industries

MDPI

Article

From Monitoring to Attention Economy: Event Design for Human Supervision in Highly Automated Industrial Systems

Martin Hollender

ABB Corporate Research Center, 68309 Mannheim, Germany; martin.hollender@de.abb.com

Abstract

Industrial production plants in sectors such as chemicals, life sciences, metals and mining, pulp and paper, and power generation operate with a high degree of automation. During steady-state operation, control systems maintain process stability with little need for human intervention, while operators primarily supervise plant behavior and intervene during startup, shutdown, product transitions, or abnormal situations. At the same time, modern plants must monitor multiple domains simultaneously, including process performance, asset conditions, cybersecurity threats, and physical security. These developments significantly increase the number and diversity of events generated by monitoring systems. Advances in sensing technologies, connectivity, and data analytics have greatly improved the ability to detect deviations from normal operation. However, the increasing volume of anomalies detected raises the challenge of determining which events should be brought to the attention of human supervisors. Since direct human intervention becomes less frequent but more critical in highly automated plants, the effective use of operator attention becomes an essential aspect of system design. This paper examines monitoring within the broader framework of supervisory control in industrial systems. Monitoring is viewed as the continuous determination of system state across multiple domains, with anomaly detection forming the basis for subsequent supervisory decisions. Building on this perspective, the paper analyzes how detected deviations are translated into events and discusses criteria for deciding which events require human attention. A structured view of monitoring and supervision is proposed that integrates process operation, asset health, cybersecurity, and physical security. The goal is to outline event generation design principles supporting effective human oversight in increasingly autonomous industrial environments.

Keywords: industrial process monitoring; alarm management; supervisory control; anomaly detection; security in critical infrastructure; human attention & situation awareness

Check for updates

Academic Editor: Ying Liu

Received: 11 September 2026
Revised: 5 October 2026
Accepted: 30 October 2026
Published: 11 November 2026

Copyright: © 2026 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license.

1. Introduction

Industrial production plants are characterized by a high degree of automation [1]. Under steady-state conditions, process control systems maintain operation with minimal human intervention. With the ongoing development towards increasingly autonomous systems, direct operator involvement is decreasing further [2]. Automation increasingly handles both normal operation and a growing range of abnormal situations, allowing individual operators to supervise larger numbers of control modules and progressively larger plant areas. Consequently, operator work is shifting away from direct interaction with the process towards supervisory control, complex diagnosis, and coordination with specialized personnel [3,4]. Tight continuous monitoring is no longer feasible, and a new kind of exception-based intervention needs to be adopted. Examples of industrial plants already

operating with high levels of autonomy include air separation units, combined heat and power plants, electrical substations, compressor stations for pipelines, normally unattended installations (NUIs), such as remote offshore production platforms and wind farms.

Sheridan [5] established the concept of supervisory control, in which lower-level control actions are performed by automation, while the human operator sets goals, monitors performance, diagnoses problems, and intervenes when necessary. Operators are not continuously controlling; they supervise. Excessive false alarms degrade their ability to supervise effectively.

Once monitoring has detected a deviation from normal, the subsequent workflow involves three key steps: first, diagnosing the problem to identify its nature and scope; second, determining which responses to the abnormality are necessary; and third, implementing appropriate actions based on the diagnosis. Achieving a sustainable corrective action requires understanding the root cause, as this approach addresses underlying issues and helps prevent recurring problems, rather than merely alleviating symptoms temporarily.

Historically, plant operation and plant maintenance have been organizationally separated. Control room operators are responsible for supervising process performance and ensuring safe and efficient production, while maintenance personnel ensure that assets such as pumps, burners and reactors remain in a technically sound condition. In practice, however, these domains are interdependent. Equipment malfunctions are a major source of operational problems. Operational constraints might require maintenance actions to be shifted to earlier or later stages, e.g., to be able to satisfy strong and urgent demand.

In recent years, cybersecurity has become an increasingly important dimension of industrial control-room operations. Modern industrial plants are embedded in highly interconnected information technology (IT) and operational technology (OT) environments, often incorporating remote access, cloud-based services, vendor connections, and networked control systems. As many of these facilities form part of critical national infrastructure, continuous monitoring of network activity, system integrity, access patterns, and anomalous behavior is now necessary to maintain both operational continuity and process safety.

