ARC WHITE PAPER

By ARC Advisory Group

MAY 2009

HIMA's Next Generation Safety Controller Maximizes Availability for Demanding Process Applications

HIMA Delivers Safety Solutions for Applications That Require the Highest Degree of Availability, Such As Those with Environmental Risks

Redundancy Level	Architecture	Advantages	Typical Applications
1	Single inputs, CPU, single outputs	Meets functional safety requirements at low cost	All applications requiring functional safety but not high availability
2	Redundant inputs, CPU, outputs	Most common configuration for absolute safety and availability	Chemical, petrochemical, popular in Europe
3	3x redundant inputs, CPU, outputs	Traditional configuration for customers who require TMR technology	Chemical, petrochemical, popular in North America
4	4x redundant inputs, CPU, outputs	One application for protection against common cause failures	Refinery, tunnels

HIMax Offers SIL3 Protection Using Various Levels of Redundancy

Executive Overview

Process 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 high-level 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). However, in the process industries, no metric is more important than productivity. To achieve productivity, a process system must be "highly available" to guarantee the operation of a process for which a sudden shutdown due to a component failure would be dangerous or extremely expensive.

Process safety has evolved from being a cost burden and necessary evil to a strategy for improving productivity by enabling process optimization on-the-fly and increasing availability.

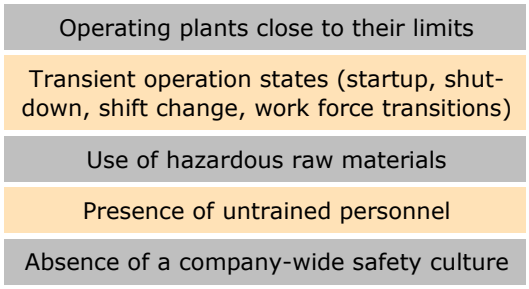
The nemesis of all continuous processes is unplanned stoppage resulting from controls malfunction, equipment failure, or operator error. System availability can be improved significantly through the use of redundant control architectures – especially those that allow hot-swapping or on-the-fly program changes. Modern process safety solutions provide comprehensive diagnostics that help users to recognize safety-critical situations and act quickly and accordingly to avoid unnecessary system shutdowns.

HIMA, an automation supplier specializing in safety systems, has spent five years developing and testing the HIMax, a new generation of process safety controller targeted at high-end applications, and recently released it for general sale. While designing the HIMax, HIMA engineers paid close attention to customers' wishes to come up with a modern, advanced solution for process industry users seeking high availability.

Why Invest in Process Safety?

Process safety refers to managing both physical and human assets to minimize the likelihood and consequences of catastrophic incidents in facilities that handle, process, or store hazardous materials. It is a dynamic concept involving the interaction and integration of technology, materials, equipment, and personnel. The unexpected release of toxic, reactive, or flammable liquids and gases in processes involving hazardous chemicals

has occurred again and again in recent decades. Unfortunately, this has resulted in loss of life and catastrophic environmental damage, as well as destruction of expensive assets and long-term production losses. Process users recognize that risks can be mitigated, but not eliminated. Regardless of the industry, an accidental release can occur any time hazardous chemicals or their manufacturing processes are not properly controlled and monitored.



Factors that Increase Risk

The concept of process safety has evolved and profited in recent years from technology improvements and the harmonization of international standards. Process users have gone from an *ad hoc,* component-based approach, to a fully developed holistic view of a potentially hazardous situation based on established best practices and supported by internationally recognized standards. Through this process, leading process manufacturers have learned to weigh the costs of process safety against its benefits and risks. This help users to justify investments in safety technology, to develop and nurture an enterprise-wide safety culture, and most importantly, to view a process safety solution as a productivity tool in pursuit of Operational Excellence, rather than as an unavoidable expense.

Availability vs. Functional Safety

The traditional purpose of process safety solutions is to protect people, equipment, and the environment from damage by ensuring Safety Instrumented Functions (SIF). In a modern sense, however, process safety also contributes significantly to the availability of process assets, which can have a significant impact on a plants overall profitability.

High availability is made possible by fault tolerance. This is the ability to maintain control functions even in the case of partial equipment failure. High availability is important in applications in which interrupting the process could cause extensive damage or, for continuous processes, for which a restart would cause expensive delays (or create safety issues of its own). Achieving high availability on the order of 99.99 percent requires the use of a modern, redundant and fault-tolerant safety architecture to ensure that continuous processes cannot be interrupted.

