ARC WHITE PAPER

By ARC Advisory Group

PROFIsafe: Networked Safety for Process and Factory Automation

ARC
Advisory Group

THOUGHT LEADERS FOR MANUFACTURING & SUPPLY CHAIN
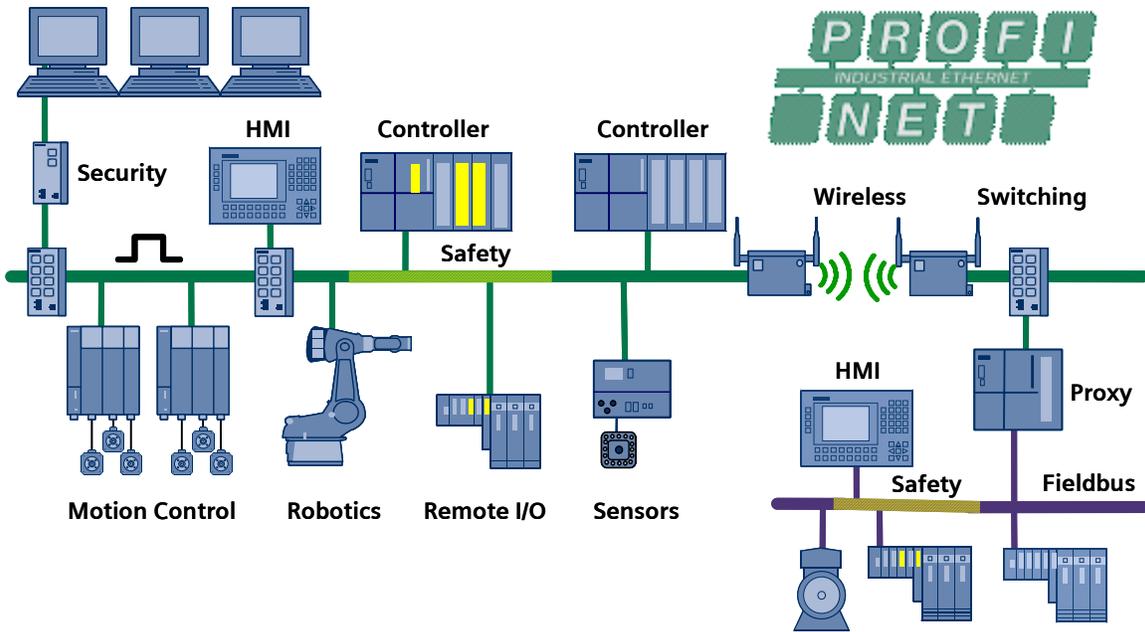
**Profinet Networks the Whole Plant, From Automation Devices
to Enterprise, With Support For Motion Control, Networked Safety
And Wireless Connectivity**
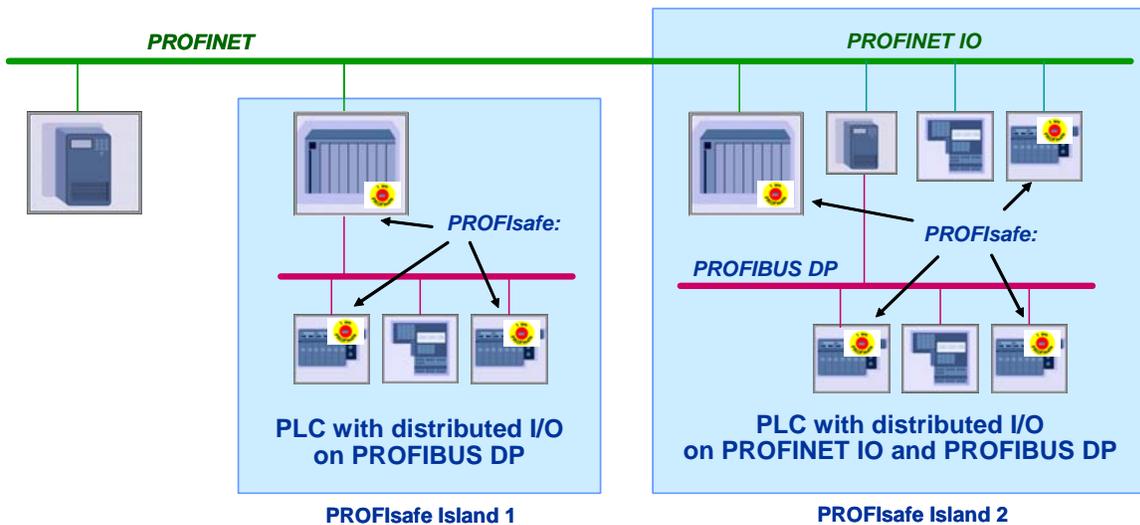
**PROFIsafe Allows Seamless Communication of Safety Data
Independent of Network Media**

Executive Overview

Industrial automation has profited tremendously from technology advances in recent years. Industrial Ethernet, distributed intelligence, "smart" safety, and wireless networking are just a few of the enabling technologies that have brought tangible value to end-users. But manufacturers are tradi-

> Safety has evolved from being a cost burden and "necessary evil" to a strategy for improving productivity and reducing downtime.

tionally arch-conservative decision-makers and don't accept new a technology until it is well proven, or until investments in these technologies can be corroborated with solid business arguments. Faced with a landscape of both fact and hype, manufacturers are learning how to match technology benefits to specific business metrics.

