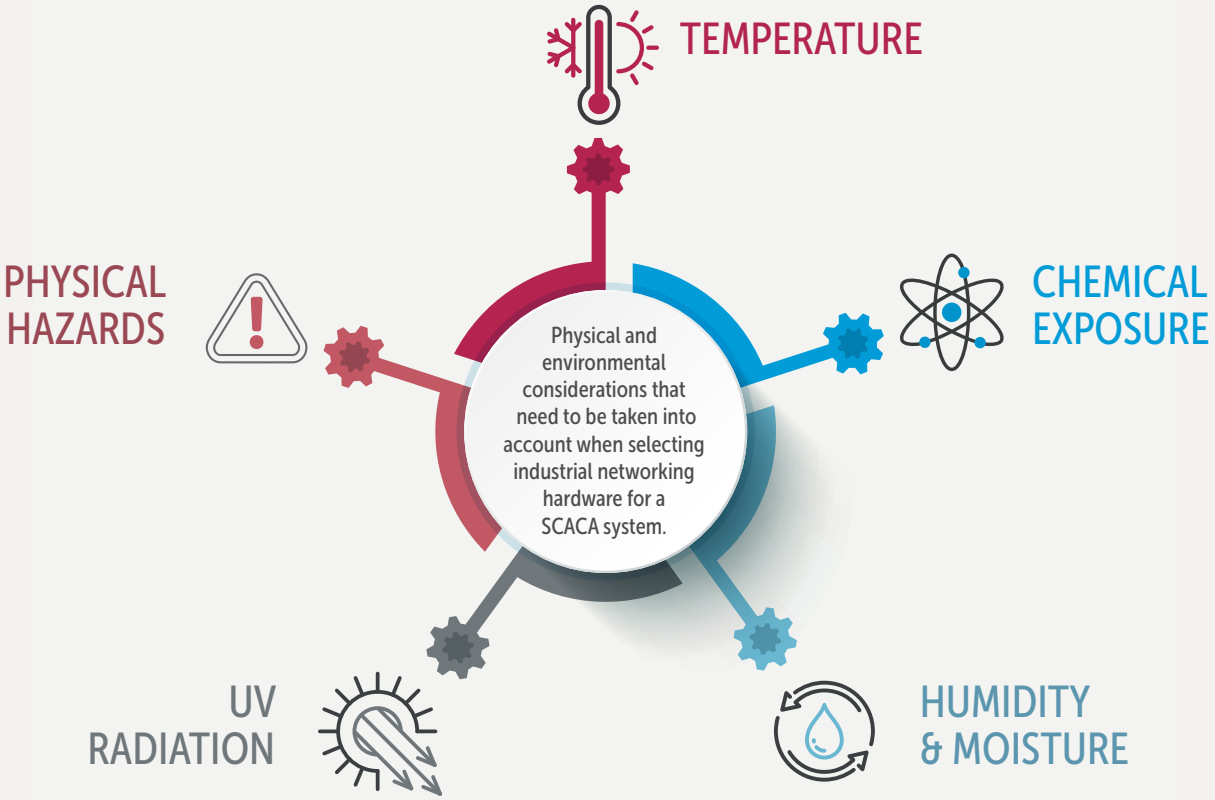
- CPU speed – how big is the system and what response rate does the process require?
- Memory capacity – how much memory is enough? Will an external memory card be required?
- Redundancy – is any level of redundancy required?
- I/O – how many devices does it need to control or monitor? Is there a requirement to work with external or remote I/O interfaces?
- Communication protocols – what devices will it need to communicate with and what protocols are used?
- Compatibility – is the system being built from scratch, or does it need to interface with existing hardware and software?
- Scalability – can the system be scaled up or down to accommodate changes with the system?
- Environment – what type of environmental conditions will it be subjected to? Will it require any special considerations such as conformal coated components, or a more robust option for harsh environments?
- Actions performed – does it need to be able to perform any unique actions, such as motion control, robotics or safety?
- Reliability – is the system expected to run with little or no downtime for extended periods of time, sometimes years?
- Cost – what is the budget? Have things been considered collectively as a 'system', such as the purchase of hardware, software licenses, programming, installation, ease of interface with existing plant/systems, maintenance, and back-up support along with any future upgrade considerations?

The brand and type of switch, cabling, connectors and associated interfaces is dependent on many things, including the size of the network, the network architecture, managed or unmanaged switches, the layer level, rack or rail mount, the client's site-specific requirements, environmental considerations, the bandwidth requirements including what traffic is anticipated, protocol requirements and any specific standards that must be adhered to (DNP3, IEC61850 etc.).