Functional safety, on the other hand, ensures safety functions in order to prevent personnel from being injured by de-energizing moving machine

parts or by switching them into a safe state if a safety barrier is compromised. A characteristic measure for a safety function is the 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 with hazardous materials.

Process Safety as a Productivity Tool

In today's challenging economic environment, process manufacturers are under pressure to contribute value to the bottom line by maintaining or improving the performance of process assets. Unexpected interruptions of critical processes may not only damage equipment and ruin production material; they can also lead to catastrophic explosions, for example if an endothermic process goes out of control. Restarting a process such as the production of paper or polymers may result in producing lower grade or off-spec product until the process can be re-optimized. Modern process safety solutions can significantly reduce these economic risks by helping users to recognize safety-critical situations quickly and to implement appropriate measures while avoiding unnecessary shutdowns.

Independent failures	Minimize risk of simultaneous failure of controller and SIS (no common cause failures)
Security	Prevent changes in control system from causing change in or corruption to SIS
Controller requirements	SIS is designed to fail in a safe way while DCS is designed for maximum availability
SIS safety features	An SIS offers extended diagnostics, special software error checking, protected data storage and fault tolerance

Justification for a Separate Safety Control System

The Costs and Risks of Not Ensuring Safety

Risk is defined as the product of the probability and the severity of an unplanned incident. In other words, how often can an incident occur and how bad are the consequences if it does occur? Examples of risks in process manufacturing operations include injury to personnel, environmental damage, loss of capital equipment, and loss of production. For many manufacturers, damage to their corporate image can also be a significant risk factor. Add to these issues the realities of increased environmental awareness, stricter government regulations, and threat of litigation, and it is easy to see why risk management is becoming increasingly important to process manufacturers.

Many companies have seen their public image suffer in recent years due to negative publicity from product recalls and boardroom scandals, resulting in a loss of trust in the public eye. From the Union Carbide Bhopal tragedy in 1984 to the BP Texas City explosion in 2005, these experiences have taught companies the importance of improving their "good neighbor" image by actively promoting adherence to good manufacturing practices and compliance with environmental and occupational safety best practices. In an increasingly social 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 many companies, this has resulted in the implementation of a complete safety culture that enhances safety by nurturing an open, communicative environment and rewards employees who take responsibility for safety.

Besides image challenges, process 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. Here, companies can at least demonstrate their "best faith" by documenting compliance with all generally accepted industry practices. While the harmonization of standards has lessened the workload, the burden of proof of compliance still lies with the end user.

The Importance of Risk Reduction

The best way to reduce risk in a manufacturing plant is to design inherently safe processes. However, inherent safety is rarely achievable in today's manufacturing environments. Risks prevail wherever hazardous or toxic materials are stored, processed, or handled. Since it is impossible to eliminate all risks, a manufacturer must decide on a level of risk that they consider tolerable. After identifying the hazards, a hazard and risk study is typically performed to evaluate each risk situation by considering its likelihood and severity. Site-specific conditions, such as population density, in-plant traffic patterns, and meteorological conditions, are often considered during risk evaluation.

Growing aware of and compliance with international safety standards

Obsolescence of legacy technology

High profile industrial incidents and disasters

Increased investments in oil & gas

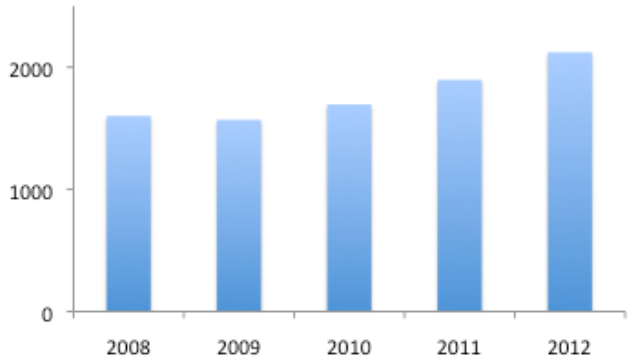
Strong growth in BRIC countries

Process Safety Market Drivers

Once the hazard and risk study has ascertained the risks, it can be determined whether they are below acceptable levels. Basic process control systems, along with process alarms and facilities for manual intervention, provide the first level of protection and reduce the risk in a manufacturing facility. Additional protection measures are needed when a basic process control system does not reduce the risk to a tolerable level. These include safety-instrumented systems along with hardware interlocks, relief valves, and containment dykes. To be effective, each protection subsystem must act independently of all others.

