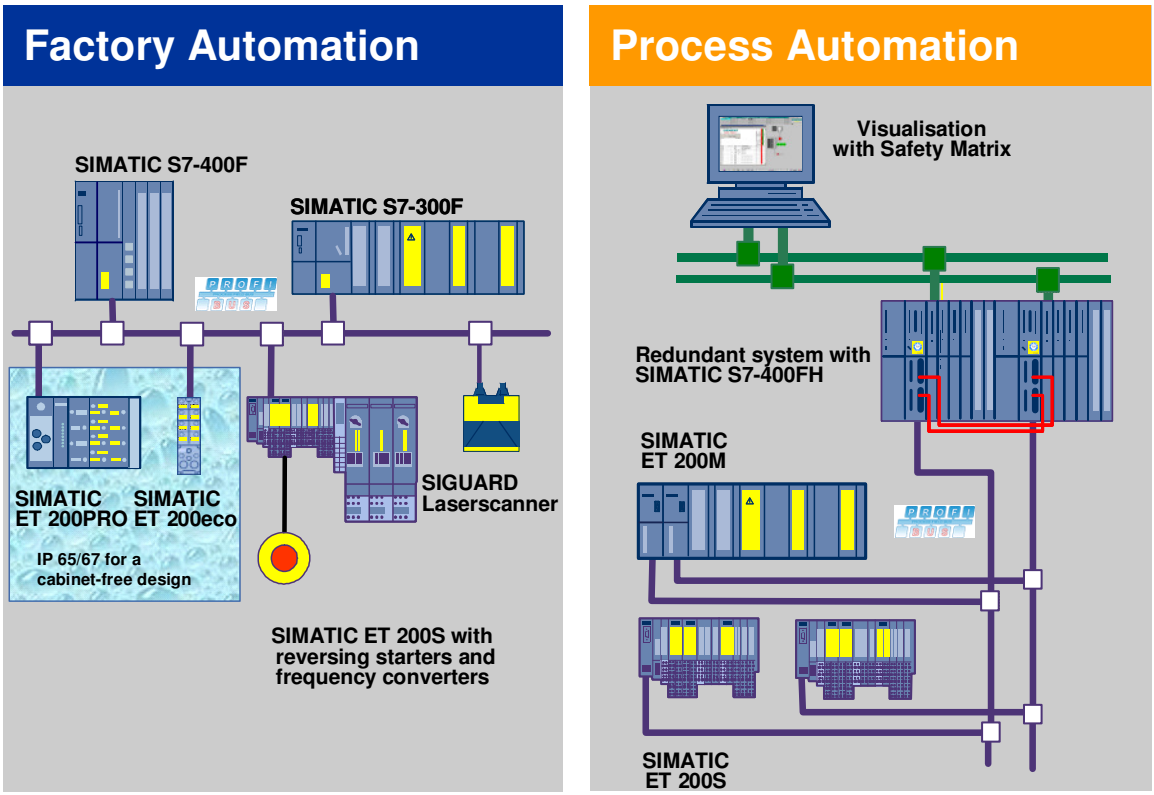
ARC WHITE PAPER

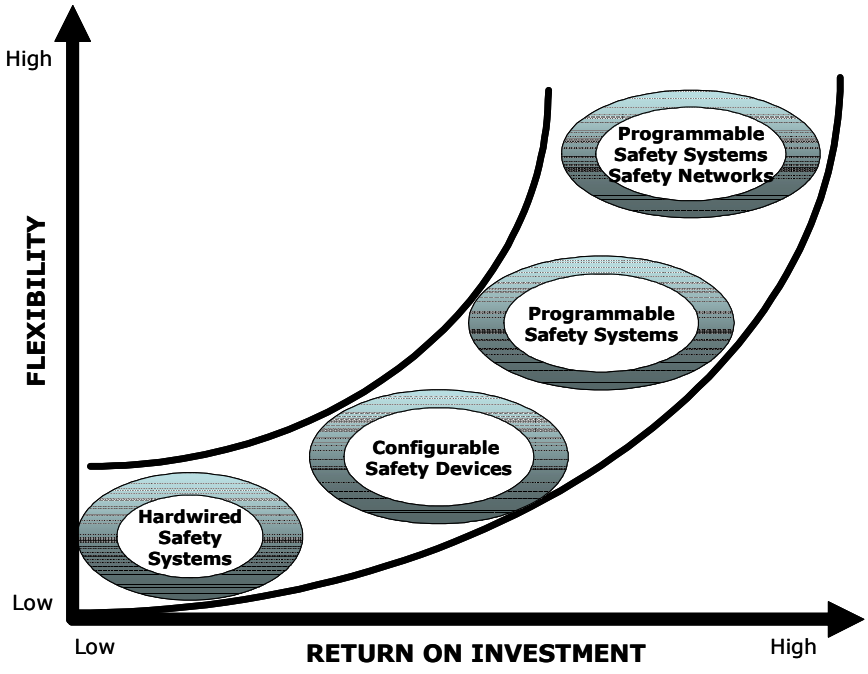
By ARC Advisory Group

APRIL 2005

Siemens' Safety Integrated Adds Value to Automation Applications



Safety Integrated Offers Solutions for Both Discrete and Process Users



Integrated Safety Solutions Maximize User Benefits

Executive Overview

Machine safety is one of the fastest growing segments of industrial automation. Safety, in terms of human and machine "health" and environmental protection, has moved to the forefront of critical topics for manufacturers due to an increased awareness of its importance. In addition to ensuring worker safety, manufacturers are learning how an intelligent safety strategy can become a competitive advantage rather than a cost burden. Driving this awareness are a greater desire by manufacturers to limit liability exposure and to improve their public image, the opinion that integrated safety systems can help improve the bottom line by reducing manufacturing KPIs, and the emergence of enabling technologies such as single-bus fieldbus and device networks that support safety protocols.

A safety system is an engineered solution that reduces the risk of harm to people, equipment or the environment that may arise from the operation of an individual piece of production machinery or line.

Harmonization of international safety standards, starting with IEC 61508 and EN 954, has simplified the regulations that a machine OEM has to understand and made it easier to develop globally acceptable safety strategies. In Asia, many countries publish equivalency charts that associate local standards with internationally recognized standards, making it possible for OEMs to declare compliance by association.

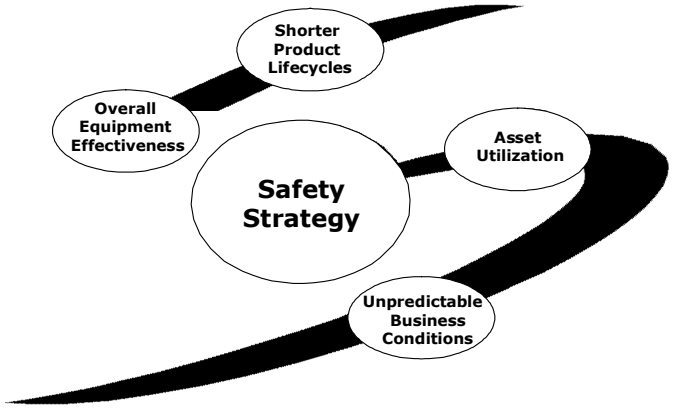