SCADA NETWORK SECURITY

Network security is a growing concern with critical infrastructure becoming a potential target of cyber criminals. This makes it imperative that communication networks and control systems are designed by experienced engineers who are up-to-date with the latest in automation and cyber security technology, trends and standards. As well as a correctly implemented SCADA system, regular security checks, report monitoring and standard protocols need to be introduced and used by anyone with access to the network.

Users should take advantage of permission-based access to restrict who can access certain tools or process areas and ensure external access is authenticated. USB keys cannot be directly plugged into the SCADA PCs, foreign laptops cannot be plugged into spare ports, and email is not directly accessible on the control network.



REDUCING RISKS TO SCADA NETWORKS: PHYSICAL AND ENVIRONMENTAL CONSIDERATIONS

There are a number of physical and environmental considerations that need to be taken into account when selecting industrial networking hardware, including:

Temperature

Commercial products are generally designed to operate in a temperature range of 0oC to +40oC, making them unsuitable for more extreme heat and cold. Extreme high temperatures (>60º) typically cause the sheath and insulation material to degrade, which can increase attenuation and cause partial or total failure of the cable. Extreme cold can cause cables to become stiff and brittle, opening them up to cracking and allowing moisture to penetrate. Industrial-grade networking cables are designed to operate in a wider temperature range and can typically withstand temperatures of-40oC to +80oC, in specialist applications the temperature range is even wider such as-70º to +150ºC.

Chemical exposure

Commercial products are typically not suitable for applications where oils, fuels, solvents, cleaning solutions or corrosive gas environments are present. These gases or chemicals can cause a breakdown of the material with many side-effects including melting, swelling or a loss of mechanical strength. Corrosive chemicals (either liquid or airborne) are usually incompatible with commercial hardware and can easily damage electronic components, PCBs, connectors, plastic housings etc. Industrial products are designed for a long life in harsh environments, some even have the option of conformal coating to minimise the damage to the electronic components caused by airborne corrosive chemicals, salt spray etc.

Humidity and Moisture

Commercial products are not generally suitable for exposure to moisture or excess humidity, they are typically designed for indoor use in a humidity-controlled environment. Industrial-grade products are designed to withstand much higher humidity levels and exposure to a wider range of temperatures, which can be conducive to the production of condensation. Industrial-grade products also offer various levels of ingress protection (IP) as outlined by international standards, up to and including IPX8.

UV Radiation

Many commercial products do not have the same level of UV protection and degrade very quickly if not installed within their design limits. Materials that are not UV resistant end up promptly fading, cracking, losing mechanical strength and pose potential safety risks where electrical wiring is involved, due to the rapid breakdown of conductor insulation. Industrial products are designed to be installed in many different areas of a particular installation, including outdoors, so are able to withstand various levels of ultraviolet (UV) radiation without degradation for extended periods of time, typically years.

Physical hazards

Commercial products are not typically designed for continuous movement or installation where vibration is a factor, any strain upon the product can lead to distortion or failure. Many industrial processes contain physical hazards including elevated levels of movement, vibration, strain, pressure or heat, sometimes all at once. Industrial-grade components are ruggedly built and hardened to withstand such environments, measures to improve reliability and integrity of the products include vibration dampers, armoured sheaths and covers, insulated metal connectors and strain relief mechanisms.

VENDOR OPTIONS

There are numerous vendors that supply industrial networking products including switches, terminals, cabling (copper and fibre optic), connectors and associated interfaces. Industrial switches and associated plug-in modules are designed with long life spans and a suite of network and security configuration tools, the main vendor products utilised in automation and control systems include:

- Cisco
- ConneXium by Schneider Electric
- Hirschmann
- Moxa
- Scalance by Siemens
- Stratix by Allen Bradley

The brand and type of switch, cabling, connectors and associated interfaces is dependent on many things, including the size of the network, the network architecture, managed or unmanaged switches, the layer level, rack or rail mount, the client's site specific requirements, environmental considerations, the bandwidth requirements including what traffic is anticipated, protocol requirements and any specific standards that must be adhered to (DNP3, IEC61850 etc.).

PLC BRANDS: WHAT'S THE DIFFERENCE?

Allen Bradley

Allen Bradley offers a variety of PLC systems including its main flagship platform ControlLogix, along with the smaller sized CompactLogix and MicroLogix.

