senses.ai

Dr. Johannes Kunz

Control and Automation of Chemical Process Equipment

November 2025

The rapid development of information technology has only slowly made its way into the reality of industrial processing environments, namely in the chemical and power generation industries. There are many reasons, often related to safety and a focus on robust, well tested approaches that have made this environment slow to adopt new ideas, particularly when it comes to automation and the use of Artificial Intelligence and Machine Learning. Equally, some operators and manufacturers often have security and confidentiality concerns when using the cloud. In this paper, the options and benefits of applying 21st century IT concepts to infrastructure with high safety or systemic risks will be demonstrated, with a strong focus on automation, predictive maintenance, security, and also a specific focus on investment and operations cost. Artificial Intelligence and Machine Learning will be explored, including limits emerging from accountability requirements and legal frameworks.

Automation and Redundancy

One of the key concepts of safely operating equipment with a potential to endanger lives and the environment has always been redundancy, particularly when automation is involved, where continuous human supervision is reduced to a minimum. In this context, it is considered risky to just use one sensor or one process control unit to ensure that no dangerous changes are creating surprises.

Traditional redundancy concepts

The traditional concept is applying physical redundancy, i.e. having every item of relevant equipment twice: two sensors of the same kind, two actors for the same actions, and double wires leading to redundant PLCs (programmable logic controllers).

This is usually supported by the introduction of sequential software redundancy to trigger interventions with multiple lines of control.

