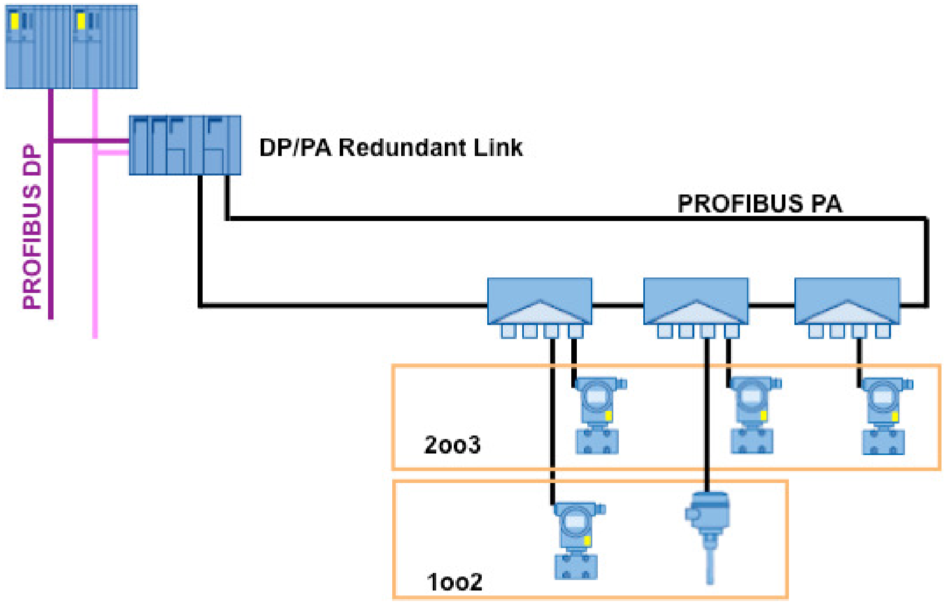
ARC WHITE PAPER

By ARC Advisory Group

APRIL 2009

Profisafe and Profibus for High Availability and Safety in the Process Industries

ARC Advisory Group



Profibus PA's Ring Redundancy for High Availability

	Profisafe	Redundancy	Profisafe and Redundancy
Application	Factory and process automation Presses, robots, level switches, shutdown valves, burner controls, cable cars	Process automation Chemical and pharmaceutical production, refineries, offshore rigs	Process automation Chemical and pharmaceutical production, refineries, offshore rigs
High Availability	--	No downtime (fault tolerance)	No downtime (fault tolerance)
Safety	No dangerous failures (required by law or insurance)	Redundancy alone does not ensure safety	No dangerous failures (required by law or insurance)

Profibus and Profisafe Support Safety and High Availability for Different Application Requirements

Executive Overview

Process automation has profited tremendously from technology advances in recent years. Distributed intelligence, network safety protocols, Industrial Ethernet, and wireless networking are just a few of the enabling technologies that have brought measurable value to process manufacturing. But, traditionally, process users are extremely conservative decision-makers who don't accept new a technology until it is well proven, or until investments in these technologies can be corroborated with solid business arguments. To help users sort out fact from the hype, manufacturers are learning how to match technology benefits to specific business metrics.

Traditionally, process users are extremely conservative decision-makers who don't accept new a technology until it is well proven, or until investments can be corroborated with solid business arguments.

Two topics in particular – process fieldbuses and open fieldbus safety protocols – have caught the attention of process users in recent years thanks to the potential to cut costs and improve diagnostics. Modern fieldbuses have helped to unify network architectures and created a high level of data transparency from which applications such as Plant Asset Management and Manufacturing Execution Systems profit tremendously. At the same time, process safety solutions have evolved from being a cost burden and "necessary evil" to a strategy for improving productivity by increasing system availability.

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

Because process instrumentation customers have made substantial investments in existing Profibus PA-, HART- or Foundation Fieldbus H1-compatible process field devices, the adoption of any new technology will be evolutionary, rather than revolutionary. In addition, many process plants have installed bases of intelligent devices – from simple remote I/O to motor control centers – that are networked with legacy device networks such as Profibus DP, Foundation Fieldbus, or DeviceNet. Therefore, the key success factor for new networking solutions in process plants will be the availability of a migration path that lets users preserve their investments in legacy networks and devices by integrating existing networks into a common backbone.

