AN ADVERTISING SUPPLEMENT TO

APRIL 2013

CONTROL

PROMOTING EXCELLENCE IN PROCESS AUTOMATION • CONTROLGLOBAL.COM

Your Best Safety Shape Ever!

Achieve and Maintain Unprecedented Levels of Safety System Performance

Take the Safety Fitness Test

Plan for Safety System Success

Stay Fit for the Safety Lifecycle

SPONSORED BY

ABB

PutmanMedia®

Contents

Your Best Safety Shape Ever

Bring Your Safety Instrumented Systems to Unprecedented Levels of Performance

January 15, 2012, didn't start out well for Luis Duran. A veteran runner of road races across a range of distances, Duran found himself well off his accustomed pace in the Aramco Half Marathon in Houston. As the miles slid slowly by, he ticked off the reasons: He didn't update his training plan. He knew he hadn't logged the necessary mileage or even gotten out the door as frequently as he should have. He didn't cross-train or stretch as much as he had planned. And he was even wearing last season's running shoes. Business travel and family commitments had simply got the best of his training discipline this time around, and when race day came he simply wasn't as prepared as he wanted to be.

Fortunately, Duran doesn't run for a living. Like most of the rest of us, training, road races and other weekend athletic pursuits are for him but a means to an end: a sound mind and fit body that are better prepared to handle whatever unexpected obstacles life throws his way. Duran's day brightened: He wouldn't record a personal best at this half marathon, but he had found an apt analogy to use in his working life, as a safety instrumented system (SIS) specialist for ABB.

THE ROAD BACK TO SAFETY FITNESS

What struck Duran that warm January day in Houston is that safety system preparedness is a lot like athletic fitness. Planning, preparation and the right equipment all contribute to successful athletic performance come race day. Safety system performance demands much the same discipline, but with an added dimension of vigilance: by design a safety system's "race day" can come any time, day or night, in the course of otherwise routine plant operations.

The road to restoring and maintaining tip-top safety system fitness may well start with the admission that your plant's protective systems—and the work processes that support them—may have suffered neglect in recent months and years. And like a runner returning from a long layoff, a visit to the doctor in the form of an assessment of current safety system fitness is the first order of business when it comes to getting back on track. This includes a full reckoning of updated process conditions, risk factors and risk reduction strategies—together with a thorough evaluation of the ability of existing layers of protection to bring risk down to a level deemed in safety parlance to be "as low as reasonably practical" (ALARP).

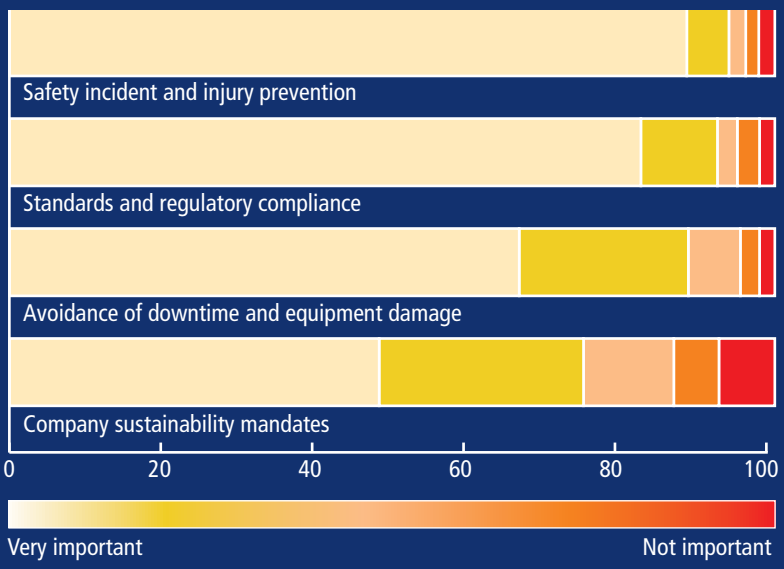
SIS FITNESS CRITICAL, BUT NOT EASY TO MAINTAIN

In order to gauge current industry views on safety instrumented systems, *Control* together with ABB conducted in late 2012 a reader survey across *Control*'s database of process automation professionals.

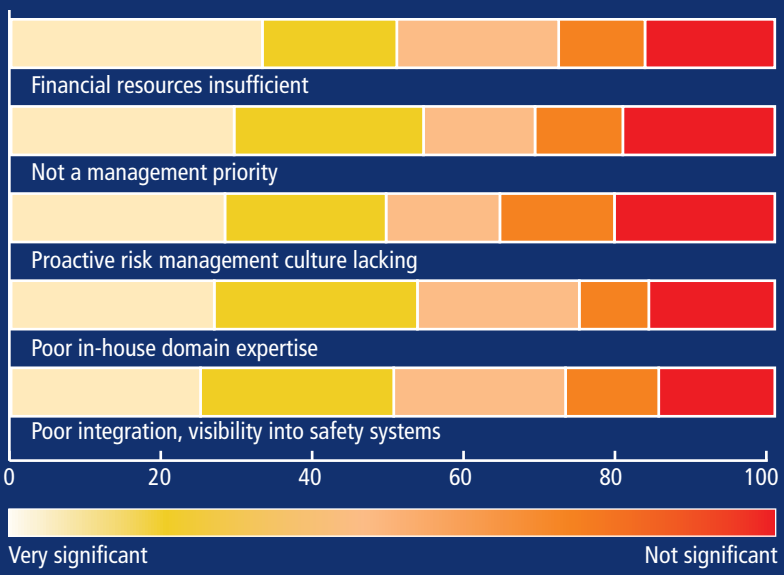
The more than 240 survey respondents acknowledged that their plants' safety instrumented systems (SIS) practices are shaped by a range of critical corporate goals, including personal safety, regulatory compliance, preventing downtime and equipment damage, as well as company sustainability mandates.