At the same time, recent armed conflicts have demonstrated that industrial infrastructure can also become a deliberate military or strategic target. Attacks may be conducted directly through kinetic means, or indirectly through cyberattacks, sabotage, disruption of supply chains, interference with communications, or coordinated hybrid operations. In this context, cybersecurity can no longer be treated solely as a conventional IT concern. Cyber incidents may form part of a broader attack intended to degrade production capacity, interrupt energy or material supply, create unsafe process conditions, or undermine confidence in critical services. Although the defense against such attacks will usually be organized by personnel outside the plant, it will also change the job profile of plant operators, for example in monitoring unauthorized physical access to the plant.

This development expands the responsibilities of industrial control rooms. Many plants, particularly smaller or geographically distributed facilities, do not have dedicated cybersecurity personnel available on a permanent basis. As a result, initial security monitoring, anomaly recognition, and incident escalation may become additional tasks for control-room operators. Operators may be required to assess whether unusual process behavior is caused by equipment failure, instrumentation problems, operator error, malicious manipulation, or an external attack. Effective support therefore requires the integration of cybersecurity information into control-room monitoring in a form that is operationally meaningful, while avoiding excessive alarm loads and demands for specialist expertise. Automated detection and correlation should handle continuous low-level surveillance, whereas human operators should remain responsible for contextual assessment, coordination, and decisions that involve process safety and operational consequences.

Human operators are particularly well suited to managing unforeseen, ambiguous, or highly complex situations in which predefined procedures and automated decision rules may be insufficient. By drawing on experience, contextual understanding, and adaptive reasoning, operators can interpret incomplete or conflicting information and develop creative responses to novel problems. In contrast, humans are less suited to the continuous and consistent execution of repetitive, low-level monitoring and control tasks over extended periods. Performance in such tasks may deteriorate because of fatigue, reduced vigilance, and the difficulty of sustaining attention during monotonous work. Consequently, routine and time-critical functions that require continuous 24/7 operation are generally better assigned to automated systems, while human operators should retain responsibility for supervision, diagnosis, judgement, and intervention in abnormal or unanticipated conditions [6].

Human operators are increasingly scarce and difficult-to-replace. As Leach, Wright, and King [7] highlight, many industrial sectors are already experiencing critical shortages of skilled operators, driven by an aging workforce, intense competition for talent, and the significant time and cost required to train a new operator to full competence. Given this context, deploying qualified operators on poorly supported monitoring tasks—where inadequate tools, fragmented information displays, or low-quality alarm systems force operators to spend cognitive effort on work that better technology could handle—represents an inefficient use of scarce operator expertise and attention. When operators are burdened with inefficient monitoring support, their attention and expertise are consumed by low-value activities rather than focused on the complex judgment and decision-making that only an experienced operator can provide.

Because human supervisors can attend to only a limited number of concurrent demands, monitoring systems should allocate their attention to situations in which human assessment or intervention adds most value. Monitoring and automation systems must be designed to support this resource rather than erode it through nuisance alarms. Accordingly, this paper develops criteria for transforming detected deviations into human supervisor-facing events and examines how these criteria can support supervision across process, asset, cyber, and physical-security domains.

In older, heavily staffed plants, an operator could be largely occupied with monitoring the alarm list and filtering out alarms with little or no operational value; alarm rates exceeding 1000 alarms per day are still encountered in practice. In increasingly autonomous plants, where human attention is a scarce supervisory resource, such use of operator capacity is no longer sustainable.

This paper reframes industrial monitoring as an attention-allocation problem in increasingly automated plants. Monitoring should not primarily be optimized for detecting abnormalities; it should be optimized for deciding which detected abnormalities deserve scarce human attention. In increasingly autonomous plants, human attention will be the limiting factor for both traditional process and asset monitoring tasks and the increasingly important cyber and physical security monitoring tasks.

Several established research streams address individual aspects of industrial monitoring and supervision, but they approach the problem from different starting points and with different objectives. Table 1 positions the present work relative to representative reviews in these fields and highlights the gap addressed here: the selection and escalation of machine-detected deviations that warrant limited human attention.

The remainder of the paper follows the progression from monitoring to human-facing escalation. Section 2 describes the conceptual and integrative review methodology. Section 3 examines the sources and forms of monitoring information in highly automated plants across process, asset, cybersecurity, and physical-security domains. Section 4 then places these monitoring functions within the broader supervisory-control loop and examines how

detected deviations are transformed into information for human supervision. Building on this analysis, Section 5 discusses the implications for meaningful escalation, cross-domain integration, and the treatment of human attention as a design constraint. Section 6 summarizes the main conclusions.

Table 1. Positioning of the present work relative to existing review literature.