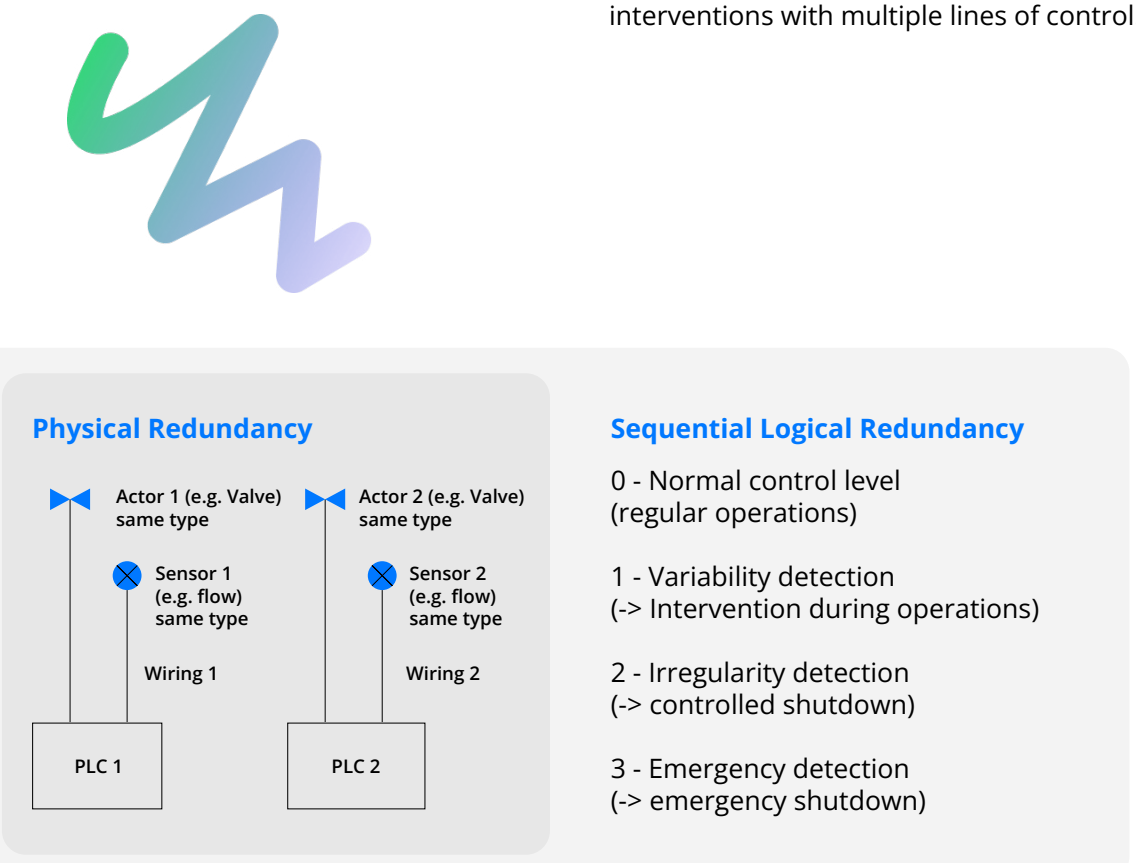


Figure 2.1 - Physical and Sequential logical redundancy

The approach of physical redundancy is expensive, given the need for everything twice, and still subject to systemic failure risk. Two identical sensors that don't work properly because of a manufacturing fault, or PLC software that has the same error in both physical computers, may fail undetected in the physically redundant environment. This risk cannot be eliminated by physical redundancy (see IEC 61508, Part 6, Annex D on Common Cause Failure).

Sequential logical redundancy is often used to catch these issues. If implemented well, with multiple layers of triggers that react to increasing deviations from an expected state, for example in liquid levels, system pressures, or key input or output parameters, it can provide for the necessary safety net. It is built on different, independent logical systems that observe certain key parameters and react accordingly. To use an example, levels in a vessel containing a key process fluid should correspond to other operating parameters, such as throughput, temperature or output. Small deviations are part of normal operations and are no reason for concern and do not lead to any interventions.

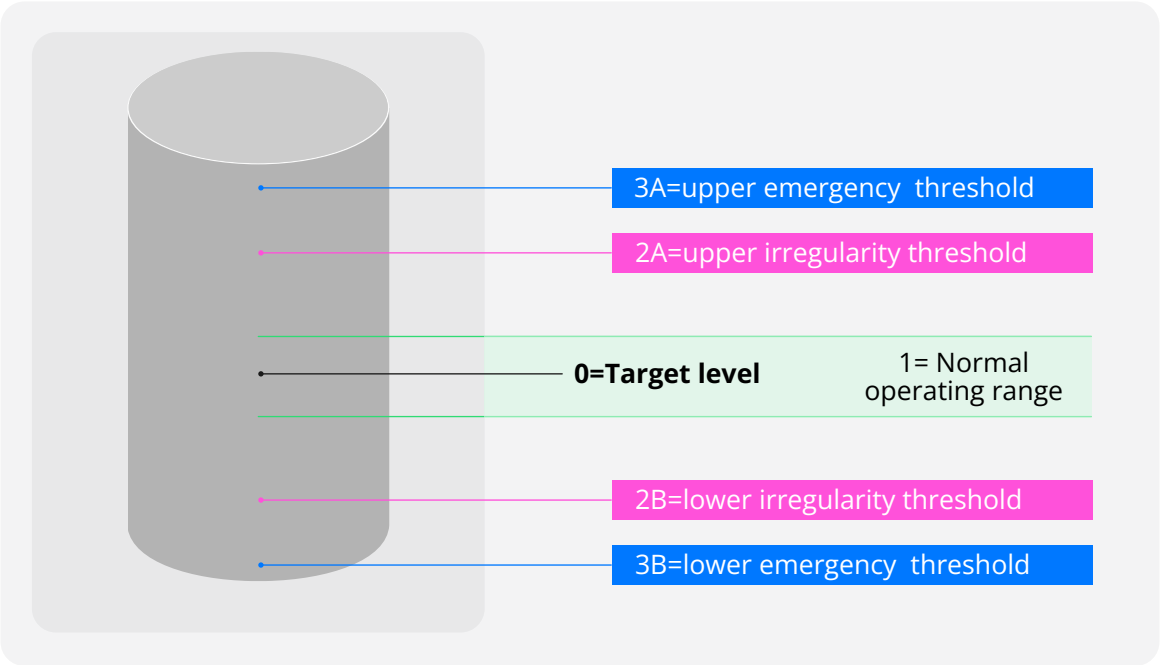


Figure 2.2. Sequential logical redundancy thresholds

If deviations become larger, signaling a serious problem, a controlled shutdown is initiated. If for whatever reason, this controlled shutdown is not happening fast enough, an emergency shutdown is triggered when deviations reach the level 3 threshold.

This approach comes with a serious risk of reacting too late in severe situations, at the cost of extended downtime, equipment damage and opportunity cost related to ensuing repairs - or even environmental damages resulting from the emergency shutdown procedures.