Investment in Safety Systems is Robust

The market for safety systems remains strong, driven by demand from the oil & gas and refining industries. Even though current crude oil prices are once again relatively low, long-term trends suggest that prices will rebound. This, combined with rising demand for oil and gas in the fast-growing BRIC countries (Brazil, Russia, India, China) are fueling new investments in oil and gas production and refining, helping to boost SIS sales. According to ARC's research, worldwide growth for safety systems, which has been hovering around 13 percent annually, will likely maintain positive growth through 2010, despite difficult economic times.



The Market for Process Safety Systems Remains Robust Thanks to Strong Demand in Oil & Gas (Market Size in $ Million)

An investment in a safety system cannot always be justified in terms of return on investment (ROI). Instead, it is more akin to buying an insurance policy. It is a sunk cost -- a form of negative opportunity cost set against the much higher cost of not having done enough to prevent an accident. However, such an investment can be justified by its contribution to bottom-line profitability through higher availability over the entire lifecycle of an asset and greater production efficiency.

Overview of HIMax

HIMA, a leading supplier of process safety systems, has a long and well-established reputation in the process industries for providing standalone

and integrated safety solutions. In 2008, HIMA introduced HIMax, a next-generation SIL3 platform that supports uninterrupted system operation throughout the whole lifecycle. Based on the company's highly available "XMR" architecture, HIMax is targeted specifically at users in the refinery, chemical, and petrochemical industries, whose processes require a greater degree of availability than previously available on the market.

The XMR architecture is scalable for SIL3 applications ranging from those needing no redundancy to applications requiring double or triple redundancy for inputs, outputs and CPUs, and up to quadruple redundancy with common cause protection (physically separated redundant components). The latter addresses the growing requirements in refining applications, such as steam crackers, and allows continued operation even if one control room is damaged or destroyed by fire or flood.

What Process Safety Users Want

While designing the HIMax platform, HIMA spent considerable time talking to process users to identify what they desire in a future safety solution. At the top of users' lists was uninterruptable operation – the ability of a system to tolerate "acceptable" faults, such as isolated component failures, without unnecessarily shutting down the whole system.

The HIMax is a SIL3 Safety Platform Designed to Deliver the Highest Degree of Availability.

Customers also felt that a safety system should contribute to their plant's performance rather than being just a cost factor. In terms of high availability, this means that processes must have the ability to be optimized on-the-fly by changing software or adding hardware components, or even updating the operating system, without having to shut down the system.

Finally, many process manufacturers today are faced with the challenge of having to do more with less. Pressure to cut costs from consolidations, restructuring and tighter capital spending budgets can undermine efforts to ensure process safety. For this reason, process users demand safety solutions that help them manage costs by minimizing CapEx and OpEx while maximizing usability. In short, users need to reduce engineering, start-up and maintenance time.

From its customer input, HIMA concluded that the ideal safety solution should contribute measurably to overall plant efficiency and productivity by guaranteeing availability. In addition, a flexible architecture should help to maximize system availability along the whole lifecycle by allowing customers to tailor the system to individual requirements to avoid overspending. Finally, a safety solution should fulfill its task of protecting workers and equipment from harm while appearing "transparent" to the process until it is needed.

HIMax: HIMA's Next-Generation SIL3 Platform

HIMax is a SIL3 platform designed especially for continuous processes that absolutely cannot be interrupted. The system maximizes availability, not only by ensuing continuous operation in the event of a component failure, but also by allowing the user to perform routine maintenance operations or hardware changes without shutting down the system. This includes every conceivable task, from hot-swapping components or modules to on-the-fly program and hardware changes, and even operating system updates. Redundancy levels from dual to quadruple are possible and each module is powered by its own separate power supply. A wide variety of I/O modules allows process users to scale each system to their particular needs.