Review Stream	Representative Reviews	Main Emphasis	Comment
Industrial process monitoring	Qin; Reis & Gins [8]; Li et al. [9]	Detection, diagnosis, prognosis; statistical/data-driven methods	Little emphasis on whether detected deviations deserve human attention
Anomaly detection/ML	Qin & Chiang [10]; Li et al. [9]	Detection accuracy, robustness, interpretability, changing operating conditions	Detection output generally remains the primary object of evaluation
Alarm management	Mustafa et al. [11]; Dorgo et al. [12]; Hollender et al. [13]	Alarm lifecycle, nuisance alarms, floods, prioritization, standards	Primarily starts with alarms already intended for operators
Predictive/condition-based maintenance	Jardine et al. [14]; Gangsar & Tiwari [15]; Giacotto et al. [16]	Asset diagnostics, prognosis, maintenance decisions	Human-attention allocation across plant domains is not the central problem
Human–automation interaction	Wilhelm & Freitag [4] and foundational literature	Roles, function allocation, interaction with automation	Does not specifically address selection among large numbers of machine-detected deviations
This paper		Detection, evaluation, escalation across process, asset, cyber and physical-security domains	Human attention explicitly treated as scarce supervisory resource

2. Methodology

The analysis draws on established concepts from industrial process monitoring, alarm management, supervisory control, human factors, asset monitoring and maintenance, and cybersecurity. These bodies of work are considered from a common supervisory perspective: an automated system observes the state of a technical system, identifies deviations from expected behavior, and may communicate information about these deviations to a human supervisor.

The analysis was structured around the sequence from detection to human intervention. First, existing monitoring approaches and the main sources of abnormal events in industrial plants were considered across four domains: process operation, asset condition, cybersecurity, and physical security. Second, the role of automated monitoring was distinguished from the subsequent functions of diagnosis, decision-making, and corrective action. Third, established findings from alarm management and human-factors research were used to examine the consequences of presenting excessive, unreliable, redundant, or non-actionable events to human supervisors.

On this basis, the paper distinguishes between machine-level detection and human-facing alarm generation. A detected deviation is treated as an internal result of a monitoring function, whereas escalation is treated as a separate decision concerning whether the information warrants limited supervisory capacity. Alarms are therefore examined according to

factors such as their operational relevance, actionability, consequences, persistence and the need for human judgement, coordination, or intervention.

This paper is a conceptual, integrative review rather than a systematic literature review. References were selected to represent established frameworks, major industrial standards, seminal human-factors findings, and recent reviews across the relevant research domains. The objective is not exhaustive coverage of each individual field, but to synthesize their implications for the common problem of human-facing event generation in highly automated industrial systems.

3. Industrial Monitoring in Highly Automated Plants

3.1. Definition of Monitoring

Monitoring can be defined as the acquisition, processing, and evaluation of information describing the state and condition of an industrial plant. This information is typically obtained from process measurements, equipment sensors, control-system data, alarms, laboratory analyses, and operator observations. The observed plant behavior is compared with expected operating conditions, predefined limits, reference models, or historical patterns. The primary objective of monitoring is to identify deviations from normal or desired operation at an early stage. Such deviations may indicate process disturbances, equipment degradation, sensor or actuator faults, control-system deficiencies, or emerging safety risks. Monitoring therefore provides the information required to assess whether the plant remains within its intended operating envelope and whether further diagnostic or corrective actions are necessary.

A highly automated plant can run for extended periods without requiring any human intervention. The alarm system constitutes one of the most important interfaces between automation and human supervision.

Figure 1 shows how a detected deviation from normal operation can evolve into a human-facing alarm. The first step is to decide whether the deviation is operationally relevant or not. This is typically determined during alarm rationalization [17]. Deviations without operational relevance should never propagate to the human supervisor. The next step is to check if automatic resolution is available. Examples are switching to redundant equipment or decreasing throughput. Finally, it must be determined whether immediate human action is required. For example, it might be sufficient to wait until the next regular maintenance interval is reached. Only in the remaining cases should an alarm be sent to the human supervisor.

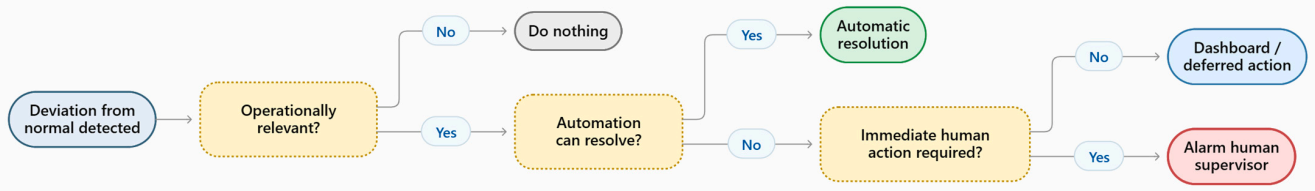


Figure 1. Conceptual decision framework for transforming detected deviations into human-facing alarms.