A key objective of a more advanced control system is a better outcome for all operational and emergency scenarios, with the objective of reducing cost (from physically redundant equipment or operational losses) and risk (for downtime and damage).

Sequential logical redundancy, if applied in a standard fashion, is also prone to systematic errors, both from sensor or actor failures (e.g. a defective sensor providing incorrect level measurements) or software errors in control processes that systematically misinterpret input. Due to these limitations, sequential logical redundancy is usually insufficient for automating operations and for triggering irregularity-driven interventions (see IEC 61511 - Safety Instrumented Systems for the Process Industry Sector).

Thus, while sequential logical redundancy improves resilience against threshold violations, it remains fundamentally dependent on homogeneous measurement and processing assumptions. As automation intensifies and decision speed increases, this structural homogeneity becomes the dominant residual risk.

Full Logical Redundancy

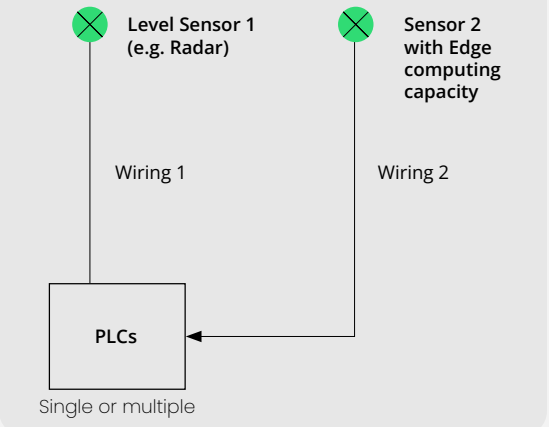
The preferred solution for automating operations, and for the application of any advanced AI logic, is redundancy achieved through epistemically independent measurement and processing pathways, minimizing correlated failure probability across sensing, signal conditioning, computation, and interpretation layers. This redundancy is not constructed traditionally, but rather delivers and processes important operational data on different pathways.

A simple example can explain full logical redundancy: Instead of having two identical level transmitters in a fluid tank that transfer data to two different (identical and identically programmed) PLC units processing the information, redundancy is created by an approach where a level transmitter of one type is complemented with a different and independent method of level measurement and processing.

For example, in a processing equipment with elevated temperature levels of process fluids, combining traditional level measurement with thermal imaging is a successfully tested approach. This also often reduces overall cost, as - for example - thermal imaging can not only be used to determine liquid levels, but can identify many other problems, for example unusually low or high temperatures in the entire environment. When combined with a Machine Learning approach, it can also detect anomalies, for example leaks indicated by unexpected temperature levels in unusual places.

In this case, the two different sensing approaches after proper calibration usually yield the same liquid levels, enabling a higher degree of certainty and accuracy in determining values, and providing the necessary ability for automation and optimization based on Machine Learning. At the same time, the dual approach enables the identification of instrument failure indicated by diverging measurements from the two sources.

If the second measurement approach provides its own (edge) computing capacity, data processing errors can equally be eliminated, creating the ability to exchange faulty sensing or processing equipment without interrupting device operations (hot-swapping). And last, but not least, this approach enables cost savings, as it allows for the use of lower cost sensing and processing equipment: shorter MTBF (Mean Time between Failures) does not threaten overall reliability.



A further improved level of measurement verification can be obtained by combining metrics in a monitoring and management system. A level drop, caused by a leakage, would likely also be detected by changing pump power demand. Ultimately, combining non-identical sensor reads can create a significantly better understanding of the operational conditions at lower cost.

Figure 2.3 - Logical Redundancy

AI Integration

The integration of Artificial Intelligence (AI) into chemical process automation introduces a new architectural dimension: probabilistic inference within traditionally deterministic control systems.