The ControlLogix and CompactLogix are modular systems that offer a wide choice of processors with different options based on memory sizes, on-board communication requirements, redundancy, safety integration and environmental considerations (extended temperature, conformal coating, etc.).

The ControlLogix platform consists of a separate base chassis, or rack, power supply, processor, I/O and communications modules. There are multiple configuration options available, from small single processor systems with a minimal I/O, to large redundant systems with an extensive I/O count and multiple remote I/O drops, all of which are scalable.

The cost for a ControlLogix system is the highest of the Allen Bradley PLC range, however this is reflected in its proven long life and reliability along with its large-scale control system capabilities. Where criticality or reliability is paramount, ControlLogix is the preferred platform.

CompactLogix consists of a separate power supply, processor and I/O modules, with or without on-board communications, all of which is DIN rail mounted. CompactLogix is typically used where a smaller system or cost is a consideration, although still designed with long life and expandability options.

The MicroLogix is a small 'brick' style PLC with a built-in power supply, processor and I/O with expansion modules available. The MicroLogix system is designed for smaller process and automation control tasks or can be integrated into a larger CompactLogix or ControlLogix system.

For those looking to upgrade an existing Allen Bradley system, all new products have good backward compatibility and legacy support, ensuring there is a migration path from previous models. Product software is also upgraded when a new product comes out to ensure any new hardware features are supported.

Allen Bradley's support service is among the best of the PLC vendors, however there is a charge for programming software, and customers are required to pay an additional annual support fee in order to upgrade and receive the support.

Allen Bradley PLCs also have compatibility issues between some protocols. As an example, most of its products don't communicate smoothly with the Modbus protocol which is widely used in industry. There are ways around this such as installing communication modules or developing software to help facilitate the transfer of data, however both options come at an additional cost.

General Electric (GE) – Now Emerson

General Electric, or GE, has a long history of PLC hardware and software development – GE control systems are now rebranded as Emerson. The legacy 90-30 and 90-70 series are being merged and replaced by the PAC Systems RX3i series.

The RX3i controller provides the foundation for industrial Internet connectivity. It is a powerful, modular Programmable Automation Controller with a focus on high availability. The RX3i features a single control engine and a universal programming environment to provide application portability across multiple hardware platforms.

With integrated critical control platforms, logic, motion, HMI, process control and high availability based on Reflective Memory technology, RX3i increases system performance and flexibility. The RX3i platform contains a range of processors from relatively low-cost offerings through to very high-performance redundant systems with true hot standby capability.

The RX3i CPE400 is the flagship CPU and has an incredible amount of power compared to almost any other PLC on the market, including a 4-core processor and 64MB of built-in RAM. The CPE400 also has a suite of built-in advanced security including Achilles Level 2 certification, so it can mitigate security and operational risks to the control system.

The compact range of Emerson (GE) PLCs consists of the Versamax Micro and Nano controllers which offer a low-cost entry point option. The Versamax standard range is pitched at small to medium systems before the RX3i takes over for larger systems.

At the time of writing, Emerson (GE) PLCs were automating the processes that generate half of the world's power!

Unfortunately, the downside for Emerson (GE) PLCs is the support network within Australia is not as comprehensive as some other major brands, there is extensive knowledge within the distributors network and Emerson (GE) does have local technical support, however the team is small relative to other major brands and occasionally there is a delayed response to certain queries.

Omron

Omron has a wide range of PLC options including rack mount, modular and compact versions. Compared to other PLC vendors, Omron typically provides lower cost options for hardware, software and licences. However, when considering a complete system, additional programming time is typically required due to the nuances of the Omron programming environment, so the benefits of lower component costs can be offset by additional engineering costs.

Omron PLCs are high performing, flexible, reliable and relatively easy to integrate, although currently only have software-based redundancy. Omron has a good reputation in the manufacturing industry for its advanced controllers, which are capable of multi-axis motion control, vision systems, robotics, sensing and safety. Many of Omron's connected devices integrate seamlessly with a PLC system to provide a complete system.

Siemens

Siemens has a wide range of PLC options available, from basic controllers through to large-scale redundant platforms utilised on some of the world's largest and most complex engineering projects.

The current flagship of Siemens PLC range is the S7-1500 advanced controller, with a 1ns 'bit processing time' in the CPU and features such as built-in Profinet, 4-Level security, integrated display and native OPC UA accessibility. The S7-1500 is one of the most feature rich PLC platforms on the market today.