Supported DCS Systems
ABB, Emerson, Honeywell, Invensys, Metso, Siemens, Smar, Yokogawa
Supported Comm Protocols
OPC (DA and A&E), MODBUS TCP, PROFIBUS & PROFINET, FOUNDATION Fieldbus, HART Protocol, TCP send & receive, ComUser Task

HIMax Integrates Easily with DCS Systems and Supports All Common Communication Protocols

As a standalone safety system, HIMax is designed to integrate seamlessly into all commercially available DCS systems including ABB, Emerson, Honeywell, Invensys, Metso, Siemens, Smar, and Yokogawa. Communication takes place using open protocols, fieldbuses and Ethernet including OPC, HART protocol, Profibus, Profinet, and Modbus. In addition, safe networks such as HIMA's own "safeethernet", Profinet with Profisafe, and Foundation Fieldbus' FF-SIS (when available) are also supported. To ensure a smooth integration, HIMA's DCS Competence Team is available to test and verify compatibility. The Team even takes over responsibility for the functional compatibility for turnkey solution projects.

The operating system supports full multitasking of up to 32 independent user programs. Each program has its own safety check sum, meaning that a part of the system can modified or expanded without influencing the oth-

er programs or causing a program to lose its safety certification -- an tant contributor to non-stop operation.

In addition, each task can be configured or monitored independently and assigned its own update time. This allows the user to optimize system performance between fast and slow tasks (e.g., time critical turbine machine control versus relatively slow burner management). With its large capacity, HIMax allows many tasks to be united in a single, central safety controller, helping to reduce upfront capital outlays and system integration costs while maintaining high levels of safety and availability.

HIMA has also improved system performance. With HIMax' improved processing speed and new statistical modeling for dynamic process control, variables can be sampled more frequently, allowing processes to be controlled more tightly and thus run closer to their limits. In many applications, even small improvements like this can have a huge impact on productivity, helping the safety controller contribute directly to the economic performance of process assets and improving a company's bottom line.

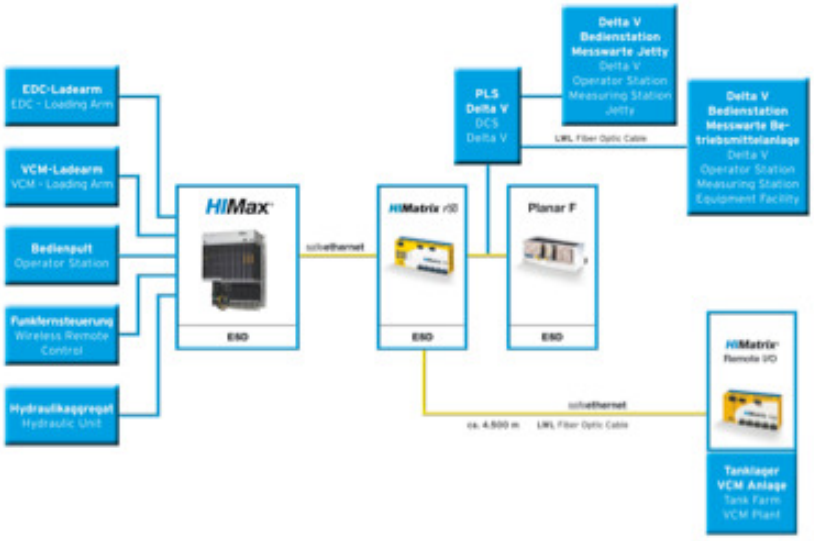
Case Study: INEOS Vinyls

Polyvinyl chloride (PVC) is petroleum-based polymer used in an endless variety of everyday products, from plastic bags to window frames. INEOS Vinyls, an English-owned chemical company, produces PVC at a plant on Germany's North Sea coast. The facility includes a dock at which ships can anchor and pump ethylene, ethylene dichloride and vinyl chloride via pipelines directly into onshore storage tanks. Automated loading arms perform the task of coupling and securing swivel joint pipes to the ship's tanks. The process is controlled and monitored via a Delta V system.

At INEOS Vinyls, the HIMax Guarantees System Availability During a Critical Loading Procedure that Transfers Chemicals from a Ship to Onshore Storage Tanks.

Pumping a chemical substance like ethylene dichloride from a ship at anchor is normally a routine and safe procedure. However, risks beyond the control of the operator, such as rough seas or maneuvering problems with the ship, could result in a chemical

spillage into the North Sea and must therefore be mitigated. To ensure safety of the loading process, INEOS recently upgraded an outdated system to the new HIMax solution from HIMA. In addition to monitoring typical process variables, such as temperature and pressure, the HIMax is responsible for executing the emergency separation procedure that decouples the pipelines from the ship to prevent or minimize spillage.