Two topics in particular – industrial Ethernet and safety - have caught the attention of manufacturers in recent years thanks to their potential to cut costs and improve business performance. Industrial Ethernet has unified network architectures and created a high level of data transparency from which applications such as Asset Management or Manufacturing Execution Systems profit tremendously. Safety has evolved from being a cost burden and "necessary evil" to a strategy for improving productivity and reducing downtime.

Profibus International, an industrial consortium of automation suppliers, has mated safety with industrial networking to create solutions for "networked safety" based on all available media, including Profibus DP and PA, Profinet (industrial Ethernet) and wireless. End-users are now taking advantage of these solutions to unify their network architectures and eliminate the need for a second, parallel bus while maintaining conformity with safety standards up to SIL3. Benefits of networked safety include shortened start-up times, lower wiring costs and, in the long-term, faster and more efficient maintenance.

Business Drivers in Safety and Industrial Networking

This was the case with industrial Ethernet, which took decades before it finally found its place - albeit in an industrialized form - in the factory. As appealing as some new technologies may be, manufacturers make decisions

based primarily on sound business rather than technical arguments. These arguments can be measured by applying standard business metrics ranging from expected productivity increases or reductions in Total Cost of Ownership (TCO) to more difficult to measure "soft facts" such as increases in manufacturing flexibility and agility. Other important metrics include as Return on Assets (ROA) and Overall Equipment Efficiency (OEE), both of which are critical contributors to the overall goal of achieving Operational Excellence (OpX).

**Total Machine Safety Business
(Millions of US Dollars)
Source: ARC Advisory Group**

Time to Market (TTM) is playing an increasingly important role in business metrics. However, it is difficult to define which particular factors have a direct influence on the time it takes to get a product from idea to marketplace. Shortening TTM means maximizing the use of the information surrounding a product throughout its design and production lifecycles. TTM excellence depends on concurrent execution of not only engineering but all development activities surrounding a new product. In the factory, industrial Ethernet has become a significant contributor to this strategy by dramatically increasing information visibility in support of information-rich applications ranging from Manufacturing Execution Systems (MES) to Product Lifecycle Management solutions (PLM).
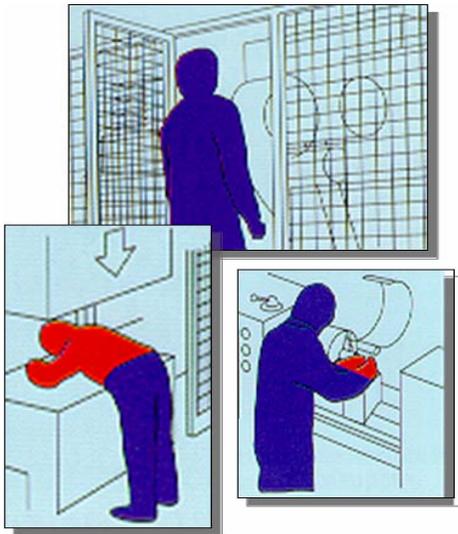
The Business Case for Safety

Machine safety in the traditional sense refers to add-on components that protect personnel working in or near industrial machinery from injury or death. However, modern safety solutions go far beyond this notion. Many end users now recognize that the deployment of intelligent, integrated safety solutions can directly affect their bottom line.

Manufacturers today are under pressure to contribute value to a company's bottom line by continuously improving the performance of manufacturing assets. The nemesis of all manufacturers is unscheduled downtime – unexpected machine stoppage resulting from equipment failure, operator error or nuisance trips. Safety solutions available today integrate directly into standard control architectures, helping to curtail downtime by allowing operators to diagnose machine stoppages more intelligently – especially nuisance trips – and quickly get production up and running again.
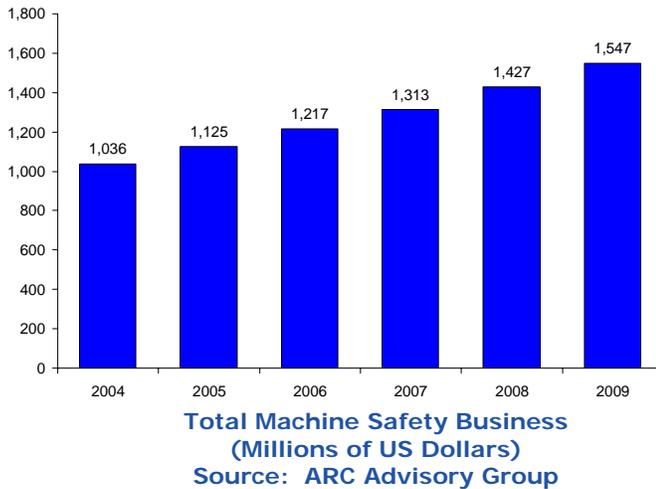
The topic of safety has caught the attention of manufacturers in recent years thanks to the potential of safety systems to improve business performance. In addition to ensuring worker safety, manufacturers and machine OEMs are learning how an intelligent safety strategy can become a competitive advantage rather than a cost burden. Several factors are driving this increased awareness, including:

Safety Is All About Personnel Protection, But An Intelligent Safety Solution Also Reduces Downtime And Increases Productivity.