Separate controller and separate safety network architectures are quickly becoming a thing of the past, thanks to the emergence of dual-purpose safety controllers that handle both monitoring and control of safety and non-safety functions with a single CPU. Moreover, safety profiles for industrial networks now support the transmission of safety-related data while meeting the safety integrated levels typically required for most applications.

Integrated safety is now available in motion control solutions and supports a wide variety of safe drives functions without the use of external safety hardware. These functions can greatly increase machine productivity by allow operators to perform tasks such as checking, , cleaning, aligning and changing tools, that in the past could only be performed if power were completely removed from the drives. The benefits include faster restarts, no loss of accuracy due to repositioning, less brake wear and shorter downtime.

Business Issues Drive Growth in Discrete Safety Market

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.

A safety instrumented system is a system composed of sensors, logic solvers and final elements designed for the purpose of automatically taking an industrial process to a safe state when specified conditions are violated.



Business Drivers for a Coherent Safety Strategy

Safety has moved to the forefront of critical topics for manufacturers in recent years. An increased awareness of the importance of safety in automation systems has resulted in a boost in markets for both process safety and machine (discrete) safety components and solutions. In addition to ensuring worker safety, manufacturers 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:

- A greater 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.

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. Today's business drivers focus on metrics such 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). 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 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 lessen-

ing the workload, the burden of proof of compliance still lies with both the OEM and the end user.