Yet they also admitted that a range of factors were obstacles to maintaining safety system performance, including insufficient financial resources, lack of management prioritization, underdeveloped risk management culture, lack of in-house expertise and poor integration and visibility into safety systems. Other data from this exclusive study is included throughout this special report.

Importance of Safety Systems Is Undiminished...



...Yet Obstacles to Safety Assurance Remain



Once you know where you stand, it's time to set goals and develop a new training plan that acknowledges where you are and where you need to be on the safety performance scale. To help make his fitness goals more tangible, our lapsed runner might put a specific upcoming race on his calendar and set a target pace and finishing time. Similarly, your safety fitness goals should take into account your plant's latest key performance indicators (KPIs) in the form of production rates, quality standards and environmental measures. With these updated parameters in mind, revisit the safety integrity level (SIL) requirements of your processes. Understand the gaps between the current and desired ability of your systems and processes to reduce risk, and you're ready to formulate a plan of attack.

As your safety training plan takes shape, it should leverage

the latest training methodologies (notably the IEC's 61508 and 61511 safety system standards) as well as the latest technologies available in the marketplace. Safety instrumented system technology, in particular, has advanced by several generations since the first programmable systems were developed and deployed in the 1970s and 1980s. Consider the technical clothing and advanced materials of today's running shoes—not to mention GPS watches and MP3 players now at our runner's disposal. They're a far cry from the then state-of-the-art Waffle Trainers and Walkmen of a few decades ago.

Indeed, the ability of today's integrated safety systems to address risk—even while reducing costs and improving engineering and operational productivity—can help bring your plant to entirely new levels of safety performance. So, even if our middle-aged runner feels a new personal record is out of reach, with modern safety system technology even an older plant is subject to no such arbitrary constraints. Further, any safety fitness plan must adequately account for the "obsolescence risk" entailed by staying with an older safety system that may perform adequately today—but for which spare parts and qualified personnel are in dwindling supply.

Another common thread between achieving safety performance and race-day preparedness is the discipline to translate your training plan into reality. Plan the work, work the plan, and, once you've arrived, make sure to cultivate the new habits, the new work processes that will help you continue to function at that same high level. Just as training logs are *de rigueur* for athletes looking to improve their physical performance, today's safety system standards emphasize the importance of documentation in the form of functional safety management systems (FSMS) at each step along the safety system lifecycle—from risk analysis to design and engineering through operations and maintenance activities. This means ensuring the FSMS compliance of your system providers and engineering firms, as well as day-in, day-out adherence to maintenance and proof-test schedules that if disregarded can cause hard-won gains in safety system performance to slip over time.

HELP FOR THE JOURNEY

So, you may say, this all sounds great in theory. But how do I figure out how to get started?

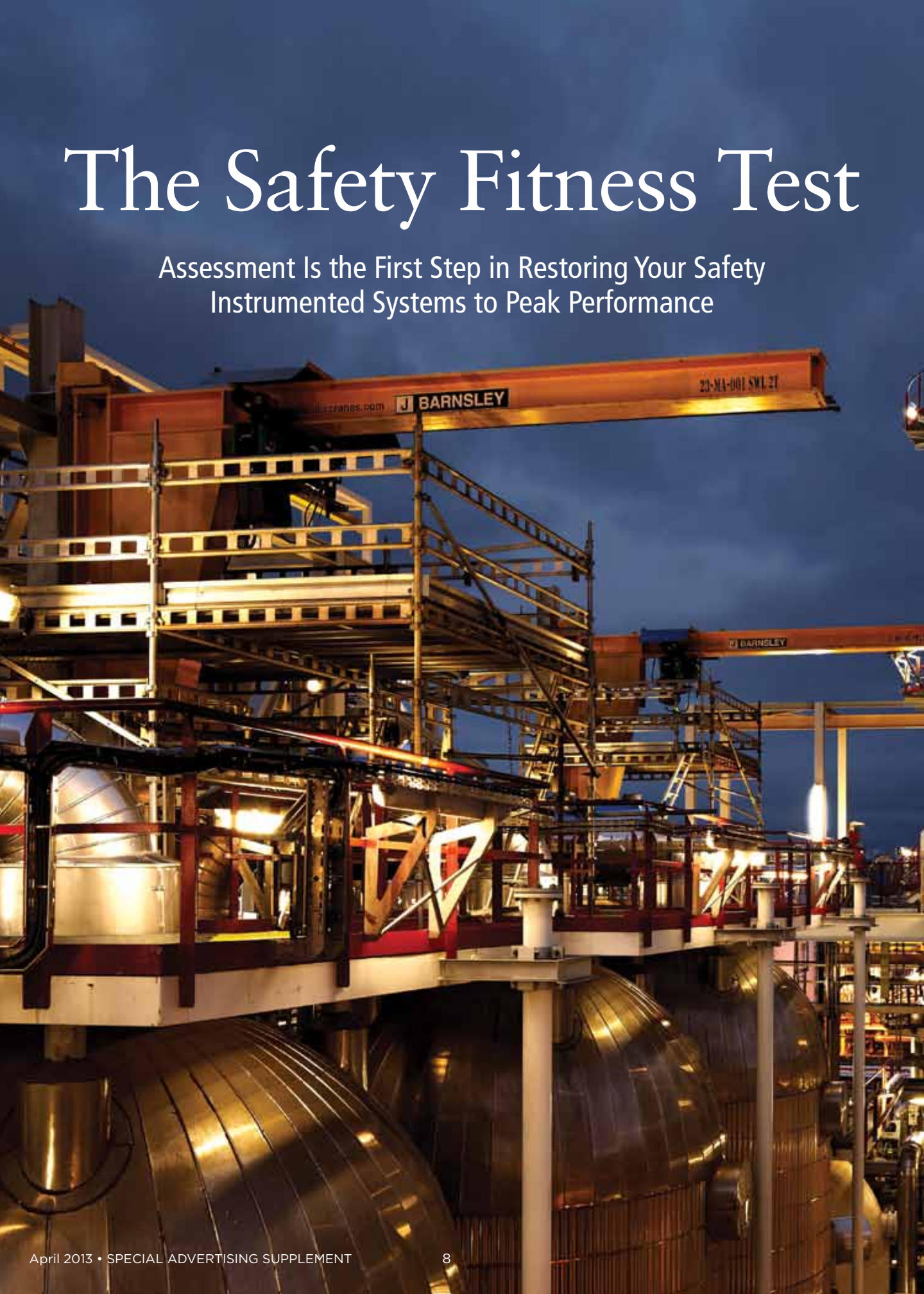
ABB, as a pioneer in the development of safety systems for industrial applications, has more than 30 years experience in their design, manufacture and implementation. With operations on all continents and dedicated safety system teams around the world, ABB has the expertise to support operating companies and engineering firms through all phases of the safety system lifecycle.