Safety and Availability: Two Sides of the Same Coin

Integrated process safety solutions address two separate and distinct issues – functional safety and system availability – both of which are critical for process users. The good news is that integrated solutions support both goals using the same hardware, meaning that safety and availability are effectively two sides of the same coin. Even so, their goals and drivers remain distinct.

Functional Safety

The goal of **functional safety** is to maintain safety functions in order to prevent personnel from being injured, such as by de-energizing hazardous elements. A characteristic measure for a safety function is Safety Integrity Level (SIL). This describes the safety function's probability of a dangerous failure per hour, e.g. 10^{-7}/h for SIL3. Functional safety is important in industries in which operators work closely with running machinery, or where unwanted process events could result in fire, explosion, or other hazardous conditions.

System Availability

In contrast, **system availability** (fault tolerance) maintains the control functions even in case of component failures. High availability is important in applications in which stopping the process could cause extensive damage or for continuous processes for which a restart would cause expensive delays. An example of this is a fired heater or a catalytic cracker in a refinery that, as an endothermic reaction, could feed on itself if out of control and lead to a catastrophic explosion. Other stoppages may not be dangerous, but might result in whole batches of product being thrown away or cause long delays due to complex start-up routines.

Controller redundancy is the typical solution to ensure high equipment availability. A characteristic measure for high availability is the ratio of uptime to the total operation time, for example, a typical minimum acceptable availability might be 99.99 percent or even higher. Profibus and the Profisafe protocol can be deployed in these applications with or without redundancy to achieve high availability. In addition, Profisafe plays an important role in high availability systems known as Flexible Modular Redundancy (FMR).

Business Drivers in Process Automation and Safety

As appealing as new technologies may be, process manufacturers make decisions based primarily on sound business benefits, rather than technical arguments. The value of these arguments can be measured by applying standard business metrics that start with system availability – a measure of uptime that is akin to buying an insurance policy against unexpected disruptions. Availability is all about ensuring that continuous processes cannot be stopped due to the failure of individual components such as CPUs or field devices.

Fault-tolerant systems ensure safety functions, while “excusing” minor faults that can result from simple equipment failure. This can directly increase productivity to ultimately reduce Total Cost of Ownership (TCO). Other important metrics for process equipment purchases include Return on Assets (ROA) and Overall Equipment Efficiency (OEE), both of which are critical contributors to the overall goal of achieving Operational Excellence (OpX).

Safety Systems and Safe Fieldbuses Go Hand in Hand

Process safety, in the traditional sense, refers to add-on monitoring and safety shutdown equipment that protects plant personnel, equipment, and the environment from disasters, small and large. In other words, process safety expenditures are a necessary evil. The modern reality is that times have changed. Process safety solutions today are integrated into process control equipment, helping to reduce system complexity while shortening engineering and start-up time. In addition, modern safety solutions take advantage of fieldbuses with "built in" safety to reduce wiring costs, improve diagnostics, and better manage assets.

Process fieldbuses, like Profibus, have brought tremendous value to process users since their introduction a decade ago. Fieldbuses replace expensive wiring of I/O and field devices with a single cable, adding flexibility while improving access to valuable device status information that is the foundation of asset management. With the addition of safety to the fieldbus, process users can integrate both safe and non-safe devices more easily into a single architecture.

Justifying Investments in Process Safety

By all rational thinking, investments in highly available systems should be directly proportional to the risk of a system failure. But when a process user considers the consequences of stopped production for days, weeks or even months; or the astronomical cost of the resulting damage to personnel, equipment and the environment; then even the high cost of redundant safety systems and redundant field devices can easily be justified. The result is a general keen interest in the market for redundant safety systems with supporting redundant and safe fieldbuses.

In addition to increasing availability and ensuring worker safety, process manufacturers are learning how an intelligent safety strategy can contribute to achieving business goals. Several factors are driving this increased awareness, including:

- A desire by process manufacturers to limit liability exposure and to improve their public image,
- The view that integrated safety systems can help improve the bottom line by increasing equipment availability, increasing Overall Equipment Efficiency (OEE) and improving Return on Assets (ROA),
- Harmonization of international safety standards that allows process equipment makers and end users to develop and deploy globally acceptable safety solutions.