Safety Standards Evolution and Harmonization Spur Product Development

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. However, regulations vary by country and the OEM still bears 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 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. 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.

New Technologies and Updated Standards Drive the Market for Safety Solutions

Technical advances in automation hardware and software and new and revised safety standards are driving the market for intelligent and programmable safety solutions. This new generation of solutions is designed to be more effective in preventing accidents, less costly to implement, easier to adapt, and more reliable than existing hard wired systems. Intelligent safety solutions are also helping end-users to more quickly locate sources of problems like nuisance trips. This can contribute significantly to an overall increase in manufacturing productivity.

Stop Category 0	Uncontrolled stop by immediately removing power to the machine drive element.
Stop Category 1	Controlled stop; power is only removed after the machine has come to a standstill.
Stop Category 2	Controlled stop, where power is still fed to the machine at standstill.

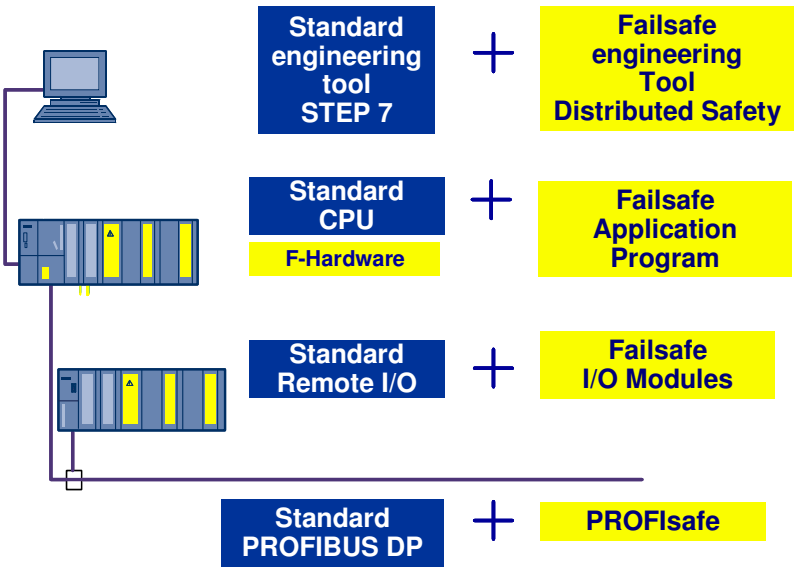
Stop Categories According to EN 60204-1

Safety Integrated, the portfolio of safety solutions from Siemens, is unique in the industry in that it offers a comprehensive set of components, complete

solutions and related services that meet the demands of both process and discrete manufacturers. Through PROFIBUS, Siemens is also a leader in the development of new safety technologies such as safe industrial networks. Safety Integrated products fall into four general categories: SIRIUS for switching device and fail-safe optical sensors, SIMATIC for fail-safe and high availability controllers, SINAMICS for integrated safety functions in drive technology and the SINUMERIK safety package for machine tools.

Standard Automation and Safety Systems are Fusing

Traditional approaches to safety architectures separate the control and monitoring of safety functions from the rest of the application. For specific applications such as presses or cranes, safety control systems are often certified together as system solutions. Discrete automation users often employ safety controllers and sometimes safety buses in parallel with PLCs. Relevant control or diagnostic information from the safety controller to the main controller can be exchanged by means of a network link, but the two controllers operate independently.



Fail-Safe Controllers Allow Users To Modify the Standard Program Without Affecting Safety Logic

This philosophy of separate solutions is changing. Technology developments have made it possible for a single controller to now handle both tasks, which has tremendous implications for cost savings in engineering and maintenance. Siemens' challenge to these dual system solutions is to offer controllers capable of handling both the monitoring and control of safety and non-safety functions with a single CPU.

At the controller level, safety components from I/O devices to fail-safe and high availability PLCs fall under the SIMATIC umbrella. Fail-safe versions of standard PLCs add an "F" to the CPU designation, such as S7-315F or S7-416F. These fail-safe CPUs are based on their standard counterparts, but with additions to the operating system that allow them to separately evaluate safety-related information while executing standard automation code at the same time.