INEOS' Architecture Integrates a Single Redundant HIMax CPU with a Legacy DCS System.

For this application, INEOS chose a HIMax configuration with a single redundant CPU, over 200 digital I/O, and intrinsic safety isolators from Pepperl+Fuchs and Stahl (including broken wire monitoring), as well as pressure transmitters from Rosemount. Communication with the legacy Delta V system takes place via relays for status and emergency stop signals. While the coupling procedure can be controlled locally, it is most often performed from an onshore control room located over four kilometers away. For this communication, INEOS chose Ethernet over a fiber optic cable after previously having had problems with lightning strikes.

For INEOS, the greatest advantage in using the HIMax controller is not for continuous availability, but rather for guaranteed availability during the loading procedure, which may take a day or longer to complete. In addition, the strict separation of safety and non-safety programs gives INEOS

the flexibility to modify and expand functionality without invaliding the system's TÜV safety certification.

Another convenient HIMax architecture feature that INEOS uses is what HIMA calls "temporary redundancy." In the event of a failure of an input or output on a non-redundant I/O module, the company inserts a backup I/O module in a slot in another chassis reserved for this purpose. This module assumes the function of the defective card while it is being replaced. Redundant wiring terminals stand ready to allow a quick changeover to the temporary module. After the repair is complete, the hardware configuration is changed back to the original state using the replacement module. This feature is only possible on a system that allows such hardware configuration changes on-the-fly, without having to shut down the system.

INEOS has decades of experience with safety controllers from HIMA and other suppliers. For this ship off-loading application at its PVC production facility, the company chose the new HIMax controller primarily for its "non-stop" availability that provides a high degree of protection against environmental damage. Thanks to the success of this installation, INEOS has also specified HIMax for other applications at the same plant as well as at other INEOS facilities.

Case Study: Evonik Degussa

Evonik Degussa is Europe's largest producer of carbon black, a color pigment commonly used in the tire industry. A by-product of the production process is a gas used to fire a boiler for steam and power generators in the same facility. Should a fault occur in one of the boilers, excess gas from the carbon black production is simply burned off with a flare until operation is resumed.

For the burner control system, Evonik Degussa employed a Foxboro IA series controller coupled to a Triconex safety controller. However, over the years the aging Triconex system was becoming more and more expensive to maintain in terms of repair and training. For this reason, the company decided to upgrade the system to HIMA's new HIMax safety controller.

The HIMax system is charged with the task of ensuring uninterrupted operation of the pre-aeration, flame monitoring, and other important process activities. The application employs redundant HIMax CPUs, two system bus modules, two digital input modules, and three digital output modules, as well as a communications module for Profibus DP. The latter provides open communication to the existing Foxboro process control system in place of a proprietary connection used with the Triconex system. HIMax fulfills the G3 standard (conformal coating, ANSI/ISA-S71.04 G3 und DIN EN 60068-2-60) and can therefore be deployed in such a dirty environment.

Evonik Degussa Chose HIMax for its Ability to Maintain Non-Stop Operation During Maintenance Work or Software or Hardware Changes.

Evonik Degussa chose HIMax because of its ability to maintain non-stop operation, even during maintenance operations or the occasional software or hardware change. According to the company, this flexibility results in lower costs over the entire system lifecycle. Another advantage that the company appreciates is the user-friendliness of the SILworX engineering tool that combines programming, configuration, and diagnostics in a single environment. Plant engineers claim that its user interface helps avoid programming errors and shortens engineering and commissioning time.

Last Word

Process safety has become an increasingly important topic for process manufacturers in recent years, spurred on by evolving business and technical drivers. To put safety's benefits and costs into perspective, manufacturers should re-assess the role that safety plays in their production strategy and learn how new technologies can not only ensure safety, but also help improve business goals.

HIMA's next-generation HIMax process safety control system addresses the demanding needs of process users in the oil & gas, refining, and chemical industries by providing a previously unattainable level of high availability and system performance. HIMA achieves this with a redundant, scalable architecture that can be easily integrated with all commercially available DCS systems. The result is a higher guarantee of system availability coupled with a performance level that lets users runs processes closer to their limits, resulting in higher overall productivity from process assets.

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 Rate
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.

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

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