- A desire by manufacturers to limit liability exposure and to improve their public image

- The view that integrated safety systems can help improve the bottom line by reducing downtime and increasing Overall Equipment Efficiency (OEE) and Return on Assets (ROA)

- Harmonization of international safety standards is allowing machine OEMs to develop and deploy globally acceptable safety solutions.

Machine Safety as Risk Management

Machine safety is a form of risk management at the automation level. A safety strategy starts with the identification of potential hazards, followed by a categorization of the hazards according to their severity. Guided by requirements spelled out in the body of international safety standards, steps are then taken to either prevent faults that can cause these hazards, or at least to significantly reduce the likelihood that these faults can occur.

The Costs and Risks of Not Ensuring Machine Safety

Many companies have seen their public image suffer in recent years due to negative press from product recalls and boardroom scandals, resulting in a loss of trust in the public eye. These experiences have taught companies the importance of actively improving their "good neighbor" image by actively promoting their adherence to good manufacturing practices and compliance with environmental and occupational safety best practices. Also, in an increasing socially conscious world, the importance of not just protecting humans from injury or death, but also of providing workers with a safe and healthy work environment has advanced to the forefront.

Besides image challenges, manufacturers are moving to limit their exposure to liability in situations within their control, such as product liability, personal injury or environmental damage. In other situations where regulations may be unclear or not yet harmonized, the risk exposure of not complying even with non-compulsory practices is still high, and companies can at least demonstrate their "best faith" by documenting compliance with all generally accepted industry practices. Such tactics can also be applied to safety strategies, especially for machine builders faced with differing safety regulations in foreign markets. While harmonization of standards is lessening the workload, the burden of proof of compliance still lies with both the OEM and the end user.
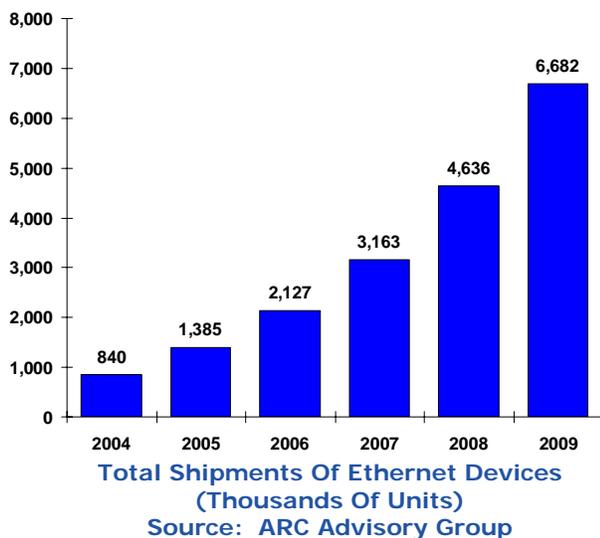
Safety Standards Evolution and Harmonization Spur Safety Product Development

Globalization has had a decidedly positive effective on developments in safety technology. The recent harmonization of safety laws and international norms has simplified the jungle of regulations that a machine OEM has to understand and comply with. For suppliers of safety components and systems, harmonization has resulted in a consolidation of product requirements, created more homogeneous product markets and paved the way to new product innovation. A good example of this is the advances made in safe motion technology that would not have been possible without an overhaul and modernization of existing regulations.

However, regulations can vary by country and machine builders still bear the responsibility for ensuring compliance. These regulations and norms include machinery and low voltage directives, EMC compatibility, as well as a slew of IEC norms starting led by IEC 61508, the basis for safety standardization. Other relevant standards include IEC 62061, IEC 60204 and ISO 13849 (previously EN 954) for machine safety or IEC 61511 for process safety, and extending to other specific standards, some of which are still currently under development or in draft form. Continuing harmonization activities with the these standards, the US has also begun updating various industry safeguarding standards such as NFPA 79 for

Total Shipments Of Ethernet Devices (Thousands Of Units)
Source: ARC Advisory Group

| Year	Units
2004	840
2005	1,385
2006	2,127
2007	3,163
2008	4,636
2009	6,682

industrial machinery, the ANSI B11 series for machine tools, S2 for the semiconductor industry, and RIA 15.06 for robots, just to name a few. The result is a globalized effort to develop improved harmonized standards for both the design and the application of this new wave of safety technology. As a part of this harmonization effort, the US standards typically reference international and European norms.

