FROST & SULLIVAN

Integrating Safety and Process Environments

Using a single programmable controller such as Schneider Electric's M580 Safety Controller to manage both process and safety systems can help speed up deployment, improve reliability and sustainability of operations, enhance cybersecurity, and support greater productivity and transparency.

A Frost & Sullivan Whitepaper

Schneider Electric

Contents

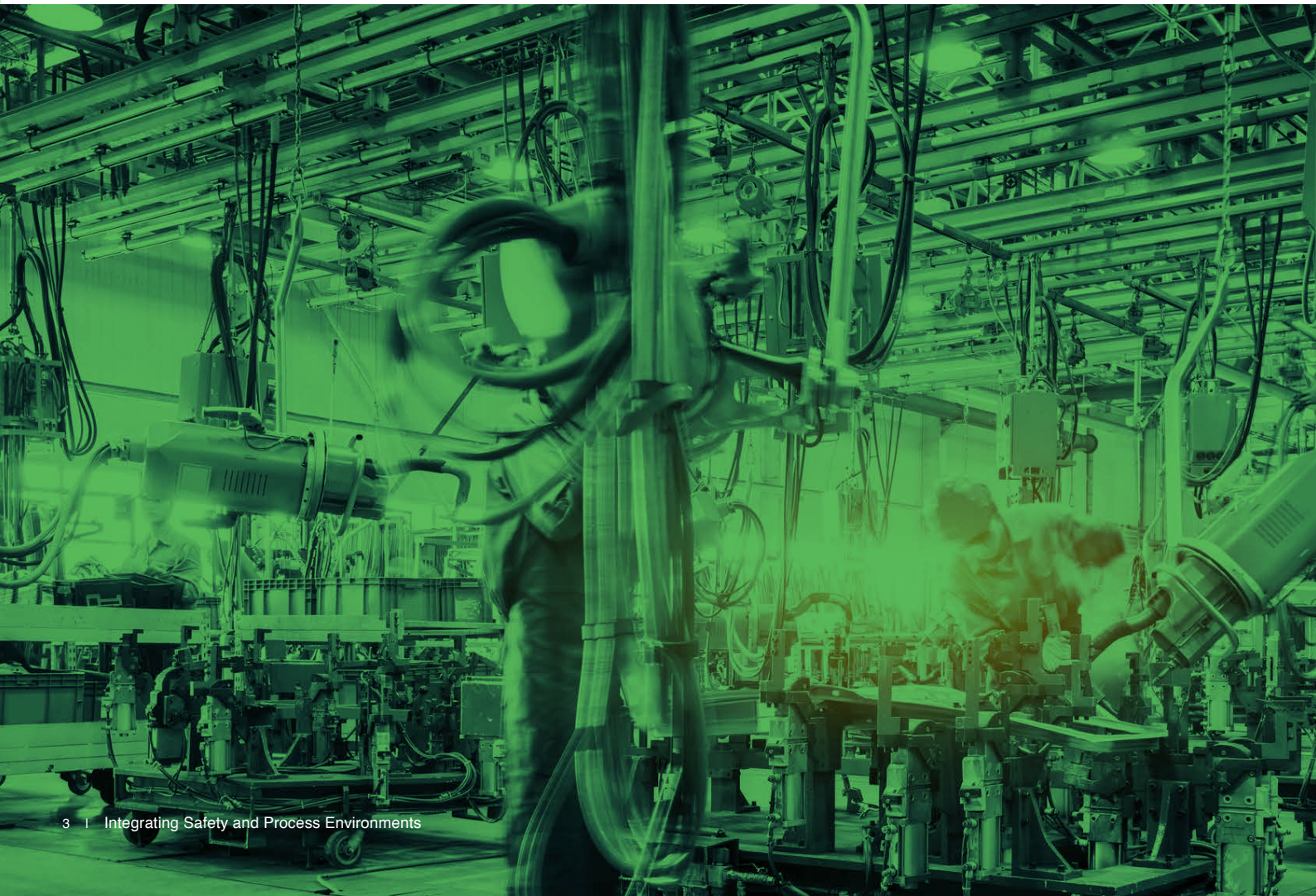
The Paper was completed in March 2018.

