Process Safety: Building Safer, Smarter Oil & Gas Operations

More automation creates more complexity; the next step in process safety is making the whole safety architecture more connected, visible and resilient.

As Oil & Gas facilities become more automated, connected and complex, process safety must evolve from a collection of individual protection systems into an integrated, continuously observable and lifecycle-focused safety architecture. The article explores how technologies such as functional safety, intrinsic safety, diagnostics, system integration and remote monitoring can help operators manage this complexity while improving safety across both new and aging assets.

Author:
Gabriele Caglio, Customer Excellence Lead at GM International.

Process safety has traditionally been built around protecting individual equipment, functions and process steps. As automation and connectivity expand, that perspective is becoming too narrow. Safety increasingly depends on how the different elements of a facility behave as an overall architecture, and on whether information moves consistently between the systems that rely on it. This makes standardization increasingly valuable. Common communication technologies and clearly defined interfaces can reduce the complexity of connecting field instrumentation with control, shutdown and monitoring systems. Technologies such as Ethernet-APL, for example, are designed to bring standardized Ethernet communication into process plants and hazardous areas while simplifying access to field data.



Yet connectivity by itself does not make a facility safer. The effectiveness of a safety function still depends on architecture, independence, diagnostics, cybersecurity, validation and lifecycle management. IEC 61511 continues to provide the framework for safety instrumented systems across specification, design, installation, operation and maintenance. The future safety architecture will therefore be not only more connected, but also more standardized, transparent and manageable, giving operators a clearer view of system health and helping them act before small deviations become larger risks.



That greater visibility, however, comes with a corresponding need to control how systems interact. As more control, monitoring and asset-management functions become connected, digitalization can introduce new dependencies if system boundaries and levels of authority are not clearly defined. The objective should not be to restrict connectivity, but to ensure that information is shared where it creates value without compromising the independence or integrity of safety-critical functions. Control, safety, Fire & Gas, asset-management and remote-monitoring systems may exchange information, but their roles should remain distinct. Access to plant data, for example, does not automatically require the ability

to influence the process or intervene in a safety function. Cybersecurity forms part of this same equation. Connected safety systems need protection against unauthorized access or changes that could affect their availability or performance, while appropriate segregation and access controls can help contain potential risks.

Handled properly, connectivity should give operators better visibility and decision-making rather than create new points of dependency. Data should move efficiently across the plant, while safety functions remain protected, predictable and dependable. With that foundation in place, the role of the technologies performing those safety functions becomes even more important. As direct human intervention becomes less frequent, more responsibility for recognizing hazardous conditions and initiating protective actions shifts toward the technology itself. This makes the reliability of both field instrumentation and functional-safety systems central to the overall protection strategy.

Intrinsically safe technologies remain fundamental in hazardous areas, allowing instrumentation and associated circuits to operate without providing sufficient electrical or thermal energy to ignite a potentially explosive atmosphere. At the same time, connected field devices are providing



richer diagnostics and more process information, creating an opportunity to combine inherent protection with greater visibility into equipment and system condition.

Functional-safety technologies provide a complementary layer. Safety instrumented systems, emergency shutdown functions and other safety-critical systems are designed to respond to defined hazardous conditions and move the process to a safe state when required.



Their importance grows as automated responses take on tasks that might previously have depended on rapid human action. The aim is not to remove people from the safety equation, but to support them when time is limited. Robust instrumentation, independent protection layers, diagnostics and validated safety functions create the foundation on which the wider safety architecture can operate. The next challenge is to ensure that these protective layers work together without undermining one another. That balance becomes particularly important in facilities where DCS, PLC, ESD, Fire & Gas, HIPPS and SCADA systems operate alongside one another. Their effectiveness depends not only on the performance of each individual system, but also on how clearly the interfaces between them are defined.

Integration can bring substantial benefits. Sharing the right information can improve situational awareness, accelerate diagnosis and help operators understand how a developing process deviation is being managed across multiple protection layers. Common engineering and monitoring environments can also simplify operations and maintenance. At the same time, seamless interaction should not

become excessive dependence. Safety functions may require defined independence, segregation and fault tolerance so that a failure in one system does not compromise another layer of protection. As networks, engineering tools and shared data connect systems that were historically separate, preserving those boundaries becomes more demanding. The answer is not to isolate every system, but to integrate selectively and deliberately: establish clear interfaces, maintain appropriate independence, and ensure that interactions are engineered, tested and documented. Done well, integration makes the overall architecture easier to understand and manage. It also creates a stronger flow of information into maintenance, where early indications of degradation can be acted upon before a fault becomes a failure.