ABB's current safety system flagship, the System 800xA High Integrity, can function as a stand-alone SIS complement to an existing distributed control system (DCS) or, for maximum benefit, work hand-in-glove with its System 800xA automation platform in its execution of basic process control system (BPCS) and other process information management tasks.

Assess and plan, implement and maintain. Each of the remaining articles in this special report discusses in greater detail the essential activities needed to keep your safety systems in tip-top shape—and how services and technology from ABB can help make your safety performance goals an achievable reality at every stage of the journey. ●

The Safety Fitness Test

Assessment Is the First Step in Restoring Your Safety Instrumented Systems to Peak Performance

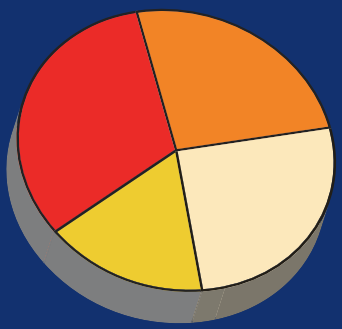


The first step in any athlete's performance improvement plan is a thorough assessment of his current fitness level. The baseline abilities of muscle, heart and lung must be evaluated—perhaps in consultation with a medical specialist—to establish the baseline readiness of core systems to respond to new training demands. Our runner's current fitness level, together with his ultimate performance goals, will identify the gaps to be addressed through an updated training plan.

In the case of our plant's safety systems, the assessment phase begins with a thorough updating of process conditions and risk factors. Safety fitness (risk reduction) goals should take into account the plant's latest key performance indicators (KPIs) in the form of production rates, quality standards and environmental measures as well as any configuration changes that may have impacted the safety system's ability to effectively reduce risk.

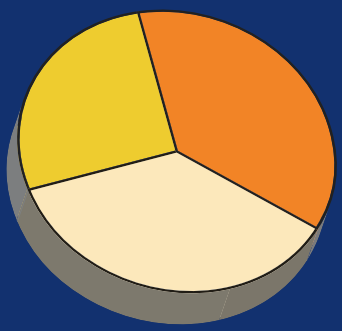
MUCH WORK REMAINS FOR INDUSTRY COMPLIANCE

In a recent study of *Control* readers, we asked about familiarity with the IEC's 61511/ISA 84 safety instrumented systems standards and their company's compliance with their requirements. Roughly half of the predominantly North American audience indicated compliance of their systems with the standard or under the ISA 84 grandfather clause. Roughly a third of those respondents who indicated their systems were not yet compliant indicated their companies had established a roadmap and timeline, while another third indicated that compliance had made their to-do lists. A full quarter of respondents indicated no plans for compliance.



Compliance Is Spotty at Best…

- Fully compliant 25.1%
- Grandfathered 26.4%
- Not compliant 16.3%
- Not sure 32.2%



…But Need Is Understood by Some

- Have established roadmap and timeframe..... 36.8%
- It's on the to-do list 36.4%
- We have no plan..... 26.8%

GET UP TO SPEED ON INDUSTRY STANDARDS

Next up for our runner is a review of the latest training methodologies, which for our plant's safety instrumented systems means the IEC's 61508 and 61511 standards and other applicable codes. Importantly, some two-thirds of safety instrumented systems in use today predate these standards.

And while the U.S. implementation of IEC 61511, ANSI/ISA 84, includes a "grandfather clause" for older systems, its insistence that operating companies ensure that safety systems are "designed, maintained, inspected, tested, and operating in a safe manner" leaves no room for less-than-rigorous safety system discipline.

Further, although the IEC SIS standards are not legal requirements *per se*, their growing acceptance as descriptors of industry best practices means that non-compliance may have very real liability implications in the event of an incident. And in some regions and industries, compliance already carries the force of law. On the other side of the ledger, demonstrated compliance can help operating companies to reduce insurance premiums.