Edge Intelligence and Control

Among the key enablers of smart factories and processing environments are edge intelligence and control, i.e., computing that pushes intelligence, data processing, analytics, control, and communication capabilities to where the data originates. It enables latency-sensitive computing, offers improved business agility through better control and faster insights, lowers operating expenses, and results in more efficient network bandwidth support.

Among the many innovations expected to enhance real-time information availability and control in edge devices are those focused on Programmable Logic Controllers (PLCs).[1]

[1]A PLC is a digitally operating electronic system that uses programmable memory for the internal storage of user-oriented instructions to execute specific functions such as logic, sequencing, timing, counting, and arithmetic. In addition, a PLC uses both digital and analogue inputs and outputs (I/O) to control various types of machines or processes.



The Evolution of Programmable Process Control

Fifty years ago, the world of industrial process control embarked on a significant shift from hard-wired relay systems to PLCs, with the launch of Modicon's 084, the world's first PLC.

With PLCs, operators required much less time to train and execute a ladder logic program,[2] providing greater flexibility in configuring new control systems.

Recognising advances in both hardware and software for PLCs over time, the International Electrotechnical Commission (IEC) eventually developed an open international standard, IEC 61131-3, which standardised five PLC programming languages: Ladder Diagram, Function Block Diagram, Structured Text, Instruction List, and Sequential Function Chart.

In addition, PLC form-factors have undergone rapid changes since their introduction. The hardware component of PLCs has evolved from being a simple input/output (I/O) controller to a microprocessor-based unit and then to a more advanced unit, with intelligent I/O modules for machine positioning and control.

Today, PLCs come in many forms such as mini-PLCs, nano-PLCs, and PC-based Programmable Automation Controllers (PACs).[3] PLCs now also offer multiple utilities, such as discrete control functionality, motion control, and Human Machine Interface (HMI).

[2]Schematic, diagram-based programming.

[3]A PAC is a controller that delivers all the functionality of a PLC with the computing power of a PC controller and can have 10 to more than 512 configurable I/O modules.

Global PLC and PAC sales to reach

$13.15 BILLION

by 2021

Frost & Sullivan estimates global sales of PLCs and PACs (comprising PACs, nano, small, medium, and large PLCs, modular I/Os, software and services) to grow from $11.31 billion[4] in 2016 to $13.15 billion by 2021.[5]

In 2016, the largest end-use sectors for PLCs and PACs were food & beverage (19.7% of the total global market), automotive (15.1%), chemicals (13.0%), power (11.9%), pulp & paper (11.4%), oil & gas (8.2%), and water and wastewater (7.4%).[6]

Increased activity across process industries (such as food & beverage, power, and water & wastewater) and discrete industries (such as automotive) in emerging countries such as China, India, Brazil, Indonesia, Thailand, and parts of the Middle East is mainly driving demand for PLCs and PACs. Government initiatives in some of these countries, such as “Make in India” and “China Manufacturing 2025”, underpin investments in a range of process control and automation solutions.

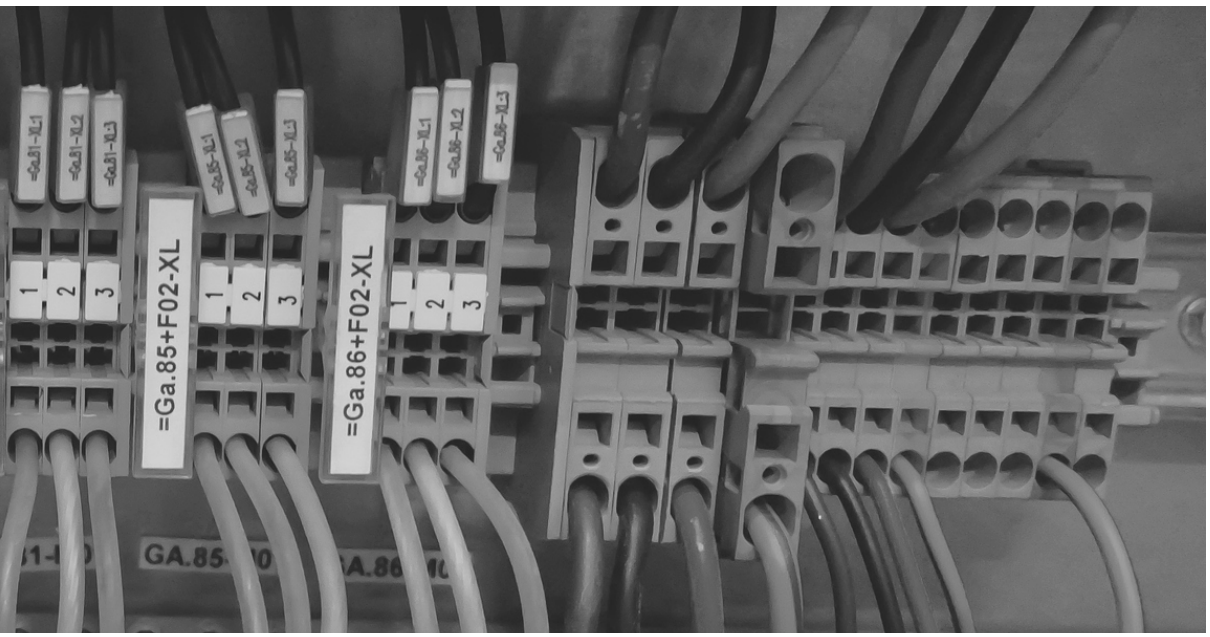
Also, the trend toward regionalisation of the manufacturing sector (and the drive to improve manufacturing productivity) in developed countries such as the US, Canada, UK, the Netherlands, France, Italy, and Japan and nearshoring of the manufacturing sector to developing countries such as Mexico and parts of Eastern Europe is attracting investments for new and advanced controller systems such as PACs.