In Asia, many countries such as Japan publish equivalency charts that associate local standards with internationally recognized standards (ISO and IEC), making it somewhat easier for OEMs to declare compliance by association. This means that OEMs no longer need to offer multiple country-specific safety designs and can streamline their portfolios by standardizing on a single, internationally accepted solution.

PI International Provides Platform for Universal Plant Communication

PI International (Profibus and Profinet), with a global community of more than 1200 member companies, is the industrial consortium responsible for
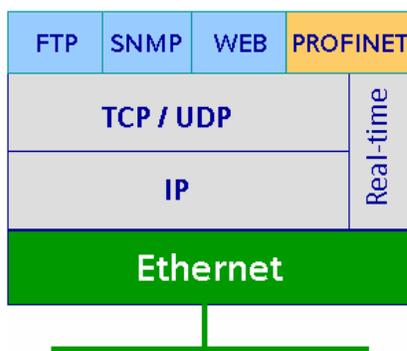
Profinet Supports Simultaneous Real-Time And TCP/IP Communication.

developing and marketing industrial networking technology. Since the first days of Profibus in the early 1990s, PI's member companies have continuously developed and expanded the technology to meet the particular needs of automation users, ranging from carmakers to petroleum refiners. This includes network media to handle a variety of tasks, including Profibus DP (IEC 61158) for typical 2-wire applications in factory automation, and Profibus PA, which offers intrinsic safety according to IEC 61784-3 for process-type applications. Profinet is PI's solution for Ethernet-based industrial networking and includes provisions for wireless communication.

Profinet allows customers to implement an integrated automation solution based around a single Ethernet network with support for different control disciplines such as peer to-peer communication, remote I/O, machine safety, motion control and data acquisition. Profinet also eliminates the complex task of programming controller to controller messages by allowing the programmer to design communication paths graphically.

End-users can greatly benefit from PI's 15 years of experience in developing industrial networking technology. Application profiles developed for Profibus such as PROFIdrive and PROFIsafe, for example, are also available for and fully compatible with Profinet. This allows end-users to reuse existing automation solutions while reaping the benefits of the newest technology.

Automation and Safety Systems are Fusing

In most automobile plants today it is still common to find dual-PLC, dual-network control architectures. "Dual" refers to one solution for standard logic control and a separate, parallel solution for control of safety-related devices such as light curtains, l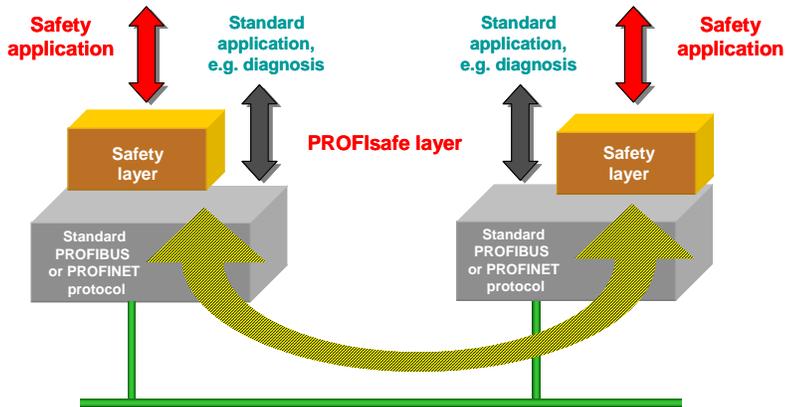aser scanners and E-stop switches. This situation, which applies to both PLCs and device networks, arose out of the desire of manufacturers to keep safety circuits separate and independent of standard control tasks. As the reliability of electronics improved and monitoring relays evolved into safety PLCs, safety still remained the domain of small, specialized suppliers such as Pilz or HIMA. The same was true of industrial networks whose protocols - with the exception of dedicated safety networks like SafetyBus p – were not designed with the right checks and balances to satisfy the requirements of safety standards.

> Running separate busses for safety and non-safety data is simply no longer commensurate with modern automation philosophy.

In the meantime, the dual-PLC strategy has given way to modern solutions that combine both standard and safety functionality in a single controller. While this lowers hardware costs, the greater benefit lies in the single programming environment that eliminates the need for multiple engineering tools and additional training, ultimately resulting in lower Total Cost of Ownership (TCO).

Safety on the Wire:
PROFIsafe Enables Single-Bus Solutions

On the industrial networking side, a parallel development to this consolidation has taken place as well. Thanks to developments in safety technology, running two separate busses for safety and non-safety data is simply no longer commensurate with modern automation philosophy. A two-bus architecture requires double the amount of training, twice the network access hardware and makes start-up and troubling shooting tasks unnecessarily complex.

Safety application — **Standard application, e.g. diagnosis** — **PROFIsafe layer** — **Standard application, e.g. diagnosis** — **Safety application**

Safety layer — **Safety layer**

Standard PROFIBUS or PROFINET protocol — **Standard PROFIBUS or PROFINET protocol**

PROFIsafe Checks Data Integrity of Failsafe Devices Alongside Standard Profibus or Profinet Communication.