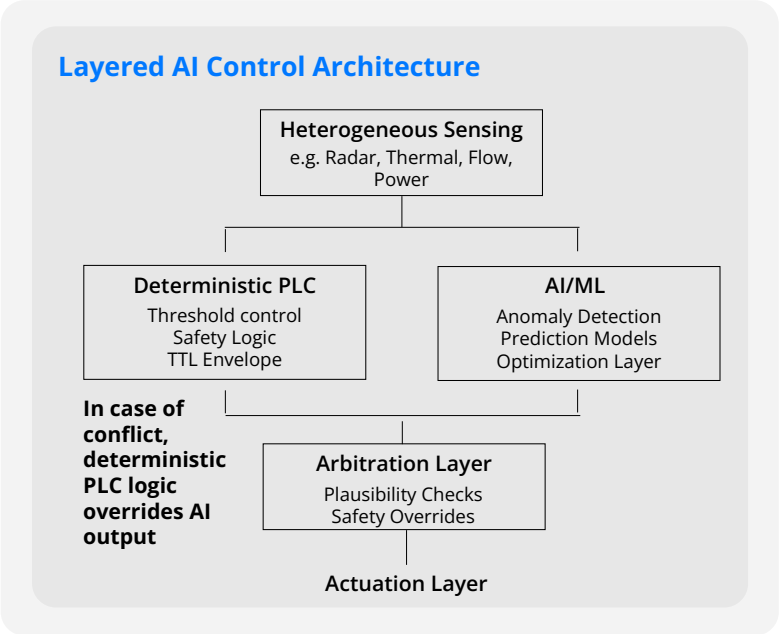
Conventional PLC-based control operates on predefined thresholds and rule logic. AI systems, by contrast, generate outputs based on statistical learning and pattern recognition. While this enables much earlier anomaly detection and predictive optimization, it also introduces new risks:

- Non-deterministic behavior
- Model uncertainty and drift
- Reduced interpretability
- Failure at inference-level

AI systems may fail systematically if trained on biased data, exposed to distribution shifts, or deployed across similarly structured processing environments. As with identical physical redundancy, correlated failure cannot be excluded if architectural independence is not ensured. For this reason, AI must not simply replace deterministic safety logic but complement it within a structured redundancy framework. Key architectural principles are:

- **Epistemic Independence**
  Sensor modalities and processing paths must be heterogeneous to minimize correlated failure across sensing and inference layers
- **Deterministic Safety Authority**
  Certified PLC logic retains final authority over shutdown and emergency functions. AI recommendations remain bounded by predefined safety envelopes
- **Bounded AI Autonomy**
  AI operates only within predefined safety envelopes and cannot violate hard safety constraints
- **Cross-Validation**
  Divergence between deterministic and AI-derived outputs should trigger review or diagnostic escalation rather than initiate automatic actuation

Properly integrated, AI enhances diagnostic resolution, reduces false shutdowns, and improves predictive maintenance capability - while preserving functional safety principles and clear accountability structures in high-risk industrial environments.



Properly integrated, AI enhances diagnostic resolution, reduces false shutdowns, and improves predictive maintenance capability — while preserving functional safety principles and clear accountability structures in high-risk industrial environments.

Figure 2.4 - AI Control Architecture

Summary

The automation of high-risk industrial process equipment cannot rely on traditional redundancy concepts alone. While physical duplication of components reduces certain failure probabilities, it does not eliminate systemic and common-cause risks. Sequential logical redundancy improves resilience through threshold-based intervention, yet remains structurally dependent on homogeneous sensing and processing assumptions.

As industrial environments become increasingly automated and AI-supported, these limitations become more pronounced. The dominant risk shifts from isolated component failure to correlated architectural failure. Addressing this requires the evolution: from redundancy as duplication to redundancy as epistemic independence.

Full logical redundancy - based on heterogeneous sensing modalities, independent processing pathways, and cross-validating interpretation layers - reduces correlated failure probability while enabling higher levels of automation and optimization. It allows for earlier anomaly detection, improved diagnostic resolution, and more efficient lifecycle management without compromising safety integrity.

The integration of Artificial Intelligence adds further capability, but also introduces probabilistic behavior into traditionally deterministic safety architectures. For this reason, AI must operate within a clearly defined governance structure. Deterministic PLC-based safety logic must retain final authority over shutdown and emergency functions, while AI contributes predictive insight, anomaly detection, and operational optimization within bounded safety envelopes.

About the Author

Johannes Kunz has been working with control and automation systems for more than two decades, across many industries, e.g. chemical, energy and automotive. His experience involves the design of hardware and software architecture, embedded systems architecture with local and cloud service processing. He holds masters degrees in law (University of Zurich), management with IT focus (University of Zurich) and a Ph.D. in economics (University of St. Gallen). Johannes has worked in corporate, startup and consulting environments across the globe.

johannes@9senses.ai