The Costs and Risks of Not Ensuring Process Safety

Many process manufacturers have seen their public image suffer in recent years due to negative press from catastrophic incidents, product safety issues, and boardroom scandals, resulting in a loss of public trust. These experiences have taught companies the importance of 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 increasingly 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.

In an increasingly socially conscious world, process manufacturers understand the importance of improving their good neighbor image by actively promoting their adherence to good manufacturing practices and compliance with environmental and occupational safety best practices.

Besides image challenges, plant operators and systems integrators 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 "good faith" by documenting compliance with all generally accepted industry practices. Such tactics can also be applied to safety strategies, especially for process equipment makers 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 the process equipment maker and the end user.

PROFIBUS and PROFIsafe Build the Foundation for Process Safety

Profibus International (PI), with a global community of more than 1200 member companies, is the industrial consortium responsible for developing and marketing Profibus 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 two-wire applications in factory automation, and Profibus PA, which offers intrinsic safety for process-type applications.

Profibus PA uses MBP technology (IEC 61158-2, Manchester-encoded, bus-powered), a two-wire cable standard that combines the functions of data transmission and power supply. MBP-IS ("intrinsically safe") is available for use in hazardous areas. With short-circuit protection and power limitation, the installation technology supports the explosion protected operation of field devices in Zones 0, 1 and 2 and/or Class I/Div.1 and Class I/Div.

Failure Type: Remedy	Consecutive Number	Time Out with Receipt	Codename for Sender & Receiver	Data Consistency Check
Repetition	X			
Deletion	X	X		
Insertion	X	X	X	
Resequencing	X			
Data Corruption				X
Delay		X		
Masquerade		X	X	X
FIFO Failure Within Router		X		

PROFIsafe Adds Failure Detection Measures That Are Lacking In Standard Fieldbuses

In addition to media, PI's working groups have developed a host of application profiles that address specific application needs ranging from motion control to weighing to time stamping. For safety applications, PI developed Profisafe to handle the transmission of safety-related information on Profibus and Profinet. PROFIsafe Adds Failure Detection Measures That Are Lacking In Standard Fieldbuses

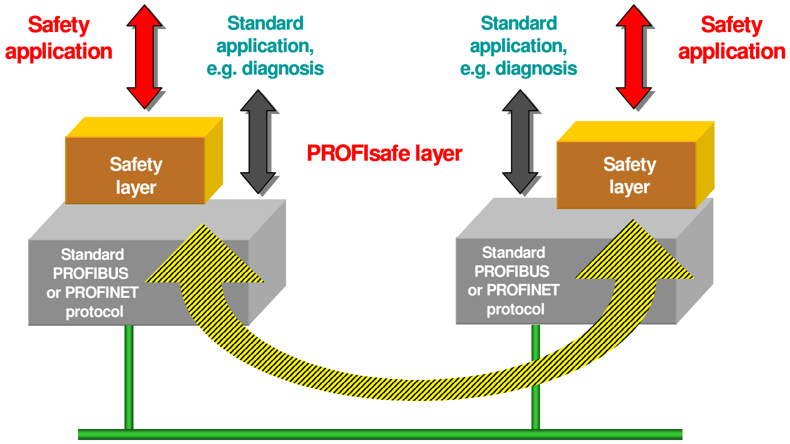
Safety on the Wire: PROFIsafe Enables Single-Bus Solutions

Thanks to recent developments in safety technology, modern automation philosophy now recognizes that it's no longer necessary to run two separate fieldbuses for safety and non-safety data. This adds considerable value, since a two-bus architecture requires double the amount of training and network access hardware and makes start-up and troubleshooting tasks unnecessarily complex.

With the arrival 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 fieldbus and reduce their network architectures to a single fieldbus. 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 Integrity Levels (to SIL3) prescribed by international safety standards. Since Profisafe is built into the communications protocol, it can be used by devices connected to any Profibus medium, including Profibus DP and PA, as well as Profinet. This single-bus approach is especially useful in industries such as food & beverage and pharmaceutical where machine safety plays an important role.

PROFIBUS PA Extends Fieldbus 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.