Purposely non-prescriptive in nature, the IEC safety standards outline a holistic methodology for

HELP WITH YOUR SAFETY FITNESS ASSESSMENT

Whether evaluating your plant's current safety performance or the requirements of a new process, ABB understands that operating companies don't always have on staff the qualified personnel they need to properly evaluate the ability of their current safety systems and work practices to properly address and manage risk. To help address each user's particular needs, ABB offers a range of broad range of relevant assessment services:

- Hazard and risk management
- Risk modeling
- Process safety management systems
- Behavioral safety and culture
- Process hazard reviews (PHR)
- Hazard & operability (HAZOP) studies
- Mechanical integrity and asset life assessment
- Determination of safety integrity level (SIL) requirements
- Computer hazard and operability (CHazop) analysis
- Hazardous area risk assessment and classification
- Environment impact assessment
- Occupied buildings risk assessment

managing every stage of a safety systems' lifecycle—from risk analysis and design engineering through operations, management of change and decommissioning. Elements specifically relevant to safety systems performance assessment include adherence to accepted risk evaluation and mitigation methodologies such as process hazards analysis (PHA), hazards and operability (HAZOP) analysis, and layers of protection analysis (LOPA).

REVISIT SIL REQUIREMENTS

In light of the updated process performance parameters mentioned above, revisit the safety integrity level (SIL) requirements of your processes as well as the ability of safety instrumented functions (SIFs) implemented in preventive and protective layers to continue to adequately reduce risk. Further, ensure that the day-to-day operational discipline (maintenance tasks and proof tests) are being routinely executed at the proper intervals.

When evaluating safety risks, don't overlook the obsolescence risk presented by older safety systems that may be at or near the end of their supportable life, whether through the dwindling availability of spare parts—or of personnel qualified to maintain them. Indeed, today's integrated safety system technology can help reduce risk by unifying the plant's basic process control system (BPCS) and SIS engineering and visualization tools so that the plant's preventive and protective layers both perform more effectively.

The IEC's safety system standards strongly emphasize the importance of documentation at all lifecycle stages, notably the need to develop and maintain over time a clear and unambiguous functional safety requirements specification (SRS). And, much like the more familiar ISO 9000 series of quality standards, the ongoing integrity of safety system performance is to be assured at all lifecycle stages through the implementation of functional safety management systems (FSMS).

Competence and security are two additional aspects of SIS performance specifically addressed in the latest IEC standards and should be addressed in the course of any safety system performance assessment. This includes the documented competence of individuals and organizations involved with all aspects safety instrumented systems work as well as the inclusion of security threats in risk analysis methodologies. ●

Services for the Safety Fitness Lifecycle

While the IEC's 61508/61511 standards define in much greater detail the full lifecycle of a safety instrumented system (SIS), it's useful to group SIS activities in three sets of continuous activities that are not unlike an athlete's drive to improve performance through repeated cycles of assessment and planning, training and maintenance. ABB, as a pioneer in the development of safety systems for industrial applications, has service operations on all continents and dedicated safety system teams around the world to support operating companies and engineering firms through all phases of the safety system lifecycle. This figure demonstrates the breadth and depth of their offering.

ABB

ASSESS

- Hazard and risk management
- Risk modeling
- Process safety management systems
- Behavioral safety and culture
- Process hazard reviews (PHR)
- Hazard & operability (HAZOP) studies
- Mechanical integrity and asset life assessment
- Determination of safety integrity level (SIL) requirements
- Computer hazard and operability (CHazop) analysis
- Hazardous area risk assessment and classification
- Environment impact assessment
- Occupied buildings risk assessment

MAINTAIN

- Reliability and operations improvement
- Modifications, upgrade management
- Brownfield project delivery
- 24/7 service level agreements
- TUV certified service organizations
- Functional safety management systems
- Performance assurance
- Testing and repairs
- Operating and maintenance procedures
- Training

ADDRESS

- Pressure relief design and calculations
- Safety instrumented system specifications
- Detailed design for up to SIL 3 requirements
- Safety instrumented system delivery
- Engineers with competence certified by TUV
- TUV-certified Safety Execution Centers around the world
- Functional safety management systems
- Comprehensive systems methodology and documentation
- Commissioning
- Validation