This single-CPU approach to safety controllers has tremendous advantages over solutions employing a separate safety PLC. Besides the obvious cost savings in hardware alone, fail-safe CPUs allow the user to program all safety functions using the same familiar engineering tools, which can substantially reduce engineering costs. Safety functions are programmed by means of the "S7 Distributed Safety" library of commands that includes TÜV-certified function blocks for functions such as emergency off, two-hand control, muting, gate monitoring and others. Additional libraries are also available for specific applications like burner management. The rest of the standard application can be programmed in the CPU as before without affecting the safety functions, which can be password protected separately.

Fail-safe CPUs execute both standard programs and safety functions, eliminating the need for a separate safety PLC. This can substantially reduce costs for engineering, start-up and maintenance.

Fail-safe controllers are certified to meet the safety requirements of international safety standards, typically category 3 or 4 for EN 954 or SIL 2 or 3 for IEC 61508.

"High availability" refers to dual redundant control systems such as the SIMATIC PCS 7 from Siemens. In a redundant control system, every element, from the operator station to field devices and including the fieldbus, is backed up by a duplicate. Control CPUs execute the same program in synchronization and can be co-located or separated by long distances, such as at opposite ends of a tunnel. Redundancy is typically required in continuous processes in which any stoppage could lead to heavy material losses.

Siemens offers CPUs in the S7-400 range as "H" versions (high availability) with or without additional "F" (fail-safe) functionality. "S7 F Systems" is the software extension to the Step 7 engineering tool that allows users to configure safety related process applications according to the IEC 61511 safety standard for process control. This package simplifies the creation of safety programs with the use of a fail-safe library with TÜV certified function blocks up to SIL 3 (IEC 61508). S7 F Systems also manages the documentation of safety programs by administration of "signatures", which are electronic codes that determine whether a function block has been modified. As with S7-300 series fail-safe CPUs, additional safety function libraries are available for specific applications like gas or oil burner management.

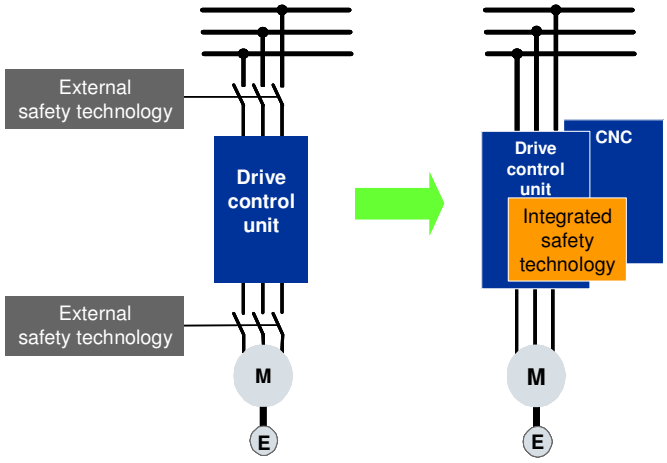
Automation systems with high availability are typically used in the oil & gas industry to protect investments in production and refining assets. Modern redundancy strategies network redundant controllers to I/O de-

vices via a fieldbus to take double advantage of cost savings versus hard-wired solutions. For redundant applications using Siemens' SIMATIC PCS 7 process controller, PROFIBUS can be engineered redundantly and integrated with AS 414H and AS 417H high availability CPUs. Available field devices include remote I/O modules ET200M, ET200 M failsafe, as well as the DP/PA link. Non-redundant PROFIBUS devices can also be integrated via a Y-link interface.

SIMATIC's product offering for safety components extends to the device level through the ET200 line, including remote I/O blocks ET200M, ET200 M failsafe, ET200S. In addition, ET200 PRO and ET200 eco remote I/O blocks provide IP67 protection for cabinet-free design. Additional devices are fail-safe motor starters and frequency converters as well as a redundant version of the DP/PA Link for PROFIBUS. Standard digital and analog I/O modules also can be combined with fail-safe modules connected to the same adapter – a major convenience for end-users.

Evolution of Standards Adds Flexibilty to Safety Systems

Recent changes to NFPA 79 in the United States and IEC 60204 now allow non-hardwired components to be used in emergency stop functions, allowing a degree of flexibility in safety unknown in the past. This is a big step forward not only for international harmonization, but also for the use of electrically programmable control systems in the implementation of E-stop safety functions. A category 0 stop is a "hard" stop that can leave axes spinning without control and usually results in machine downtime while drives are homed and repositioned. Implementing a category 1 or 2 stop by programmable means brings a machine to a controlled stop in a known position from which a faster recovery can be made. This also allows the machine to maneuver to a safe position after which operators can manually correct problems in the machine such as product jams.