Standard und safety data are transmitted on one single cable
Standard and safety modules can be mixed in one I/O device
Safety logic can be programmed using standard engineering tools
Supported by both Profibus and Profinet

PROFIsafe's Strengths

Thanks to the introduction of PROFIsafe, the safety protocol that is part of the communication protocols of both Profibus and Profinet, end-users can now eliminate the need for a separate safety network and reduce their industrial network architectures to a single bus. PROFIsafe extends the standard Profibus communications protocol to address special requirements for safety-related information necessary to conform to strict safety standards. For example, PROFIsafe adds elements such as message numbering and data consistency checks to rule out typical network messaging faults, enabling networked safety devices to meet the reliability requirements of Safety Integrated Levels (to SIL3) prescribed by international safety standards. Since PROFIsafe is built into the communications protocol, it can used by devices connected to any PI network: Profibus DP and PA or Profinet, as well as Profinet over wireless.
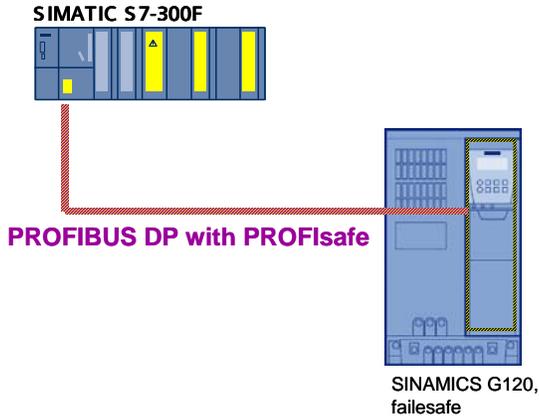
PROFIsafe works with safety devices on Profinet in the same way as with Profibus. Since it is part of the communications protocol, transmission of safety data occurs automatically and seamlessly, even between different network media.

Safety on Board in Motion Control and Standard Drives

As machinery employs more automated subsystems for material handling or automated changeover, the trend in the market is towards safety solutions that allow operators to work more efficiently within the work envelope of the machine. Safety standards now allow the integration of configurable safety systems directly in motion control systems and standard drives. This embedded functionality in the drives makes it possible for machine builders to incorporate safety strategies that improve the operator productivity. With safe drives, safety solutions are becoming less complex, with far fewer cables and connections, resulting in reduced design, commissioning and installation costs. Safe Drive functionality has two fundamental modes of operation: Safe stopping with various stop re-

SIMATIC S7-300F

PROFIBUS DP with PROFIsafe

SINAMICS G120, failsafe

Safe Drives Can Be Integrated Via PROFIsafe Into Control Systems Just Like Any Safety Device.

sponses in accordance with EN60204-1 and safe monitoring of speed and position.

Operational benefits of Drive-Integrated Safety

The ability to incorporate slow speed modes and higher speed response in the safety zone effectively obsoletes the use of multiple lock-out-tag-out requirements in powered machinery and work cells. While the external safety solution and the drive-integrated safety implementation have the same end result, the real difference is in performance. This is where drive based safety has a distinct advantage.

Critical to safety systems is the response time betweens pushbuttons or sensors and actuator. Realizing the safe motion functionality in the motion controller or Safety PLC is an option, but this solution has inherent performance disadvantages. The underlying issue is the time delay between the safety PLC or motion controller and feedback devices. A drive-based

Stop Category 0	Uncontrolled stop. Immediately remove power to drives.
Stop Category 1	Controlled stop; Power is removed after the machine has come to a standstill.
Stop Category 2	Controlled stop; Power is still fed to the machine at standstill.

Stop Categories According to EN 60204-1

solution, on the other hand, has access to all the required signals, but benefits from the faster update time of the controller cycle time. From a performance perspective, an external solution forces the machine designer to incorporate greater margins of safety that reduce the operator's ability to work within the machine envelope.

Just like any safety device, safe drives can be integrated into any system architecture using Profibus or Profinet with PROFIsafe.

Extending Networked Safety to the Process Industries

A large portion of the classic process industries actually contain many applications typically associated with discrete or factory automation. Chemical plants or wastewater treatment plants, for example, often employ motor control centers or discrete I/O modules together with process instrumentation. The higher the discrete application content, the more the industry is classified as "hybrid" rather than pure process or discrete.

Profibus PA offers communication to field instruments in process applications that require a different network medium, for example, for use in explosive environments. Since Profibus PA uses the same communications protocol as Profibus DP, devices on both networks can communicate safety data via Profisafe seamlessly without having to worry about bridges or gateways.