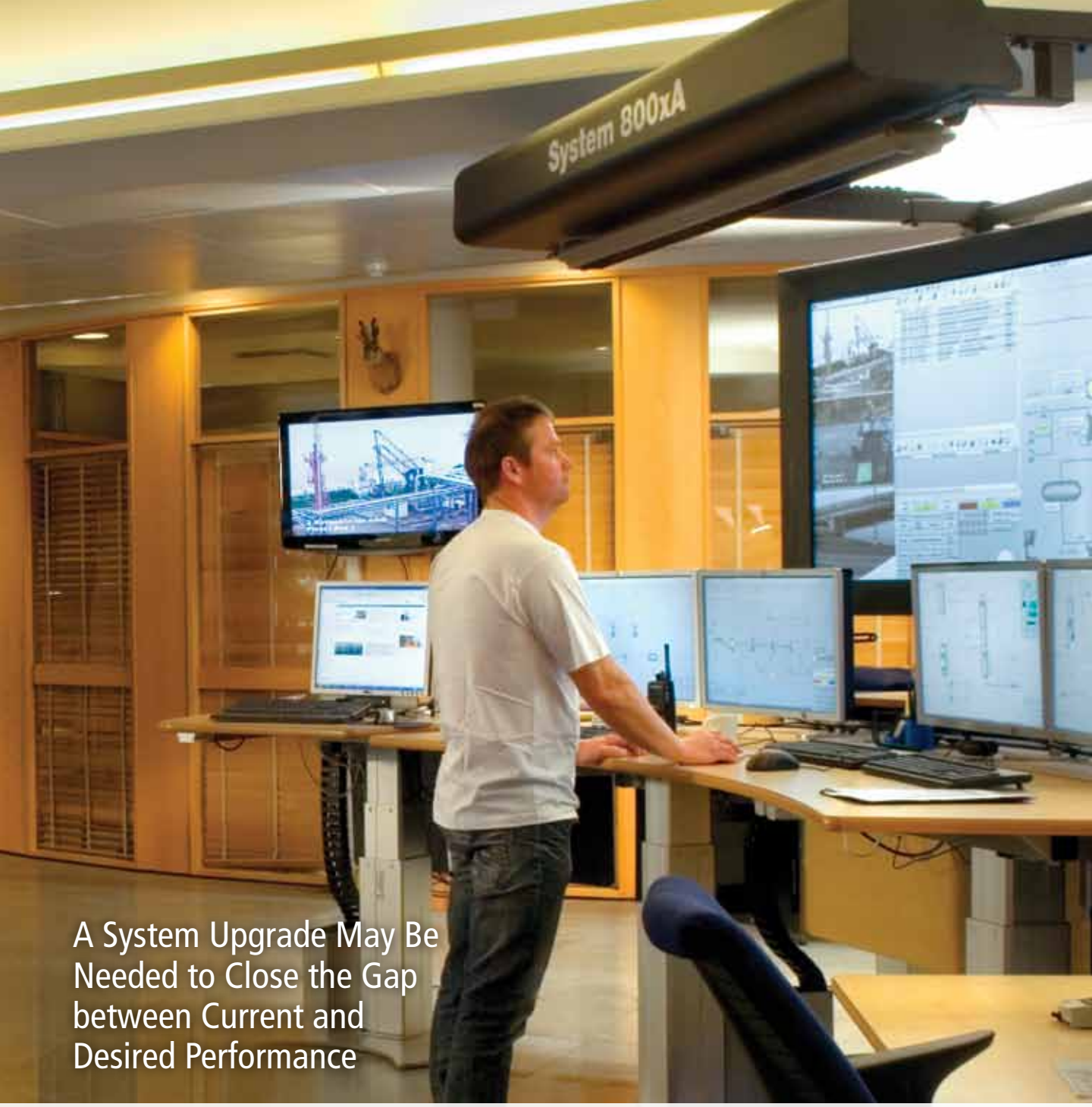
- Organizational culture/change
- Human reliability assessment
- Safety critical procedure assessment
- Staffing levels and workload assessment
- Pre start-up safety review
- Legacy systems review
- Control room performance assessment
- Alarm management health check
- Management of change auditing
- Mechanical integrity auditing
- Incident investigation support

Plan for Safety System Success

Whether you're a weekend runner gunning for a 5k personal record or an aspiring Olympian with her eye on the medals stand, understanding one's current capabilities is a necessary first step in realizing one's athletic performance goals. Similarly, the first step in achieving—or restoring—the performance of your plant's safety systems begins with a cold-eyed assessment of their current capabilities. Only then can you begin to develop a plan to bring your safety systems to the desired level of performance.

The previous article in this special report ("The Safety Fitness Test", p9), discussed how to go about assessing the current risk-reduction capabilities of your plant's safety systems, and identifying gaps relative to goal. In this article, we'll focus on applying new safety system technology as a first step toward bringing performance back up to speed.

Among the first go-to solutions in the runner's toolkit is an upgrade to supporting systems and technology—notably new shoes or technical clothing, perhaps the purchase of a new GPS watch or even the hiring of a new coach if funds allow. True, money alone won't solve your fitness problems, but



A System Upgrade May Be Needed to Close the Gap between Current and Desired Performance

it's hard to focus on building new speed when shin splits or chafing forces you off course, or you can't tell just how fast or how far that last tempo run was. Similarly, your safety fitness assessment may have pointed to the need to update the plant's safety instrumented systems. Choose the right supplier and engineering partner carefully to make sure this project is off on the right foot from the very start.

'PROVEN IN USE' COMPLIANCE

One of the key advances in safety systems practice promulgated in the IEC's 61508 and 61511 safety standards is the primacy of functional safety management systems (FSMS) for all organizations involved with safety instrumented systems work. This includes those organizations manufacturing the hardware and developing the software; those organizations engineering, installing, testing and validating them; and those organizations operating and maintaining them.

If your plant's safety systems were developed and installed under the aegis of the 61508 and 61511 standards, it's likely that standards compliance was mandated at the project stage. This means that the

systems and instruments themselves—as well as the development and engineering organizations behind them—were certified by a third-party agency to conform to the standards.

But for systems that predate the 61508 and 61511 standards (and necessarily their certification to them), standards compliance dictates that users demonstrate safety performance by "proven in use" criteria. This non-trivial task may include retroactively demonstrating the adequacy of the manufacturer's quality management systems in use at the time, a thorough inventory and description of systems components and sub-systems currently in use, and demonstrated performance of these components and sub-systems in similar operating profiles and physical environments. This accumulation of documented evidence must adequately demonstrate that your plant's safety instrumented functions (SIFs) as implemented meet the current safety integrity level (SIL) requirements of your process.

Further complicating the risk profile of older safety instrumented systems is the spreading obsolescence and scarcity of system components, and shortage of personnel qualified to work with them. Indeed, many systems currently in use are beyond their supplier's stated support terms. As a result, "proven in use" compliance or the grandfathering of an older system may be an adequate near-term plan, but continued safety performance will require that many of industry's safety fitness plans incorporate a full system update or upgrade in the not-too-distant future. Indeed, a recent report by the ARC Advisory Group indicates that some two-thirds of the safety systems in use today are at or near the end of their supportable lives.