SINUMERIK „Safe" Drives Contain Internal Logic to Monitor Safety Functions

Safety Comes to Motion Control

As machinery employs more automated subsystems for either material handling or automated changeover, the trend in the market is towards safety solutions that allow operators to work better within the work enve-

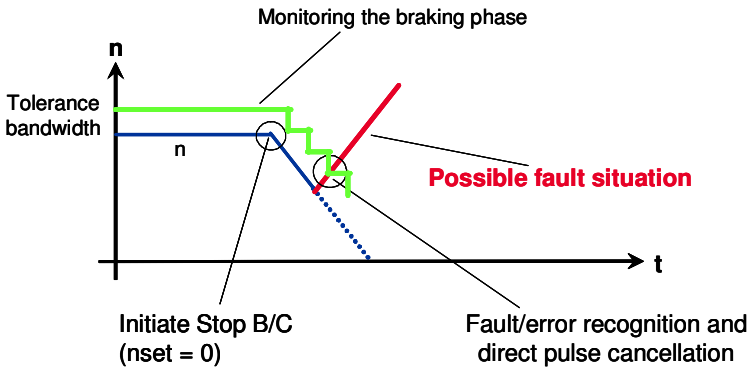
lope of the machine. Revised safety standards now allow the integration of electronic and programmable safety systems directly in servo drives, mak-making it possible for machine builders to design machine safety so that axis movement can operate at safe speeds while the operator is in the work envelope, replacing previous requirements that power must always be removed from drives by electromechanical means. With safe drives, safety solutions are becoming less complex, with far fewer cables and connections, resulting in reduced design, commissioning and installation costs.

Safe standstill
Safe operating stop
Safe stopping process
Safe brake ramp
Safe brake management
Safe brake control
Safely reduced speed
Safe software limit switch
Safe software cams
Safe programmable logic
Safety-related input/output signals
Safety-related communication via PROFIsafe

Safety-related Functions Supported by SINUMERIK

SINUMERIK safety integrated motion control from Siemens supports a wide variety of safe drives functions, including safe standstill, safe operating stop, safe brake ramp, safely reduced speed, safe software limit switch and others. These functions can greatly increase machine productivity by allow operators to perform tasks such as checking, measuring, cleaning, aligning, removing chips, changing work pieces and tools, that in the past could only be performed if power were completely removed from the drives. The benefits include faster restarts, no loss of accuracy due to repositioning, less brake wear and shorter downtime.

It is important to note that safety integrated motion control, first available in 1996, meets the requirements of EN 954 Cat 3 and IEC 61508 SIL 2 levels. This has enabled European machine builders in particular to design new generations of machinery that enable increase operator productivity. Arguably, this has also made machines safer by making them more tamper-proof than traditional hardwired systems. By providing factory floor operators with equipment that allows them to work productively while minimizing their risk of injury to the lowest possible level, there is less likelihood that safety subsystems will be overridden. Overall, the use of safety integrated motion control technology can offer machine OEMs a significant competitive advantage.



The Safe Braking Ramp Function (SBR) Monitors the Braking Phase for Possible Faults and Generates a Category 0 Stop if Necessary

SINUMERIK Safety Integrated also meets the Nationally Recognized Testing Laboratory (NRTL) functional safety requirements of NFPA 79-2002.

With the recent changes to NFPA 79 and the granting of the NRTL listing in the USA for SINUMERIK Safety Integrated, manufacturers are now starting to implement this technology to meet demands for more workplace safety and productivity. It is now dependent upon the local regulatory agencies and standards making organizations to revise older machine standards to accept widespread use of these solutions.

Technology alone doesn't enable manufacturers to become more productive. It is the combination of regulatory agencies, industry awareness and innovative technology that will drive the wider adoption of more intelligent machine safety solutions.