However, customers continue to face significant challenges in the way they utilise PLCs and PACs.

[4]All currencies refer to USD unless stated otherwise

[5]Global Programmable Logic Controllers Market, Forecast to 2021, Frost & Sullivan, Dec 2017

[6]Ibid; “Others” accounting for 13.3% include life sciences, metals and mining, machinery, cement, semiconductor and electronics, glass, textiles, aerospace and defence, and other niche applications.

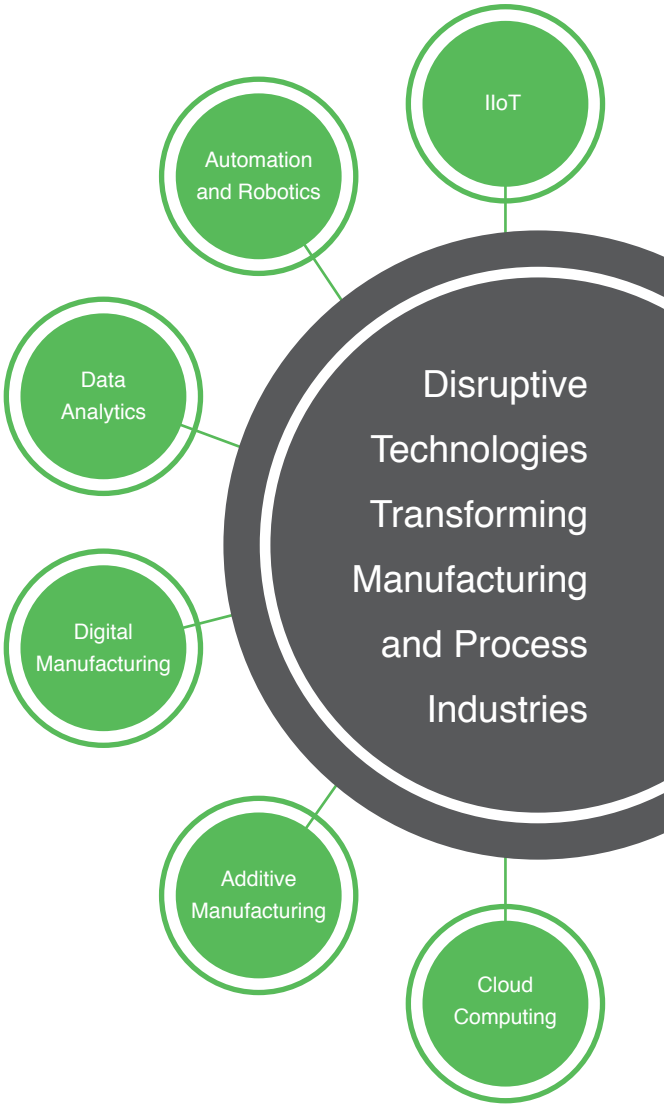


Challenges in Leveraging Programmable Process Control

Some of the critical challenges in realising the full potential of PLCs/PACs are discussed below:

01 Realising the Potential of Disruptive Technologies

A growing number of industrial facilities are exploring the power of the Industrial Internet of Things (IIoT), cloud computing, advanced automation and robotics, data analytics, digital manufacturing, as well as additive manufacturing to optimise their operational performance. In a highly competitive global marketplace, industrial organisations seek "digital intelligence" to manage hundreds of thousands of assets in an enterprise. Being data-driven allows manufacturers and process managers to gain a competitive advantage by analysing information to improve various processes in production, logistics, and supply chain management.



