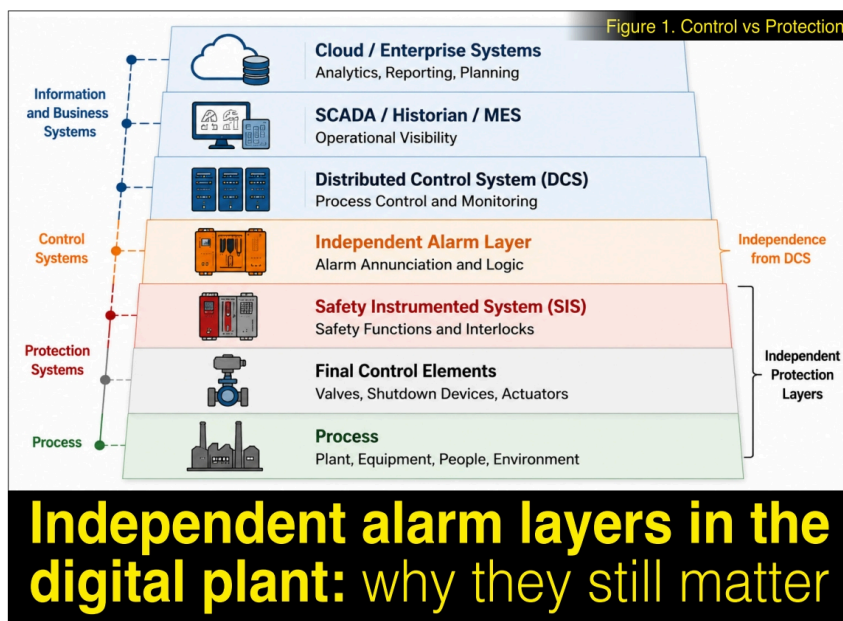




**D**igital transformation has changed the way process plants operate. Today's facilities are more connected than ever, with distributed control systems (DCSs), smart field devices, Ethernet networks, asset management software, and cloud-based analytics providing operators with a level of visibility that would have been difficult to imagine just twenty years ago.

Those technologies have improved plant performance. Operators have better diagnostics, maintenance teams can identify developing equipment problems earlier, and engineers have more process data for optimisation than ever before.

Yet one basic principle of process safety remains unchanged: the system controlling a process should not be the only system responsible for protecting it.

That is worth revisiting as plants become increasingly dependent on connected automation systems.

### When Everything Happens at Once

Most control systems perform well during normal operation. The real test comes when something unexpected happens.

Consider a compressor operating outside its normal pressure range. As the upset develops, discharge pressure and temperatures rise and downstream

equipment reacts to changing conditions. Within seconds, the control room may receive dozens of alarms.

None is necessarily wrong, but they arrive at nearly the same time.

Operators must determine which alarm represents the initiating event and which are consequences. Even experienced operators can become overwhelmed when alarm rates increase dramatically during an upset.

This alarm flood remains one of the industry's biggest human factors challenges. Adding more alarms does not necessarily improve safety and can have the opposite effect.

That is why independent alarm layers continue to play an important role.

### Control and Protection Serve Different Purposes

A DCS may monitor every process variable, but that does not mean it can provide every layer of protection a facility needs. Control and protection are different engineering problems.

A control system keeps a process running efficiently by adjusting valves, regulating pumps, maintaining temperatures and optimising production.

Protection systems have a narrower objective: monitoring specific conditions that could

lead to unsafe operation and initiating predetermined actions.

The distinction is important during abnormal conditions. If the control system experiences a software or communication failure, or becomes overloaded with events, protective functions should remain available. Independence reduces the possibility that a single failure can affect both process control and protection.

This philosophy has been embedded in process safety for decades and continues to underpin Layer of Protection Analysis (LOPA) and Safety Instrumented System (SIS) design.

### The Risk Isn't Always Equipment Failure

When engineers think about protection layers, they often picture failed transmitters, sticking control valves or failed pumps. Those failures occur, but they are only part of the picture.

Modern plants also face common-cause failures: events affecting multiple systems because they share infrastructure.

Examples include a failed network switch, loss of a common power supply, a problematic software update or a cybersecurity incident affecting plant communications.

None necessarily damages field instrumentation. Measurements may remain accurate, but operators may no longer receive the information they need.

Independent alarm layers reduce this risk through separate hardware, logic or communication paths. They do not eliminate failures, but reduce the likelihood that one event can compromise multiple safeguards.

### Alarm Management Still Matters

The process industries have improved alarm management through rationalisation, prioritisation and standards such as ISA-18.2 and IEC 62682. Despite these efforts, alarm overload remains a common finding after major incidents.

A well-designed alarm should provide information requiring operator action, with enough time for that action to be effective.

If every minor process deviation generates an alarm, operators eventually learn to ignore them. Conversely, delayed or unnecessarily suppressed alarms can cause critical warnings to arrive too late.

Independent alarm systems can help by focusing on process variables requiring immediate attention. Rather than competing with hundreds of operational alarms, they provide clear notification that a protective action is required or underway.

## Modernisation Doesn't Always Mean Replacement

Many hazardous-area facilities were commissioned decades ago. Their control systems have evolved, but much of the field wiring, instrumentation and shutdown philosophy remains intact.

Replacing an entire control or safety system is not practical for many plants because of budget limitations, production schedules and limited shutdown windows.

An incremental approach can introduce additional protection layers without replacing the existing DCS or redesigning an entire Safety Instrumented System. Independent alarm logic can be added to specific units, aging alarm trips consolidated, and critical applications given more sophisticated voting strategies while leaving the rest of the process unchanged.

This allows plants to improve safety without committing to complete system replacement.

## There's a Gap Between Alarm Trips and Safety PLCs

Historically, engineers selecting protective equipment faced two choices: individual alarm trips for straightforward single-variable applications, or programmable Safety PLCs for complex Safety Instrumented Functions across entire process units.

Many applications fall between these extremes.

A compressor protection system may require several transmitters using two-out-of-three voting. A tank farm may need multiple independent level inputs before initiating a shutdown, while a burner management subsystem might require several discrete and analogue signals.

These applications may not justify a full Safety PLC, yet exceed the capabilities of traditional single-loop alarm devices.

The industry has increasingly recognised this "middle ground", leading to compact multiloop logic solvers providing deterministic hardware, configurable voting logic and functional safety capabilities without the engineering complexity of larger programmable platforms.

For many brownfield applications, they provide a practical balance between capability and cost.

## Looking Ahead

Artificial intelligence, predictive analytics and machine learning will continue improving industrial operations.

Maintenance teams will become better at predicting equipment failures, while operators receive increasingly sophisticated decision-support tools.

Those technologies should be welcomed. They do not, however, replace independent protection.

When a process exceeds a safe operating limit, protective action must be deterministic, reliable and available regardless of network traffic, software updates or operator workload.

Digital transformation has made industrial facilities smarter, but also more interconnected and, in some respects, more dependent on shared infrastructure.

That reality does not diminish the value of independent alarm layers. If anything, it reinforces why they remain an essential part of modern process safety.

As automation evolves, the most resilient facilities will be those that embrace new digital technologies while preserving a principle that has served the process industries well for decades: control systems keep the process running, but independent protection systems keep it safe. ■



### About the author



**Sergio Magana** is an Applications and Marketing Technical Specialist at Moore Industries with over 12 years of experience in process instrumentation. He supports customers with signal conditioning, alarm systems, and hazardous-area applications, helping engineers select and apply reliable solutions for demanding industrial environments.