In the process industries, PROFIsafe plays an important role in supporting highly available, redundant systems using Flexible Modular Redundancy (FMR). Using a fieldbus allows a system to tolerate multiple faults without interruption and provides for I/O redundancy independent of CPU redundancy. FMR architectures with PROFIsafe are certifiable up to SIL3 according to IEC 61508.
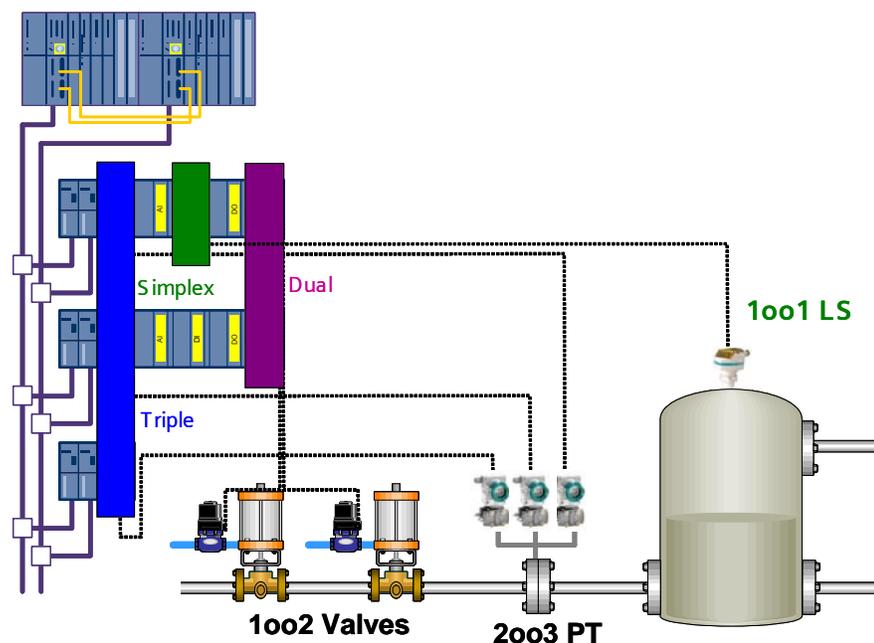
FMR Architectures Tolerate Multiple Faults Without Interruption And Allow Independent I/O Redundancy.

Industrial Ethernet will soon play as important a role in the process industries as currently in the discrete industries. Process production systems have long lifecycles, so the acceptance of new solutions and technologies simply takes longer than in factory automation. To meet this challenge, Profibus International is preparing now to support the future needs of process users. Process instrumentation suppliers have built up and refined their portfolios of Profibus PA-compatible products over many years, so it is unlikely that any will switch support to Profinet overnight! More likely,

field instruments that require intrinsic safety or bus power will be integrated into backbone Profinet networks via links. The advantage for end-users is that valuable field data will flow directly into a real-time, high bandwidth network that makes these data available to a variety of information consuming applications ranging from MES to asset management.

For networked safety in process instrumentation, efforts are already underway at Siemens to add support for PROFIsafe to existing products. The company plans to offer PROFIsafe compatibility by the end of 2006 to Pointek CLS 200 und 300 capacitance level switches and SITRANS P DSIII pressure transmitters. Support for SITRANS T3K temperature transmitters should follow in the spring of 2007.

AIDA Backs Profinet With Integrated Safety

At the end of 2004, a consortium of Germany's top carmakers including Audi, BMW, Daimler-Chrysler (for the Mercedes Car Group) and Volkswagen, announced a conditional commitment to standardize on Profinet as their preferred industrial networking solution in the future. The condition was the availability of integrated safety, which has now been met with the availability of PROFIsafe for Profinet.

The consortium, known by the German acronym AIDA (Automation Initiative of German Automobile Manufacturers), is supported by the Vice Presidents of production of each of the four carmakers. Consortium members point to the increasing cost pressures facing carmakers in Germany and see the potential in meeting these challenges by reducing engineering, start-up and operational costs through the use of open communications standards.

 AIDA was founded with the goal of eliminating the coexistence of multiple, dissimilar industrial networks in factories after hard lessons learned during the fieldbus wars of the 1990s. The consortium recognizes that the full value proposition of industrial networks is not being achieved by the current situation of multiple hierarchies, master/slave architectures and low bandwidth networks. The use of multiple solutions leads to compatibility problems that result in higher integration, training and operational costs, which ultimately adversely affect a manufacturer's bottom line. Moreover, product innovation is held back because too many resources are needlessly expended on developing support for and maintaining compatibility with multiple networks.

AIDA further recognizes that the time is ripe for a technological paradigm shift – the chance to migrate to a proven, ubiquitous medium that is flexible enough to support the various legacy communications protocols and "tweakable" enough to adapt to some specific application needs. Industrial Ethernet has turned out to be the only medium on which every automation supplier can agree.

According to the commitment, Profinet will be preferred over other conventional and Ethernet-based industrial networks at both the controller and the device levels, wherever the use of the network makes business and technical sense. In return, AIDA members expect to enjoy benefits including reduced engineering costs in the design and operational phases of production equipment (training and maintenance), lower hardware costs due to increased competition, a greater variety of available products, and more requirements-oriented development of new products.

Networked Safety in Practice: Two Case Studies

The following section looks at applications of networked safety at two end-users who have realized benefits from using Profinet and PROFIsafe in a variety of industrial applications.