SYSTEM UPDATE CONSIDERATIONS

For process plants with older safety instrumented systems, then, the outcome of any responsible safety fitness assessment and planning process is likely not whether to upgrade, but the timing of the inevitable. In the real world, of course, replacing a dated or soon-to-be-obsolete system must take into

HELP WITH SAFETY SYSTEM DELIVERY

Through its System 800xA portfolio and more specifically the 800xA High Integrity offering, ABB continues to focus on delivering integrated safety systems solutions worldwide. System 800xA facilitates a fully integrated and optimized system design while also allowing the user to tailor system design and integration concepts to meet plant-specific functional safety management requirements. Further, ABB offers a range of safety system design and engineering services through its Safety Execution Centers worldwide:

- Pressure relief design and calculations
- Safety instrumented system specifications
- Detailed design for up to SIL 3 requirements
- Safety instrumented system delivery, including for emergency shutdown, alarming, fire and gas applications
- Engineers with competence certified by TUV
- Safety Execution Centers around the world, certified by TUV
- IEC61508/61511-compliant functional safety management systems
- Comprehensive systems methodology and documentation
- Commissioning
- Validation

account risk factors but also financial, production and other resource constraints. But with the decision to upgrade finally made, users face quite a different technology landscape than even 15 years ago.

Today, the bid specifications for more and more new plants include not only compliance with the IEC 61508/61511 standards but also "integrated safety" as a base requirement. While at first blush this contradicts long industry practice of ensuring diversity by physically separating safety systems from basic process control systems, new technology together with users' desire to reduce costs and improve productivity are fueling an industry-wide movement to integrated systems.

Integration, or at least "interfacing," of safety instrumented systems with basic process control systems is in fact not a new practice. Indeed, the IEC standards' non-prescriptive language doesn't rule out even the physical integration of control and safety in the same box or on the same network. Rather, the standards assert that functional safety cannot be compromised by a failure or by maintenance activities associated with the basic process control system.

Diagnostics technology, meanwhile, has advanced in its ability to intercept dangerous faults, and some of today's integrated safety alternatives feature embedded diversity in hardware and software that reach all the way back to separate development teams. As a result, some of today's integrated safety system options can meet demanding SIL 3 application requirements even without the use of hardware redundancy.

"Process safety systems suppliers continue to cost reduce their hardware offerings and integrate their safety solutions with basic process control systems," wrote Barry Young, principal analyst for the ARC Advisory Group in a recent report on the global safety systems market. "Suppliers offering a truly integrated offering of process and safety are saving end users substantial project costs in engineering and lifecycle expense," he said.

With current technology a range of separate, interfaced or integrated solutions are possible among

process control system and safety system suppliers (see sidebar box below). The most highly evolved option—an integrated platform from a single supplier that is designed from the ground up to perform both safety and control functions—is typified by the ABB System 800xA process automation platform.

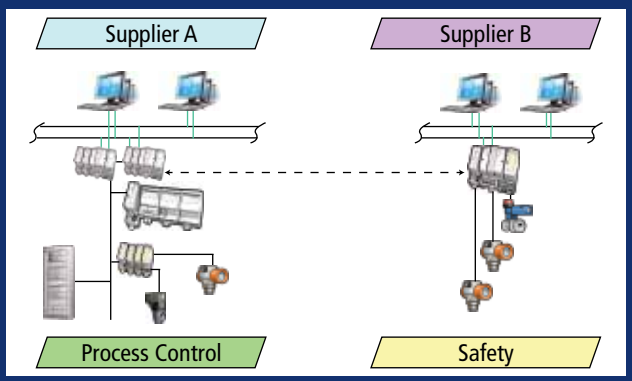
Because it performs as a single integrated system, it features both high- and low-level integration of control and safety system components without compromising the performance of either. Further, taken separately, the ABB High Integrity safety instrumented system can be deployed with control systems from other suppliers either in standalone mode or with top-end integration.

The 800xA platform with 800xA High Integrity safety system functionality features common engineering and visualization tools for both process control and safety functions, boosting both engineering efficiency and operator effectiveness. The integrated approach also allows functions such as information management, asset management and production management to be fully leveraged across the entire automation system. The ABB approach even enables certified safety controllers that can run both process control and safety applications simultaneously—a feature that in some high speed applications can both optimize safety and control performance while reducing capital and hardware needs.

ROBUST SAFETY WITH LOWER PROJECT COSTS

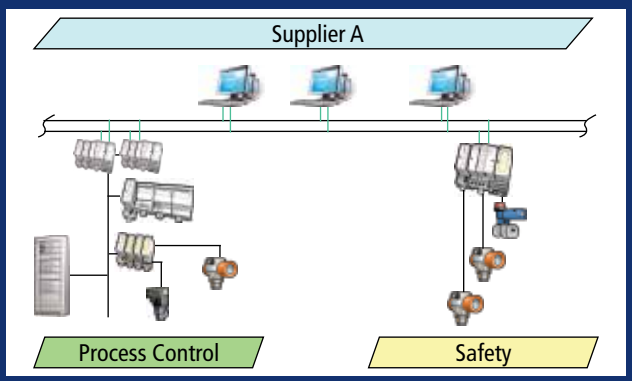
While the safety components of an integrated environment must adhere to the design, testing, validation and certification processes applicable to safety systems, an integrated approach to control and safety functions can cut capital costs by eliminating some redundant aspects of independent safety and control networks. A smaller system footprint, a unified engineering environment and elimination of a custom interface between the control and safety systems also contribute to project savings.