In addition to the advanced S7-1500, Siemens has the range of industry proven S7-300 and S7-400 controllers, the latter of which provides a full redundancy option. One of the features of its S7 PLC range is that it can offer two safety runtime groups, which means the infrastructure can be divided into two groups with each section having different control parameters, including priorities and time cycles. The benefit of this is that operators don't need to stop any processes when modifying the programming blocks and downloading them to the PLC.

Historically, the Siemens S7 PLC programming environment could be challenging for the uninitiated, however the latest Total Integrated Architecture (TIA) software suite provides a wide range of programming options that makes it easier than ever to configure and set up not only PLCs, but HMIs, drives and other associated Siemens equipment. Siemens also offers standard technical support for free.

Schneider Electric

Schneider Electric's main PLC range, Modicon, provides various platforms of all sizes from small brick style controllers through to the M340 and M580 redundant system and numerous legacy systems like Quantum, Premium and Momentum. Schneider Electric PLCs, PACs and dedicated controllers are easy to program, commission, maintain and are IIOT ready.

This range is particularly good in applications where hot redundancy is required as the Ethernet/IP standards have been incorporated, allowing for deterministic distributed I/O.

PLC to PLC communications is very easy with Schneider Electric's Unity software and it is favoured by many engineers for this reason. The local support within Australia is quite extensive with large offices in most major cities.

CONCLUSION

Installing a SCADA network is complex, with numerous considerations to take into account and decisions to make, for critical applications it is imperative to get it right the first time. And with so much to consider around PLC selection, it can get a bit overwhelming. It's important to select an experienced electrical and control systems engineering company such as Automation IT to ensure the networking hardware, software and other components are correctly chosen to ensure any security, environmental and safety risks are minimised and the system remains reliable and secure in the long term.

Automation IT is able to design, configure, implement and commission high-quality, end-to-end networking solutions for a wide range of industries and clients, matching a client's requirements to the right PLC. Automation IT is vendor neutral, so is able to offer solutions that are tailored to best meet the requirements of the project and ensure the end client gets the most out of their network and assets.

Automation IT works closely with authorised Australian distribution channels for all brands and can provide full support for its clients if there are any manufacturing issues with the products within the specified warranty periods. Many of the vendors can also offer the option of extended warranties of up to seven (7) years, this shows the confidence they have in their products.

With qualified engineers on staff, Automation IT's solutions comply with all laws, standards and warranties, giving clients peace of mind that their system will be designed and integrated correctly the first time.

ABOUT AUTOMATION IT

Automation IT is a 100% Australian owned and operated control system engineering company specialising in PLC, SCADA, RTU, automation, control, telemetry, networking, energy management and electric vehicle (EV) charging solutions. The business was incorporated in 2000 and our Head office is located at Springwood in the Brisbane- Gold Coast corridor, we also have offices in Sydney, New South Wales and Perth, Western Australia.

Automation IT employs a team of experienced and professional engineers who have provided industrial hardware and software solutions from the factory floor to the resource planning and management levels of large organisations throughout Australia.

As a systems integration company we specialise in control systems engineering and real-time software development for a diverse range of hardware platforms. With recognised systems integration relationships with most PLC, SCADA, RTU, Telemetry and Network vendors such as Rockwell Automation, Schneider Electric, Siemens, Emerson (formally GE-Fanuc / GE-IP), Omron, Brodersen, 4RF, Hirschmann and Cisco, our trained network and engineering professionals offer custom product solutions across multiple industries including transportation, infrastructure, power & energy, mining, defence, water & waste-water, food & beverage, manufacturing, robotics & motion control and electric vehicle (EV) charging solutions.

As an electrical engineering company, Automation IT provides electrical design services to tightly integrate both the electrical infrastructure and control system and ensure that the entire electrical system functions as one with no gaps or finger pointing between vendors.

Automation IT provides all facets of control system engineering services from project management and conceptual design right the way through to final site commissioning. In addition to this, Automation IT provides a dedicated 24x7 support service.

Automation IT's customer commitment and professional attitude has been recognised with multiple achievements and awards over the years such as, nominations to IE Aust for Engineering Excellence, highest QLD sales and Integration partner of the year. Automation IT employs multiple Registered Professional Engineers of Queensland (RPEQ) along with TUV Rheinland (Machinery) Certified Functional Safety Engineers, this ensures our customers are informed and up to date with the latest trends in automation legislation ensuring our engineering services and solutions offer the best protection for our client's projects.

CONTROL SYSTEMS ENGINEERS
AIT