CAMotion Pioneers Safety Over Wireless in a Gantry Robot

Gantry robots are used in a wide variety of materials handling applications in many industries. Unlike simple "commodity" machines, gantries often employ a high degree of sophistication by combining vision, sensors and highly dynamic motion control to meet demanding performance requirements. The competition is keen for sophisticated machines that end-users perceive as giving them a competitive advantage.

CAMotion, Inc., a Robotic OEM and integrator based in Atlanta in the USA, recently developed a vision-guided overhead gantry robot for a Fortune 500 manufacturer. The system is equipped with a host of sensors to identify the shape, size and type of parts to be moved as well as to verify starting and destination locations. The automation solution includes patented motion

control software that dampens oscillations caused by the movement of the gantry over Zimmerman rails.
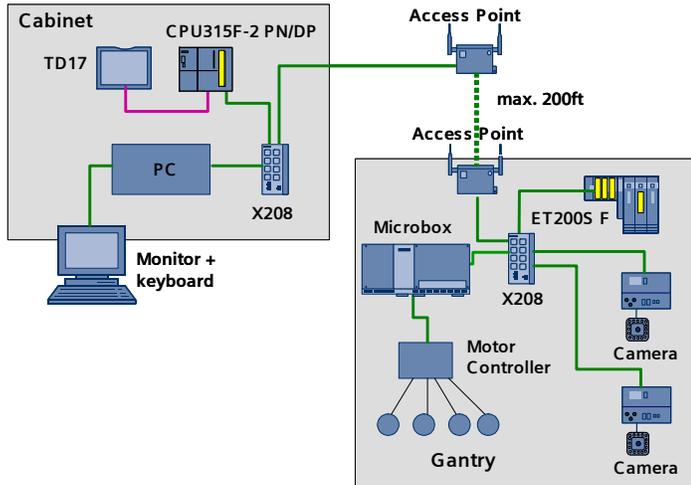

CAMotion User Profinet Over Wireless To Transmit Both Safety-Related and Normal Control Data Between The Overhead Gantry And The Main Control Cabinet.

As with any machine with moving parts, the gantry is also outfitted with safety devices ranging from light curtains to laser scanners to protect personnel working on or near the machine. In addition, CAMotion was interested in using a wireless solution to cut down on cabling costs and to eliminate the physically complex cable festooning solutions that are commonly used. While "normal" automation components could have tackled this job, the company sought a forward-looking solution that would take advantage of recent developments in both networking and safety technology.

According to CAMotion's engineers, the only solution available on the market that offered both wireless connectivity and distributed safety was a combination of a Siemens failsafe PLC networked to safety devices via Profinet using the PROFIsafe protocol. The Siemens S7-315F controller eliminated the need for a separate safety PLC or safety monitor by combining normal and safety functionality in a single CPU. That alone reduced the upfront hardware costs of the machine, but will also likely lower lifecycle costs for the end-user by simplifying maintenance in the long run and shortening downtime.

The availability of products to transmit Profinet wirelessly fulfilled CAMotion's desire to reduce cabling costs by as much as 30 percent as well as to shorten installation time and simplify start-up. The benefit of using a single bus was the fact that both normal and safety devices could be combined on just one network. Safety devices supporting PROFIsafe were readily avail-

able from Sick, Siemens, Banner and others. For remote I/O, CAMotion used ET200S modules from Siemens.

CAMotion's system architecture now uses Profinet between all devices, regardless of whether they transmit safety-related or normal data. To bridge the gap between the PLC in the stationary cabinet and the industrial PC in the moving gantry, Scalance wireless access points from Siemens are employed to transmit data seamlessly on Profinet. CAMotion's vision was to have both standard and safety-related data transmitted wirelessly to support future expandability and rapid deployment.

CAMotion feels the use of the combination of a single failsafe PLC together with a single bus for both standard and safety-related data has given it a distinct competitive advantage in both price and performance that has resulted in lucrative, long-term business.

The Availability Of Products To Transmit Profinet Wirelessly Fulfilled CAMotion's Desire To Reduce Cabling Cost, Shorten Installation Time And Simplify Start-Up.

Swedish Solution Provider Rejlers Uses Networked Safety to Shorten Integration Time

Automobile manufacturers typically lead the rest of the industry in the adoption of new technologies. Carmakers and their suppliers are highly engineering-driven and work closely with automation suppliers in specifying and testing new solutions. As with the AIDA group of carmakers mentioned previously, this includes integrating safety into automation systems to help lower both start-up and operational costs.

One company with a reputation for innovation in the Scandinavian automobile industry is Rejlers, a systems integrator based in Sweden. The local office in Skovde recently designed the architecture for a new handling line for pistons and connecting rods around failsafe PLCs from Siemens networked to safety devices and standard I/O via Profinet and PROFIsafe.