INTEGRATED SAFETY: THE FOUR ARCHITECTURE OPTIONS



TWO SUPPLIERS, SEPARATE SYSTEMS

A system architecture based on completely separate basic process control systems (BPCS) and safety instrumented systems (SIS) from different suppliers, typically with a limited, OPC- or Modbus-based link between the two systems, was once the preferred way to incorporate safety systems into the overall plant automation scheme. Physical separation and different development teams helped to minimize common cause and systemic failures, but a custom interface between the two systems introduces an additional set of development and maintenance concerns. Further, different engineering tools and HMI methodologies increase complexity and training requirements as well as limiting operational visibility and synergy between the two systems.



SINGLE SUPPLIER, DIFFERENT SYSTEMS, HIGH-LEVEL INTEGRATION

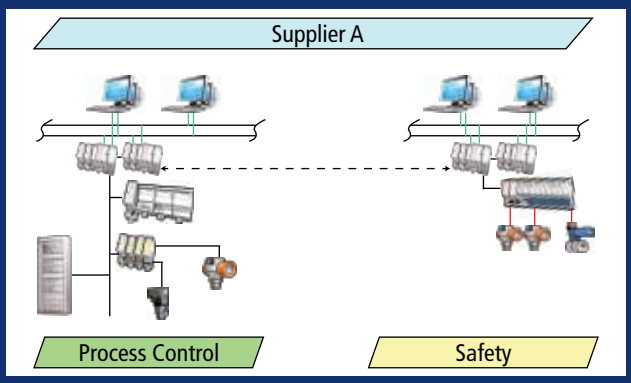
Another typical architecture is the result of an overall automation system delivery from a single supplier but with different BPCS and safety systems. Both systems are based on in-house products, but have been developed separately (or added to the product portfolio through acquisition) without any significant commonalities. The potential for common cause and systemic failures are addressed as with systems from different suppliers, but a common HMI and more rigorous connectivity will likely help operators be more effective and reduce interface maintenance costs. Engineering tools are likely to remains separate, however, allowing for little improvement with regard to training needs or productivity.

With the ABB System 800xA, users can decide how much separation to maintain between safety and process control. Even if fully segregated systems are chosen, many residual benefits apply. For example, potential sources of common cause failure already have been analyzed and minimized during the design phase by the development team and independently reviewed by the assessor during the certification of the product. This effectively makes the system smarter and safer from the day it's turned on.

Further, integrated testing is performed during the design validation and verification test, which includes network security as part of the test protocol. Version control, compatibility and interoperability testing are included in the release procedure. The result is a set of common best practices resulting in implementation of an integrated safety system that costs less, works better and even extends the capabilities of the process control system.

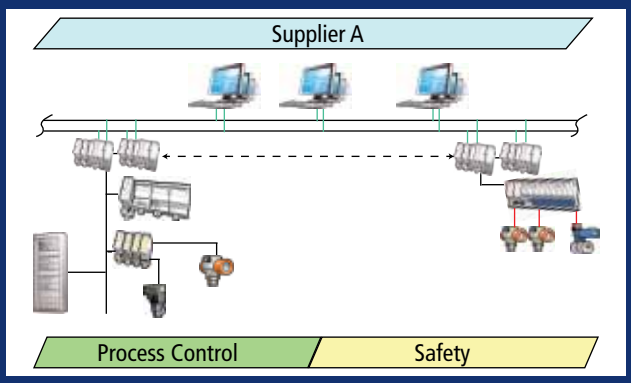
In the case of ABB's System 800xA, access control and security are built into the system as an off-the-shelf set of features, including user privileges, user action validation and a common audit trail. It also includes such extended capabilities as write protection, SIL access control and authorization, bypass management, and override mechanisms. The result is a robust set of security controls that apply uniformly across all systems.

As safety systems get replaced, or as new projects are developed, there is an opportunity to decide how you want to address safety in your operation—not just today but for years into the future. Integrated safety can deliver significant performance and cost benefits not only during the project phase, but during the entire operating life of the system. And that's the safety system lifecycle phase that we'll discuss in the final article in this series: Once your safety system is running at peak performance, how can you keep performance from degrading over the next 20 years it's likely to be in use? ●



SINGLE SUPPLIER, SIMILAR SYSTEMS, INTERFACED

Another system architecture option features similar systems from the same supplier, deployed as two separate systems for BPCS and safety functions. This approach requires that safeguards be in place on the supplier side to ensure that sources of potential common mode and systemic failures are identified, engineered out of the system design or otherwise addressed and managed. And while a similar set of engineering tools and operational displays will boost familiarity and reduce training costs, two separate systems—and all the management discipline involved with them—will need to be separately maintained, resulting in less than optimal engineering productivity. Also, since the two systems share a common heritage, the integrity of the communications link between the two systems should not be a concern.



SINGLE SUPPLIER WITH INTEGRATED SYSTEM

The final architecture option is a fully integrated BPCS and safety system, designed from the ground up to simultaneously satisfy the requirements of both realms. This option is based on, in principle, common hardware and software but using diverse technology and implemented as one system. In addition to sharing the advantages of separate but similar BPCS and safety systems (with similar qualifications), the integrated solution can further leverage the commonalities between the two systems. Common engineering tools and HMI reduce engineering times as well as contribute to more effective operations while maintaining functional independence. This approach allows information management, asset management and production management to be operated across the entire automation platform.

Safe for Life!

Once Safety System Performance Is Back on Track, New Work Practices and Feedback Mechanisms Can Help Keep It There

For most runners or other weekend athletes, preparing for that upcoming race on the calendar is really only an interim milestone: the ultimate goal is achieving a new fitness level to be enjoyed many years into the future.

Indeed, once race day has come and gone, our recovering runner's focus is likely to shift from a more aggressive, corrective action training plan to new exercise routines intended to keep those hard-won fitness gains from slipping away. A watchful eye on the exercise log and key metrics such as body mass index, resting pulse and other updated race results provide the continuous feedback our runner needs to tweak his routines in line with the changing demands of everyday life.