This is where advanced diagnostics and continuous monitoring begin to change the way safety systems are maintained. Rather than relying solely on scheduled testing or waiting for a device to fail, operators can use condition information to identify degradation, abnormal behavior and developing faults earlier. For safety-critical instrumentation, this provides a more detailed picture of system health between proof tests and maintenance interventions. Diagnostic information can help teams prioritize attention, identify potential failures sooner and reduce the likelihood of discovering a problem only when a safety function is demanded.

Remote condition monitoring is especially valuable in offshore, remote or difficult-to-access facilities, where physical inspection can be costly and operationally disruptive. Bringing relevant information into a centralized view can support more targeted maintenance planning and reduce unnecessary field intervention. Established functional-safety practices remain essential: proof testing, inspection and maintenance are still needed to demonstrate that a safety function will perform when required. What changes is the quality and timeliness of the information available between those activities. The result is a shift from simply asking whether a safety system is operational to understanding its condition, availability and emerging risks. For existing facilities, this can provide a route to improvement without wholesale replacement. For brownfield facilities, that distinction is critical. Modernization rarely starts with a blank sheet of paper: operators need to introduce new capabilities while maintaining production, preserving proven safety functions and controlling the risks associated with modification. The most practical approach is therefore often incremental rather than transformational. Modern safety platforms can increasingly coexist with legacy control and instrumentation, allowing improved diagnostics, communication and safety functionality to be introduced in stages. This can extend the useful life of existing assets while addressing limitations created by obsolete technologies.

The starting point should be a clear understanding of the installed safety system and its lifecycle: its architecture, dependencies, proof-test regime, obsolescence risks and remaining performance. New technology should then be introduced where it can deliver a measurable improvement in safety performance, availability, maintainability or lifecycle support. Interoperability is important, but disciplined change management is equally critical. Every modification needs to be considered in the context of existing protection layers, including its potential effect on independence, failure modes and established safety functions. The objective is not simply to make an aging facility more digital. It is to modernize selectively and systematically, improving capability while avoiding unnecessary disruption or new dependencies. That lifecycle perspective also changes how operators should judge whether a safety system is genuinely delivering value.

A safety system should ultimately be judged by how effectively it manages risk in real operating conditions, not simply by whether it meets the requirements defined at installation. This means looking beyond certification and assessing how the system will perform, be maintained and evolve throughout the life of the asset. A robust assessment begins with the safety lifecycle itself: the quality of the hazard and risk assessment, the definition of safety requirements, the suitability of the architecture, verification and validation, and the ability to demonstrate that required safety functions remain effective during operation.

Maintainability is equally important. Diagnostics, proof testing, fault identification and access to relevant system information influence how quickly degradation can be detected and corrected. Long-term considerations such as obsolescence, spare parts, software support, cybersecurity and maintenance competence are equally important. The most capable safety system is therefore not necessarily the one with the most sophisticated technology. It is the one whose performance can be understood, verified and maintained



over time while continuing to meet its defined risk-reduction objectives.

Functional safety is ultimately a lifecycle commitment rather than a compliance milestone. Technology, processes and people must continue to work together so that the intended level of protection remains effective for as long as the asset operates. That requirement becomes even more demanding as facilities move into harsher and more complex operating environments.



Offshore installations, LNG facilities and high-pressure production and processing environments can combine extreme temperatures and pressures, hazardous-area requirements, limited physical access and highly consequential process conditions. In these settings, safety-critical instrumentation and control systems must deliver dependable performance while offering better insight into their own condition. For instrumentation, this places greater emphasis on robustness, reliability and diagnostics. Devices need to provide accurate measurements in harsh environments while identifying potential faults early enough for operators to respond. The challenge is particularly significant where equipment is difficult or costly to access, making unnecessary maintenance undesirable and reliable condition information increasingly valuable. The wider safety architecture is affected too. Safety functions must remain predictable and available despite environmental stresses, equipment degradation and complex interactions between control and protection systems. Solutions also need to remain maintainable and supportable over potentially decades-long asset lifecycles.

Technology selection therefore needs to move beyond individual specifications. Environmental suitability, functional safety, diagnostics, maintainability and lifecycle support should be considered together. As facilities operate closer to demanding process limits and in locations where intervention is more difficult, safety-critical systems must deliver not only high reliability, but also greater confidence that their performance can be understood, verified and maintained throughout the asset lifecycle.



About the author: Gabriele Caglio is Customer Excellence Lead at GM International, with more than 20 years of experience in intrinsic safety and safety solutions for the process industry. Combining technical expertise with customer support, product training and technical communication, he works closely with engineering teams worldwide. He regularly develops technical articles, white papers and digital content focused on intrinsic and functional safety, translating complex technical subjects into clear, accessible insights for industry professionals.

Contact Details:

G.M. International S.p.A.
W: www.gminternational.com
E: info@gminternational.com
T: +39 039 2325038