The line consists of several machines that mark, classify, sort, buffer and palletize up to 60 different piston types as they come out of production. Parts handling is now fully automated using robots from ABB to identify parts and store them in temporary buffers. The previous solution consisted

of standalone machines with only semi-automated handling. The new automated solution employs uses Profinet as a backbone medium to network safety PLCs, industrial PCs and standard I/O blocks as well as E-stops, light curtains, and safety interlocks.
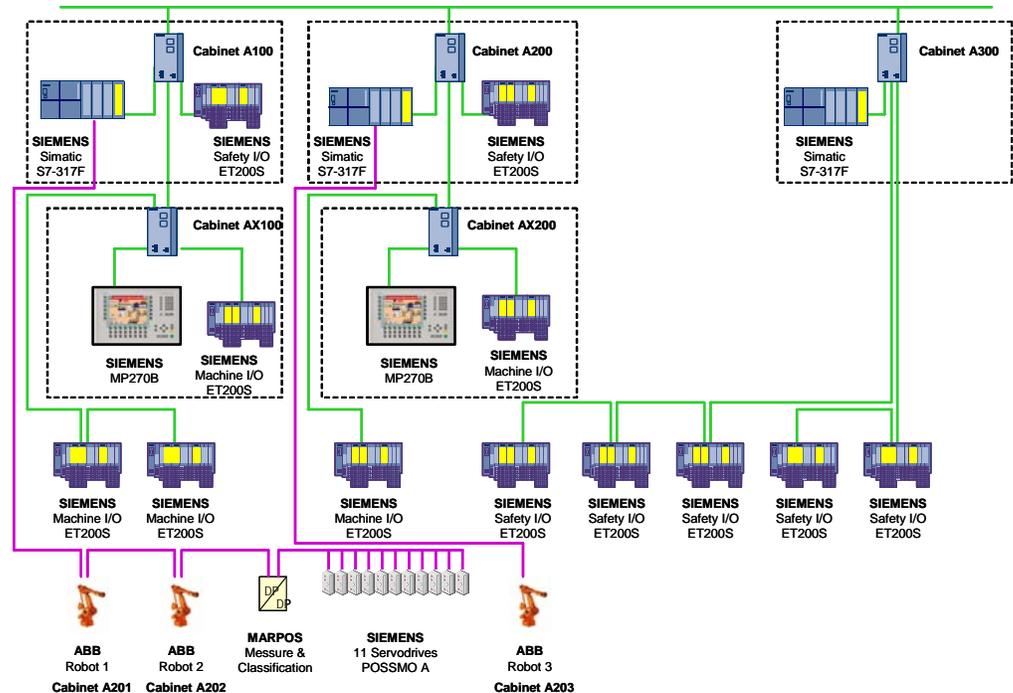
Rejlers' Architecture Uses PROFINET To Network Both Standard I/O And Safety Devices.

According to Rejlers, engineers decided on the PROFIsafe/Profinet solution – despite slightly higher hardware costs – because of the lower time it takes to install and integrate the system components. The company estimates a 30 to 35 percent time savings in integration efforts by using this architecture, thanks mostly to the solution's flexibility. A Rejlers engineer stated, "The hardware configuration is usually not finalized at the beginning of a project. Using Profinet, we can easily 'integrate in' an additional safety component on short notice - something that would take a lot more time with a hard-wired solution".

Due to the success of the initial project, the integrator has already been awarded follow-on contracts to extend the line in the near future.

Recommendations

- Safety strategy has become an increasingly important topic to manufactures in recent years, spurred on by both business and technical drivers. To put safety's benefits and caveats into perspective, manufacturers should re-assess the role that safety plays in their production strategy and learn how new technologies can help support business goals.

- On a technical level, two-bus architectures are a thing of the past, thanks to PROFIsafe's support of safety-related information on Profibus and Profinet. For new projects, machine builders, system integrators and end-users should find out how a single bus strategy can both cut installation costs and lower TCO for future production equipment.

- Safety component suppliers should assess the business opportunity of supporting industrial networks such as Profibus and Profinet with open safety communication. As the benefits of single network architectures become clear, customer demand with increase accordingly. Listen to your customers and you will hear the truth.

Analyst: David W. Humphrey

Editor: Uwe Grundmann

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/Community/terms/terms.htm

API	Application Program Interface	**ERP**	Enterprise Resource Planning
APS	Advanced Planning & Scheduling	**HMI**	Human Machine Interface
B2B	Business-to-Business	**IT**	Information Technology
BPM	Business Process Management	**MIS**	Management Information System
CAGR	Compound Annual Growth Rate	**MRP**	Materials Resource Planning
CAS	Collaborative Automation System	**OpX**	Operational Excellence
CMM	Collaborative Manufacturing Management	**OPC**	OLE for Process Control
		PAS	Process Automation System
CNC	Computer Numeric Control	**PLC**	Programmable Logic Controller
CPG	Consumer Packaged Goods	**ROA**	Return on Assets
CPAS	Collaborative Process Automation System	**RPM**	Real-time Performance Management
CPM	Collaborative Production Management	**SCM**	Supply Chain Management