The standardisation of IIoT architecture is set to create a $90 billion opportunity by 2021 for the global IIoT market.[7] This includes the standardisation of terminal devices, communication protocols, and other IIoT application protocols. Mobile applications will be an integral part of IIoT technology in the manufacturing space. Data analytics will utilise mobile phones as a processing platform for geo-distributed analytics. The IIoT software and services market, including connected device platforms and application development platforms, is expected to experience a compound annual growth rate (CAGR) of 30% to 35% from 2016 to 2021.[8]

[7]Industrial Internet of Things (IIoT) and the Future of Manufacturing, Forecast to 2021, Frost & Sullivan, Dec 2017

[8]Ibid

Technological advances in information and communications technology (ICT) continue to deliver enormous processing power in analysing vast volumes of data. The advent of Big Data has enabled enterprises to tap into data for new insights and better decision-making. However, industrial end users have always faced challenges in collecting and analysing data. Three new trends are emerging to overcome these challenges:

Pervasive Sensing

The cost of sensors and sensor interfaces is on a downward trend. This allows end users to track an increasing range of data types and the respective variables.

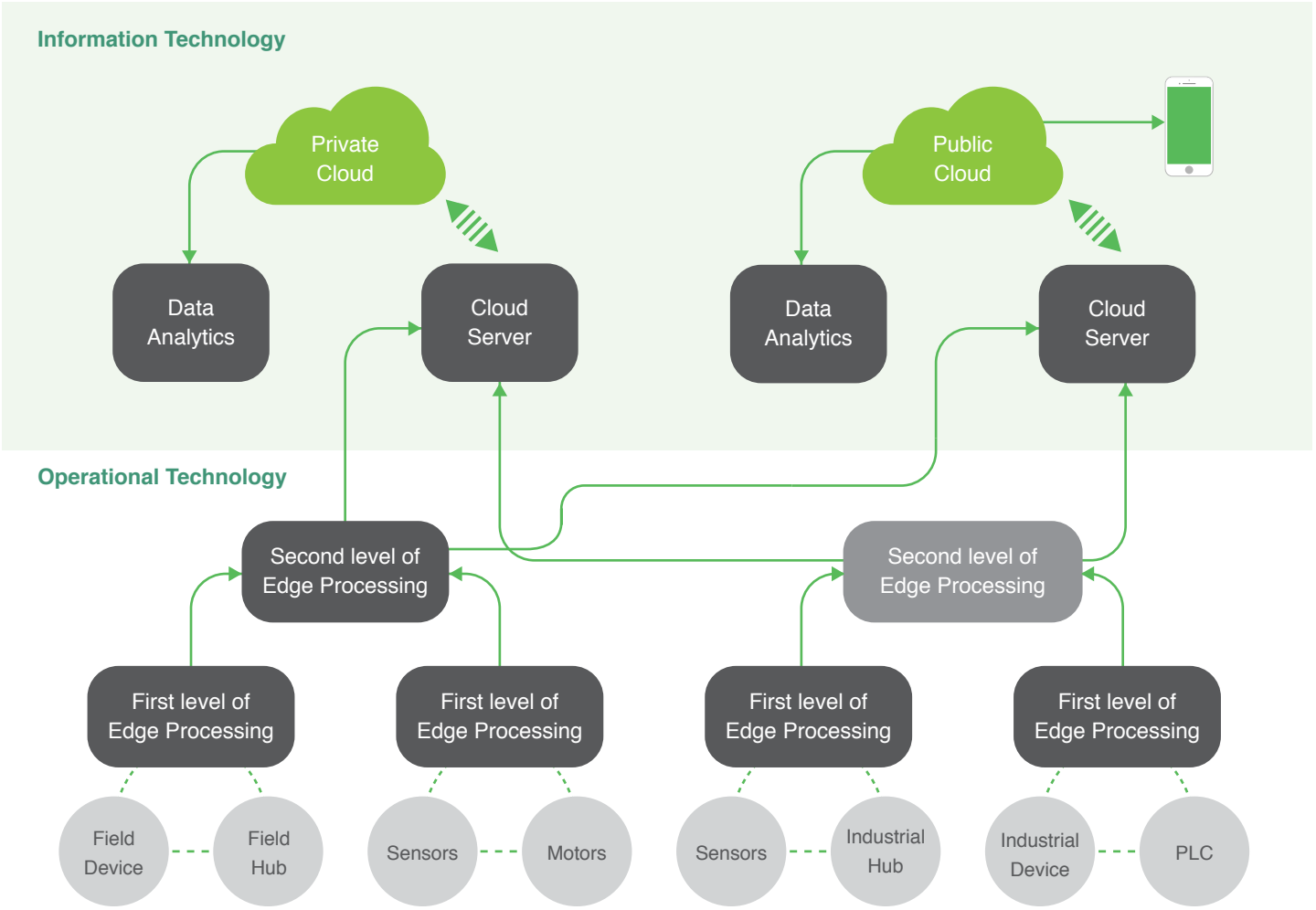
Distributed Control

Technological advances in microprocessor-based controllers are enabling the integration of DCS with PLC. This allows for better control, elimination of bottlenecks, flexibility, and improved throughput.

Seamless Connectivity

M2M communications technology is in the early stage of transforming the connected factory floors. Communication technologies such as Ethernet and Modbus, and cellular networks and wireless technologies such as Bluetooth, ZigBee, Wi-Fi, and LPWAN, bring numerous benefits to industrial end users along with cybersecurity concerns.

IIoT System Architecture



Source: Frost & Sullivan

02 The Integration and Maintenance Challenge

While aging equipment and operator errors remain the major reasons for overall unscheduled downtime in the manufacturing sector, there are specific integration and maintenance challenges that are hampering the effective use of PLCs/PACs.

The operation of multiple PLCs/PACs in a single plant, with multiple owners managing various PLCs/PACs across the site - e.g., engineering, procurement, and construction (EPC) companies, original equipment manufacturers (OEMs), or PLC vendors themselves - results in complex integration of systems and high maintenance costs.