SIRIUS Completes the Safety Integrated Portfolio

SIRIUS is a large family of safety components that includes safety monitors, emergency stop switches, position switches, safety locks, two-hand operator consoles and signal columns and lamps. Together with light curtains and grids this family completes the portfolio. For simple applications, these components can be either hard-wired with safety relays or networked using the AS-Interface bus and the "Safety at Work" safe protocol, which only requires the addition of a configurable safety monitor and associated safety slave devices. Taking this approach, a standard PLC can be used without the expense of adding a failsafe PLC to the architecture. Practically any PLC or PC is capable of interfacing with the AS-Interface network via an AS-Interface master card or gateway to a higher level network.

SIRIUS Components Can Be Networked Via AS-i Bus And The Safety-At-Work Protocol

For more complex applications, PROFIBUS with its PROFIsafe profile adds safety telegrams to the communications layer. Turning a normal PROFIBUS into a safety bus only requires the addition of a failsafe PLC and associated safety slave devices. Siemens offers S7300F and S7400F series PLCs that allow both failsafe and standard control in the same architecture. As an alternative to replacing a standard PLC, an ET200S distributed I/O module system with a failsafe CPU head module can be used for a distributed PROFIsafe network allowing both safety and standard I/O.

For applications involving operator interaction such as mechanical and hydraulic presses, edging presses, punching machines, production and packaging machines, robots and transport equipment, the SIRIUS line offers configurable light curtains and grids as well as more sophisticated laser

scanners. The light curtains include features such as muting and fixed and floating blanking, which increase flexibility by allowing certain objects to enter the protective field without tripping a shut down.

For full spatial protection in robot cells, for example, a laser scanner allows the user to configure multiple protective fields to detect personnel at distances up to 4 meters and non-safety-relevant objects up to 15 meters. Laser scanners are especially adept at defining sophisticated geometries in which multiple sub-zones can be defined. Protective fields can be switched on-the-fly, giving commissioning personnel more flexibility without endangering normal operations. Finally, the laser scanners are also appropriate for automatic guided vehicles (AGV) where they can allow higher operating speeds when used as "soft bumpers". The laser scanners can be either hard-wired or networking via AS-I or PROFIBUS.

PROFIsafe Brings Single-Bus Solution to Safety

With over 13 million installed nodes, PROFIBUS is probably the world's most widely deployed industrial network. PROFIBUS International, the consortium of suppliers behind the network's development, continues to expand the scope of PROFIBUS in the discrete and process industries. The introduction of the PROFIsafe profile and compatible products heralded a new era of industrial networking in which a single bus now can handle both standard and safety-related telegrams. A separate safety bus is no longer necessary.

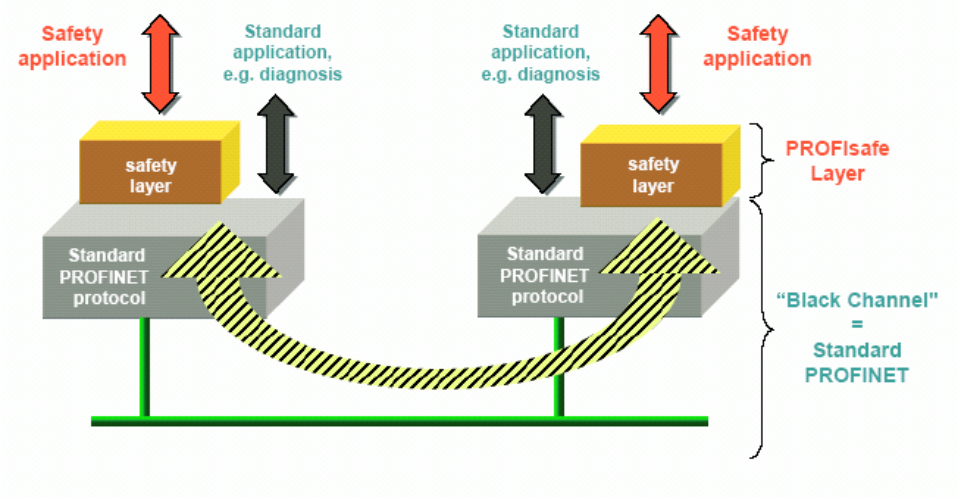
Failure Type -> Remedy	Consecutive Number	Time Out with Receipt	Codename for Sender and Receiver	Data Consistency Check
Repetition	X			
Deletion	X	X		
Insertion	X	X	X	
Resequencing	X			
Data Corruption				X
Delay		X		
Masquerade (standard message mimics fail-safe)		X	X	X
FIFO failure within Router		X		