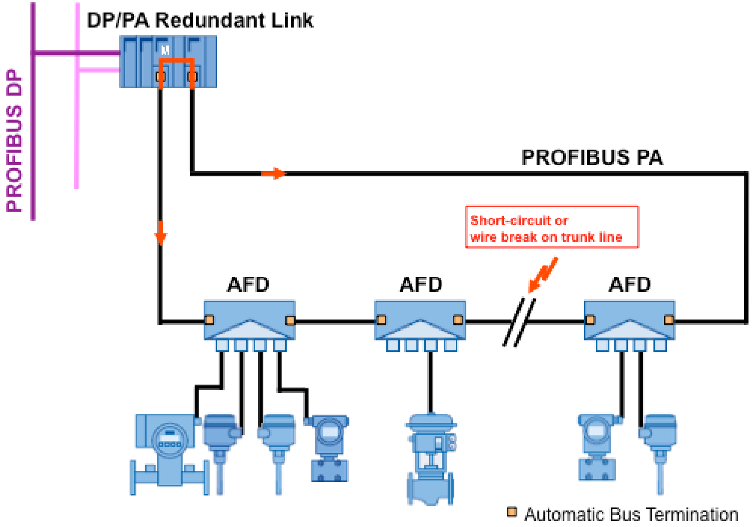

Safety application
Standard application, e.g. diagnosis
Standard application, e.g. diagnosis
Safety application
PROFIsafe layer
Safety layer
Safety layer
Standard PROFIBUS or PROFINET protocol
Standard PROFIBUS or PROFINET protocol

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

Profibus PA offers networked 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 without having to worry about bridges or gateways.

Ring Redundancy for High Availability

For applications requiring high availability, Profibus PA can be configured in a ring architecture that ensures communication, even if part of the network cable is disabled due to a short circuit or physical damage. A ring architecture uses "active field distributors" (AFD) to integrate field devices via four short-circuit-proof spur line connections in a Profibus PA ring with automatic bus termination. This ensures that, in the case of a break in the ring, the end of the remaining segment is terminating so that network communication can continue.


PROFIBUS DP
DP/PA Redundant Link
M
PROFIBUS PA
Short-circuit or wire break on trunk line
AFD
AFD
AFD
Automatic Bus Termination

Ring Redundancy on Profibus PA is Possible with Active Field Distributors with Automatic Bus Termination.

The ring is connected to two DP/PA couplers that can be operated on a single or redundant Profibus DP. Up to eight AFDs and 31 Profibus PA devices can be configured per ring. Profibus PA also allows AFDs to be hot-swapped.

Smart Fieldbuses Enable Smart Diagnostics

Intelligent diagnostics of field devices can contribute not only to reducing operational budgets, but also to increasing system availability by heading off device failures through predictive maintenance. To accomplish this, two things are necessary: 1) the reliable extraction and storage of information, and 2) tools to evaluate information and act on the results.

To extract information from field devices, Siemens offers a tool called Simatic Process Device Manager (PDM). PDM is a universal, vendor-independent software tool for configuring, commissioning, diagnosing, and maintaining intelligent process field devices networked with Profibus. The flexibility of PDM allows the use of one tool to configure a host of field devices from different vendors using a single user interface. Functionality includes changing process device data, checking plausibility, and simulating various modes of operation. Using PDM from a central engineering station, users can parameterize and troubleshoot intelligent field devices remotely over Profibus. PDM serves as the communications basis for an asset management system.

Plant Asset Management (PAM) systems are a combination of hardware, software, and services deployed to help the workforce predict and assess the health of plant assets by monitoring asset condition periodically or in real time to identify potential problems before they affect the process or lead to a catastrophic failure. Closer integration of PAM with control and safety systems and fieldbuses facilitates early detection and notification of failures of field devices and processors.

A key driver behind the acceleration of PAM adoption is the critical need for the current workforce to do more with less by providing information at the right time and in the right context. Profibus and other fieldbuses make this possible.

A key driver behind the acceleration of PAM adoption is the critical need for the current workforce to do more with less. By providing information at the right time and in the right context, workers work smarter. This provides maximum benefit to the enterprise. Success in today's "flat world," where a plant's assets and workforce may be scattered across the globe, requires the availability of information 24 hours a day, seven days a week.

PROFIsafe Product Availability

With over 630,000 Profisafe devices installed to date, many automation and field device suppliers are coming out with Profisafe-compatible products. These include PLC and DCS controllers, standard and intrinsically safe remote I/O, transmitters, drives and fail-safe sensors.