The risks of this scenario include discrepancies in standard operating procedures (SOPs) of the PLC/PAC system. Poor connectivity between assets is another issue end users face, which challenges data capture from proprietary protocols. This, in turn, decreases the quality of visualisation and potentially increases downtime, owing to delayed service leads.

03 The Safety Challenge

The megatrend of “innovating to zero” is prompting manufacturers and process operators to work towards a “zero concept” operational environment – with zero emissions, zero accidents, zero fatalities, zero defects, and zero breaches of security. The central role of safety in achieving these goals is because safety risks in process environments can lead to unavailability of production systems resulting in production outages and service-level agreement penalties.

It could also lead to the loss of integrity of control systems resulting in injuries/fatalities and delayed/compromised production. Finally, it could result in the loss of intellectual property (IP), reducing competitiveness.

All of these risks can have significant ramifications in the form of a reduced market share, as well as negative impacts on stock price.

04 The Cybersecurity Challenge

The vulnerability of industrial environments is aggravated by the increased number of connected devices in operation, greater use of cloud computing solutions, as well as the higher sophistication of cybercriminals, for whom industrial facilities are becoming a growing target for cyber attacks.

Manufacturers and process operators of all sizes are increasingly expected to demonstrate that they have in place state-of-the-art technologies and internal processes needed to protect their plants, intellectual property, supply chains and customers from cybersecurity vulnerabilities. Much of the push for security audits and documentation will come from industrial customers. However, regulators also require that manufacturers and process operators prove that they have mitigated the kinds of security threats that could have profound financial impacts.

With the introduction of IIoT, the traditional walls between information technology (IT) and the operational technology (OT) worlds are fast disappearing. As a result of this convergence of technologies, the gap between industrial safety and information security that currently exists in industrial processes is also becoming narrower.

Connectivity gives manufacturers the power to improve manufacturing operations, but there is still a considerable gap in understanding the implications of IT-OT convergence in the manufacturing sector. This ongoing change in the manufacturing landscape is likely to make security needs much more complex in the factories of the future. Currently, a number of regions across the globe do not possess a strong cybersecurity infrastructure, making their industrial facilities particularly vulnerable to cyber attacks.