In much the same way, safety system performance over the "operate and maintain" phase of its lifecycle relies on disciplined work processes and feedback mechanisms to ensure that its abilities don't deteriorate over time, and that process changes don't subvert its abilities to adequately reduce risk.

FUNCTIONAL SAFETY MANAGEMENT IN OPERATION

A subset of the broader concept of the functional safety management systems (FSMS) concept described in the IEC 61508 and 61511 safety standards, FSMS for the operations and maintenance phase of the safety system lifecycle are intended to ensure that safety system preparedness is maintained over time and that any process or organizational changes are assessed for their potential to affect safety system performance.

In particular, the standards stress the importance of documentation in all aspects of safety system operations and maintenance. For example, the functional safety requirements specification (SRS) that is typically developed during the project phase of a safety system implementation should be updated and kept continuously current throughout the system's operating life.

Safety system proof tests and maintenance tasks—the frequency of which may play into the safety system's risk reduction calculations—must be performed thoroughly and on schedule. Training and qualification of employees also plays into the FSMS equation, as the competence of all individuals that work with the safety systems needs to be ensured.

A cycle for continuous improvement in safety performance also should be part and parcel of a plant's FSMS: processes should be in place to track any near misses, analyze them for root causes, and use the results to further improve safety system performance. The number of times that a safety system has tripped, or the number of hours spent in bypass mode, are other importance metrics making their way onto management's list of safety performance KPIs.

INTEGRATION'S LIFECYCLE APPEAL

Even with the best of intentions and management commitment, keeping safety system performance at that same high level month after month, year after year, can be an understandably daunting task. But just as the integration of safety and control functions in one unified platform can cut safety system project costs, it can also pay off big after the system is up and running. Indeed, the integration of safety with control and other plant information management tasks can help streamline the management of safety systems preparedness as well as improve operators' ability to head off escalating process conditions before automated intervention is needed.

In contrast, having two separate systems for control and safety increases maintenance effort as well as short-circuits the potential operational synergies to be gained from an integrated system. A byproduct of dated efforts to avoid common mode failures, the separation of safety and control systems also means that operators

SUPPORT SERVICES FOR LIFE

Once your safety instrumented systems are up and running, core to ABB's service offering is its Safety Sentinel program, an extension of its Automation Sentinel Lifecycle management program. Sentinel programs ensure optimal operation and availability of the installed safety system as well as access to software enhancements and 24/7 support and maintenance services. Other ABB services available during the operations and maintenance phase of your safety system lifecycle include:

- Reliability and operations improvement
- Modifications, upgrade management
- Brownfield project delivery
- 24/7 service level agreements
- TUV certified service organizations
- Functional safety management systems
- Performance assurance
- Testing and repairs
- Operating and maintenance procedures
- Training

ABB's consulting organization also can help with operational management and management of change assessments to make your safety systems—and the systems and organizations that work with them—as effective as possible:

- Organizational culture/change
- Human reliability assessment
- Safety critical procedure assessment
- Staffing levels and workload assessment
- Pre start-up safety review
- Legacy systems review
- Control room performance assessment
- Alarm management health check
- Safe systems of work
- Management of change auditing
- Mechanical integrity auditing
- Incident investigation support

and engineers must work on two systems throughout the system lifecycle, essentially doing double work to keep the systems in sync. Different suppliers for the two systems also can mean delays and finger-pointing when it comes to trouble-shooting problems.

Separate control and safety systems also mean different HMI screens and operational methodologies. If control room operators must take in information from several consoles, presented in various formats, decision-making can take longer and be less effective, potentially reducing the operator's ability to prevent a hazardous event from taking place or subsequently mitigate the impact of such an event.

A partial solution to this problem is a custom interface that combines information from the safety and process operating systems. Such interfaces, however, are notoriously expensive in both initial and lifecycle costs, and because each one is a custom effort there's little assurance it will work as well as intended. And training programs still must encompass two completely different systems, demanding additional time and resources.

THE CASE FOR ABB

Integrated systems, on the other hand, can provide a common interface to other vertically integrated system functions—safety and control as well as sequence-of-events capture, asset management and engineering/configuration tools. This sort of unified visibility has been shown to improve operational performance—as well as reduce the incidence of unwanted shutdowns—without compromising safety.

The concept of integrated safety and control is far from new. ABB, a long-time pioneer in both safety system and process automation technology, installed the first such large-scale system in 1984 on a North Sea oil platform, and has introduced four subsequent generations of technology—the latest being its 800xA High Integrity system in 2005. Already there are more than 2,700 successful installations of 800xA High Integrity operating worldwide, with an accrued five million hours of operation, and still not a single failure on demand.

Integrated safety and control from ABB: More effective operators, safer operations and lower project and lifecycle costs. Because there is no finish line when it comes to safety. ●

ABB Safety Systems. Integrated or integrated?

Absolutely.

ABB provides the enabling technology to integrate safety into the core of your operations. Regardless of your chosen approach, ABB has addressed the fundamental design elements required to maintain independent protection layers while fully integrating safety systems into our System 800xA DCS. Our integration capabilities enable operators to access safety related data seamlessly from a multitude of plant systems to perform their function, run the plant safely and make timely decisions in the case of abnormal conditions. For more information visit **www.abb.com/highintegritysafety**

ABB Process Automation Division
Visit us at our blog or on YouTube:
www.processautomationinsights.com
www.youtube.com/user/ABBProcessAutomation

Power and productivity
for a better world™

ABB