Case Study: Greylogix Deploys Profisafe in a Pipeline Compressor Station

GreyLogix GmbH, a systems integrator based in Flensburg, Germany, specializes in turnkey process systems for industries ranging from power generation and natural gas pipelines to food & beverage and chemicals. Founded in 2000 as a spinoff of the internal engineering department of Hamburg Gas Consult GmbH, the company employees about 250 people. As a Siemens Solution Partner and certified PCS 7 Safety Specialist, GreyLogix standardizes on Siemens' Simatic PCS 7 distributed control system.

In a recent project, GreyLogix modernized the control system in a natural gas pipeline compressor station in Northern Germany. The station is one of many along a pipeline that transports natural gas from the Netherlands to two gas distribution networks in Germany. Natural gas is re-compressed in each station to ensure that the required transport pressure is maintained. The safety requirements for these compressor stations are high with particular emphasis on the safety loops for temperature and pressure. In this project, GreyLogix used the latest control and fieldbus technology to achieve the required safety integrity level (SIL) for all the safety instrumented functions.

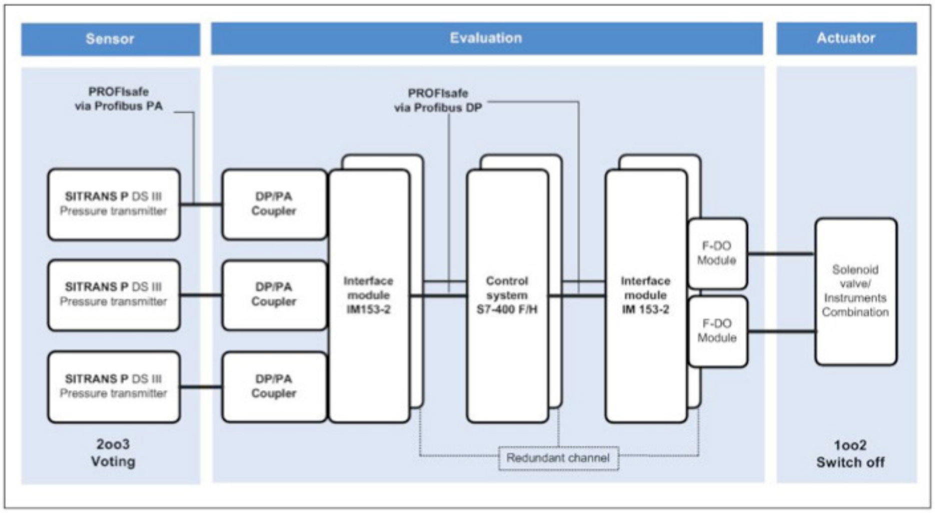
Originally built in the early 1970s, the compressor station was upgraded to a Siemens Teleperm M control system in the 1990s. However, the Teleperm product has been discontinued, so getting spare parts will become more difficult with time – a real problem for a control system that has to be highly available. For this reason, the customer decided to migrate to the Siemens Simatic PSC 7 for the three gas turbines in the station.

The Gas Compressor Station Uses Pressure Transmitters with SIL2 Safety Loop Capability. SIL3 Is Possible In A 2oo3 Configuration, as Shown Here.

The compressor station is normally operated remotely, but can also be run from a central control room. A redundant server supplies each of four operator station (OS) clients with project data, process values, alarms and messages. A further server supplies the connected Dispatch Center with data around the clock. The PCS7 process control system monitors all relevant data including pressure, temperature and flow. The emergency shut down and the fire and gas systems are integrated into the process control system giving a uniform visualization of all aspects of the process. This single-window approach simplifies the operation of the plant considerably and also consolidates alarm management, time stamping, sequence of events recording and asset management.

For the communication with the field instruments, GreyLogix decided to use Profibus with the Profisafe protocol instead of conventional 4-20 mA technology. In addition to reducing wiring and improving measurement accuracy, Profibus enables direct access to device status and configuration information. The safety-related communication is based on standard Profibus enhanced by the Profisafe profile. Profibus allows safety-related and standard communications to co-reside on the same bus, thus avoiding the need for a separate safety bus while still fulfilling safety requirements for up to SIL3. To provide lightning and surge protection, GreyLogix used a fiber optic cable for Profibus.