Failure Detection Measures for Safety-Related Data Using PROFIsafe

The communication on standard industrial networks including PROFIBUS is not adequately fault tolerate to achieve the required levels of reliability to satisfy safety standards. Telegrams can get lost, become corrupted or get delivered out of sequence. To ensure data integrity to meet safety requirements, PROFIsafe adds additional safety data checks at the application layer that monitor watchdog timers, check telegram numbering, verify sequencing and signatures and perform additional data consistency checks. These extra steps take place within normal PROFIBUS telegrams and coexist on the same network. Fail-safe slaves that support the PROFIsafe profile, such as the ET200M series of remote I/O devices, contain logic to automatically and seamlessly integrate with fail-safe CPUs. These devices can be combined on the same network with standard remote I/O devices.

PROFInet Looks to the Future

Ethernet has become a *de facto* standard in controller-to-controller communications since it first appeared in the factory in the early 1990s. Industrial Ethernet, in the meantime, is now a viable alternative for communication at the device level as well. Based on the IEEE 802.3 standard, industrial Ethernet extends the network's capabilities to address specific needs of



PROFIsafe Checks Data Integrity of Fail-Safe Devices Alongside Standard PROFIBUS or PROFInet Communication

manufacturers such as device power and deterministic response. PROFInet, the industrial Ethernet standard created by PROFIBUS International, is more than PROFIBUS on Ethernet. Through network proxies, segments of PROFIBUS and other industrial networks such as Interbus-S can connect to PROFInet, effectively turning it into a high-speed factory backbone network.

To support the growing acceptance of PROFInet in the factory, PROFIBUS International is porting application profiles such as PROFIsafe to PROFInet. Plans are to publish a new PROFIsafe V2.0 specification by Q3 2005, after which the first products are expected to appear by the end of the year.

Recommendations

- Safety technology has evolved into a sophisticated set of technological solutions that provide measurable business benefits. A well thought out, intelligent safety strategy should not only protect humans, machines and the environment, but also support business benefits such as increased productivity, improved machine efficiency and reduced downtime. Manufacturers should consider these factors in the planning stages when considering new automation strategies.

- Users should carefully observe the development and certification of new technologies such as safe industrial networks and drives with built-in safety features, as these can lower hardware costs, increase machine flexibility and boost overall productivity.

Analyst: David W. Humphrey
Editor: Sal Spada

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

AI	Artificial Intelligence
API	Application Program Interface
APS	Advanced Planning & Scheduling
B2B	Business-to-Business
BPM	Business Process Management
CAGR	Compound Annual Growth Rate
CAS	Collaborative Automation System
CMM	Collaborative Manufacturing Management
CNC	Computer Numeric Control
CPAS	Collaborative Process Automation System
CPM	Collaborative Production Management
CRM	Customer Relationship Management
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IT	Information Technology
LAN	Local Area Network
MIS	Management Information System
OpX	Operational Excellence
OPC	OLE for Process Control
PAS	Process Automation System
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
ROA	Return on Assets
ROI	Return on Investment
RPM	Real-time Performance Management
WAH	Web Application Hosting
WMS	Warehouse Management System

Founded in 1986, ARC Advisory Group has grown to become the Thought Leader in Manufacturing and Supply Chain solutions. For even your most complex business issues, our analysts have the expert industry knowledge and firsthand experience to help you find the best answer. We focus on simple, yet critical goals: improving your return on assets, operational performance, total cost of ownership, project time-to-benefit, and shareholder value.

You can take advantage of ARC's extensive ongoing research plus experience of our staff members through our Advisory Services. ARC's Advisory Services are specifically designed for executives responsible for developing strategies and directions for their organizations. For subscription information, please call, fax, or write to:

ARC Advisory Group, Three Allied Drive, Dedham, MA 02026 USA
Tel: 781-471-1000, Fax: 781-471-1100, Email: info@ARCweb.com
Visit our web page at ARCweb.com

3 ALLIED DRIVE DEDHAM MA 02026 USA

BOSTON, MA | PITTSBURGH, PA | PHOENIX, AZ | SAN FRANCISCO, CA
CAMBRIDGE, U.K. | Düsseldorf, GERMANY | MUNICH, GERMANY | HAMBURG, GERMANY | TOKYO, JAPAN | BANGALORE, INDIA