According to the 2017 SANS Institute survey of Industrial Control Systems (ICS) security practitioners, the top overall threat vector of concern was for devices and “things” that cannot protect themselves. Embedded controllers or components (such as PLCs or Intelligent Electronic Devices (IEDs)) were considered the third most significant control system components in terms of impact if compromised or exploited.[9]

05 The Engineering Cost Challenge

The imperative to maximise profitability is prompting greater scrutiny of engineering costs in all automation projects. However, operator requirements in relation to documentation, safety, functionality, and flexibility result in engineering costs equating to approximately half of total automation project costs (the other half being hardware and software).[10]

[9]Securing Industrial Control Systems-2017, Bengt Gregory-Brown, SANS Institute, June 2017

[10]Frost & Sullivan estimate

The Concept of Common Safety

Common safety ensures that both process and safety operations are separate and independent in a common engineering environment.

The assumption that industrial assets are safe if air-gapped and disconnected is no longer defensible. This is why common safety – an approach that ensures that both process and safety operations are separate and independent in a common engineering environment – is seeing increased traction.

Firstly, with growing advancements in manufacturing/processing technology and connectivity, it has become practically impossible for manufacturers/process operators to completely stay disconnected or isolate a part of the manufacturing/process plant. Therefore, complete automation solutions are now expected to offer both safety and non-safety control systems.

Secondly, integration of safety and non-safety controls reduces the overall cost of engineering. Finally, modifying standalone safety systems following commissioning, has always been viewed as an overly complicated process that end-users could not undertake themselves.

Approaches to Safety System Configuration in Plants

BPCS: Basic Process Control System;
SIS: Safety Instrumented System

Source: Schneider Electric

A common safety approach eliminates the need for complicated custom interfaces by systems integrators. It delivers the benefits of flexibility, ease-of-use, and reduced cost of engineering without compromising the independence of either the process safety system or the safety system.

Schneider Electric's M580 Safety Controller

[11]Schneider Electric's Unity software package provides access to a range of program libraries which can be assembled to combine PLC, DCS and SCADA functions with energy management in a single integrated platform.

[12]Schneider Electric

Using the common safety approach described above, Schneider Electric has now launched the **M580 Safety Controller**, providing the same high performance of the M580 Ethernet-enabled programmable automation controller (e-PAC), but with plant safety functions integrated through dual redundant processor architecture. The safety functions are password protected and have different memories and microprocessors.

This solution delivers a range of benefits to end-users, including:

Rapid deployment:

The M580 Safety is a member of the Unity family – the one programming package from Schneider Electric for all PLCs. The access which Unity provides to Schneider Electric's Modicon Libraries can help users drive standardisation and enjoy the benefits of reduced start up and commissioning. Feedback from ongoing projects suggests that when implemented as part of Schneider Electric's EcoStruxure Architecture., the M580 Safety Controller can support customers with up to 25% less deployment time required than with other systems.[12]

For our first application of the M580 Safety Controller - in gas burner oven safety management - we found the all-in-one PLC easy to assemble and install, with no physical interface needing to be wired (IO or network) between process and safety parts. Also, being only one engineering tool, the M580 Safety Controller gives us the benefit of the same ergonomics, programming language and methods for debugging and commissioning.

- EUROPRODUCTIQUE
(Systems Integrator)

Improved reliability and sustainability

Certified SIL 3 for functional safety,[13] the M580 Safety Controller's enhanced diagnostics, redundant-managed power supplies, dynamic memory error correction, and common spare parts enable minimisation of downtime and the optimisation of process energy. The controller's mobile device compatibility also helps operators optimise performance in real time. In addition, the M580 Safety Controller offers the same high-performance benefits and leverages the same tools of the M580 e-PAC including being designed for operating in harsh environments (in terms of temperature, corrosion, vibration).

Enhanced cybersecurity

The M580 Safety Controller has Achilles Level 2 Certification for cybersecurity.[14] This, along with the dual-core microprocessors (which ensure process and safety are separated as functions), reassures customers of best-in-class protection for plant assets and people.