To set parameters, commission, diagnose and maintain the field devices, GreyLogix uses the Simatic Process Device Manager (PDM), a tool for managing field device data that supports products from more than 100 different vendors. Device configuration is handled from the PDM tool based on the standardized Electronic Device Description (EDD) supplied by the device vendor. Using PDM, operators have access not only to fault diagnosis information, but also to detailed troubleshooting guidelines to help rectify problems.


Sensor
Evaluation
Actuator
PROFIsafe via Profibus PA
PROFIsafe via Profibus DP
SITRANS P DS III Pressure transmitter
SITRANS P DS III Pressure transmitter
SITRANS P DS III Pressure transmitter
DP/PA Coupler
DP/PA Coupler
DP/PA Coupler
Interface module IM153-2
Control system S7-400 F/H
Interface module IM 153-2
F-DO Module
F-DO Module
Solenoid valve/ Instruments Combination
2oo3 Voting
Redundant channel
1oo2 Switch off

GreyLogix Employs the Simatic S7-400 F/H In A Redundant Set-Up To Achieve High Availability And To Fulfill Failsafe Requirements For SIL3.

With over 22 different safety loops for pressure, temperature and fire detection, functional safety is extremely important for the compressor station. To meet the required SIL level, a safety function was necessary to keep the compressor station in a safe state by making sure the pressure of the compression does not exceed defined limits.

For the SIL calculation, the safety loop is split into three segments: sensor, transmission and evaluation, and actuator. For each element of this chain a failure limit value is determined, called Probability of Failure on Demand (PFD). This value, which is typically available in the device's operating manual, describes the average probability that the safety function will fail on demand. In this application, the safety functions for pressure protection are designed for low demand because a fault in the process control is expected only one time per year.

For the SIL level of the complete safety loop, the PFD values of the sensor, transmission and evaluation and actuator part are added together. The use of the Sitrans P DSIII pressure transmitter for each compressor unit and the exclusive use of SIL3 certified components for the signal processing simplified the calculation. The Sitrans P DS III is SIL2 certified and, when used redundantly in a 2oo3 architecture ("two out of three"), the safety function for the end pressure protection has a PFD value of 0.00013, which meets the requirements for SIL3 according to IEC 61508. The use of Profibus, a certified safety fieldbus, had a positive influence on the SIL calculation.

Recommendations

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

- On a technical level, Profibus and other modern fieldbuses now combine standard fieldbus features with a safety protocol such as Profisafe. For new projects, process equipment makers, system integrators and end-users should find out how a single fieldbus strategy can 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.

Analyst: David W. Humphrey

Editor: Paul Miller

Acronym Reference: For a complete list of industry acronyms, refer to our web page at www.arcweb.com/C13/IndustryTerms/

API	Application Program Interface
B2B	Business-to-Business
BPM	Business Process Management
CAGR	Compound Annual **Growth R**ate
CAS	Collaborative Automation System
CMM	Collaborative Manufacturing Management
CPG	Consumer Packaged Goods
CPM	Collaborative Production Management
CRM	Customer Relationship Management
DCS	Distributed Control System
DOM	Design, Operate, Maintain
EAM	Enterprise Asset Management
ERP	Enterprise Resource Planning
HMI	Human Machine Interface
IOp	Interoperability
IT	Information Technology
MIS	Management Information System
OpX	Operational Excellence
OEE	Operational Equipment Effectiveness
OLE	Object Linking & Embedding
OPC	OLE for Process Control
PAS	Process Automation System
PLC	Programmable Logic Controller
PLM	Product Lifecycle Management
RFID	Radio Frequency Identification
ROA	Return on Assets
RPM	Real-time Performance Management
SCM	Supply Chain Management
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.

This research has been sponsored in part by Profibus International. However, the opinions expressed by ARC in this paper are based on ARC's independent analysis.

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 membership 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 pages at www.arcweb.com

ARC
arcweb.com

3 Allied Drive   Dedham   MA   02026   USA   781-471-1000

Boston, MA | Washington, D.C. | Pittsburgh, PA | Phoenix, AZ | San Francisco, CA
Cambridge, U.K. | Düsseldorf, Germany | Munich, Germany | Hamburg, Germany | Paris, France | Tokyo, Japan | Bangalore, India | Shanghai, China