Higher productivity:

The M580 Safety Controller helps deliver productivity enhancements through increased processor performance for quicker PLC scan times, time stamping that saves implementation time, memory to support local data logging (enabling safety system performance to be monitored for continuous improvement), one common engineering platform and I/O platform for simpler training and spare part management (including safety I/O), as well as faster migration with native integration of legacy systems inside M580 architecture.

Greater transparency

With the Ethernet communications backbone, 1Gbps redundancy communication link and the use of ODVA-compliant[15] protocols to provide open network implementation, the M580 Safety Controller enables operators to achieve production outcomes safely in an increasingly IIoT-enabled environment. The mobile device compatible system also ensures that transparency and control are possible irrespective of location of the industrial workforce.

Ideal Use Cases

The M580 Safety Controller has hot-standby[16] available. It is best deployed where IIoT-ready systems are expected to enjoy high traction in use cases such as material handling, conveyor control, burner management, fire detection, gas/dust detection, as well as a range of other machine safety uses in the food & beverage, water & wastewater and mining, metals and mineral sectors.

With the M580 Safety Controller, all are integrated in ONE product. There is no need to have an additional PLC to implement the safety part of the process. With ONE interface as Unity, the programing is well structured with the safety part and the process part.

- PACECO
(Container Handling
Equipment and Systems)

[13]IEC 61508 standard for functional safety defines four safety integrity levels (SIL) i.e., SIL 1 to 4; 1 being the least dependable.

[14]An industry-leading certification for cybersecurity, Achilles Level 2 Certification (from GE Digital Cyber Security) has stricter requirements than its precursor, Level 1.

[15]Open DeviceNet Vendor Association Inc

[16]A method of redundancy in which the primary and secondary (i.e., backup) systems run simultaneously.

Conclusion

As the business environment remains cyclical due to economic uncertainty and dampened investment flows, manufacturers and process operators are under pressure to retain their profit margins by reducing production costs.

Due to the constant fluctuations in raw material, labour, and energy costs, manufacturers and process operators are shifting their investment focus to adopting advanced automation solutions that help in enhancing plant productivity, operations, and maintenance. However, it is not only about the process. A safer work environment, as more businesses are beginning to realise, can reduce employee turnover and costs, increasing productivity and overall customer retention.

Fortunately, connectivity and IIoT are redrawing not only ways of doing business and consumption of products and services, but also production/process optimisation and protection strategies. This is pushing the boundaries of traditional automation systems, encouraging both automation vendors as well as end users to rethink their traditional approaches. As the focus moves from corporate-facing business dashboards to more widespread plant floor analytics, the priority is increasingly to empower frontline personnel with insights.

In this context, Schneider Electric's M580 Safety Controller, with its open, integrated, safe, IIoT-fit edge intelligence and control, could help to maximise return on assets (ROA) across a range of industries, without compromising safety for both people and plant. By leveraging the legacy of the Modicon family of PLCs and PACs, this solution is expected to allow manufacturers and process operators to drive profitability, improve sustainability, and raise operational excellence in a safe and secure manner.


R+
UDC-
U2
V2
W2

We Accelerate Growth

WWW.FROST.COM

Auckland	Colombo	London	Paris	Singapore
Bahrain	Detroit	Manhattan	Pune	Sophia Antipolis
Bangkok	Dubai	Mexico City	Rockville Centre	Sydney
Beijing	Frankfurt	Miami	San Antonio	Taipei
Bengaluru	Iskandar, Johor Bahru	Milan	Sao Paulo	Tel Aviv
Bogota	Istanbul	Mumbai	Seoul	Tokyo
Buenos Aires	Jakarta	Moscow	Shanghai	Toronto
Cape Town	Kolkata	New Delhi	Shenzhen	Warsaw
Chennai	Kuala Lumpur	Oxford	Silicon Valley	Washington D.C.

ABOUT SCHNEIDER ELECTRIC

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries. With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software. In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency. We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

ABOUT FROST & SULLIVAN

Frost & Sullivan is a growth partnership company focused on helping our clients achieve transformational growth as they are impacted by an economic environment dominated by accelerating change, driven by disruptive technologies, mega trends, and new business models. The research practice conducts monitoring and analyzing technical, economic, mega trends, competitive, customer, best practices and emerging markets research into one system which supports the entire "growth cycle", which enables clients to have a complete picture of their industry, as well as how all other industries are impacted by these factors.

Contact us: Start the discussion

To join our Growth Partnership, please visit www.frost.com