In the underlying domains, these terms are not synonymous. Event is used here as the generic term for a detected occurrence or state change, whereas alarm, notification and alert denote information communicated to a human which does not necessarily imply a required operator response; in alarm-management standards, an alarm specifically implies the need for timely operator response. Concerning terminology, a key issue is that foundational documents such as EEMUA 191, ISA-18.2, and IEC 62682 define an alarm as an event that requires a timely operator response. In industrial practice, however, this represents an

ideal that few plants achieve, and many plants continuously generate alarm notifications that do not require meaningful operator action. Practitioners often use the term alarm more broadly to refer to a configured condition that may generate a notification to a human supervisor. A persistent problem is that a substantial fraction of these human-facing events may have little or no operational value. For the purposes of this paper, all events presented to a human supervisor are referred to as alarms, while human-facing events that lack operational relevance are referred to as nuisance alarms.

In older, more heavily staffed plants, operators could themselves determine whether an alarm required action or could safely be ignored. In modern plants, human attention and cognition become scarce resources, so that the generation of many nuisance alarms is no longer an option.

3.2. Sources of Process Deviations and Their Monitoring Implications

Under steady-state conditions, industrial plants operate with minimal human intervention. Process control systems maintain stability and performance, while control room operators supervise overall system behavior rather than executing continuous control actions [5]. Industrial process systems are subject to a wide range of disturbances that can degrade performance, reduce product quality, increase operational risk, or lead to complete process failure. These disturbances may originate from material variability, environmental influences, technical degradation, or automation-related issues. The most relevant categories are summarized below.

3.2.1. Feedstock and Material-Related Disturbances

Variability in raw materials represents one of the most common and influential disturbance sources in industrial processes. Changes in chemical composition, impurity levels, or concentration directly affect reaction kinetics and separation performance. In addition, fluctuations in physical properties such as density, viscosity, particle size distribution, or moisture content may alter heat and mass transfer behavior. Disturbances may also arise from inconsistent feed rates, upstream process variability, supply interruptions, or unintended contamination. Even small deviations in feed characteristics can propagate through tightly integrated process units and lead to significant downstream effects.

3.2.2. Environmental and External Influences

Process performance can be sensitive to changes in ambient and environmental conditions. Variations in temperature, humidity, or atmospheric pressure influence cooling efficiency, heat exchanger performance, and energy consumption. Seasonal effects may systematically shift operating conditions, while extreme weather events can disrupt utility systems or supply chains. Such disturbances are typically exogenous and not directly controllable by the plant operator, yet they may require compensation through control adjustments or operational adaptations.

3.2.3. Utility and Infrastructure Disturbances

Reliable operation depends on stable utility supply and functional infrastructure. Interruptions or fluctuations in electricity, steam, compressed air, cooling water, or inert gas can immediately compromise process stability. Voltage drops, pressure variations, or degraded utility quality may cause suboptimal equipment performance or process constraint violations. Additionally, failures in communication networks, distributed control systems (DCS), programmable logic controllers (PLCs), or data acquisition systems can impair monitoring and control capabilities.

3.2.4. Equipment and Asset-Related Disturbances

Physical degradation of equipment represents a continuous source of disturbance. Gradual phenomena such as fouling, corrosion, scaling, erosion, or catalyst deactivation alter process dynamics over time and often manifest as slow performance drifts. Mechanical wear in pumps, compressors, bearings, and seals can reduce efficiency and eventually lead to failure. Sensor drift, calibration errors, and actuator degradation (e.g., valve stiction) further compromise control accuracy. In severe cases, sudden equipment failures—such as pump trips or heat exchanger leakage—introduce abrupt and potentially hazardous process deviations.

3.2.5. Control and Automation-Related Disturbances

Automation systems themselves may introduce disturbances if not properly designed or maintained. Poorly tuned or unstable control loops can amplify process variability instead of attenuating it. Controller saturation, constraint handling issues, or model mismatch in advanced control strategies (e.g., model predictive control) may lead to suboptimal or oscillatory behavior. Software configuration errors, incorrect parameterization, or unintended interactions between coupled control loops can further destabilize operation. As automation complexity increases, systematic validation and monitoring of control performance become essential to ensure robust process stability.

3.2.6. Malicious and Geopolitical Disturbances

Industrial operations may also be affected by deliberate actions originating from criminal organizations, hostile state actors, or other malicious entities. Such disturbances may be motivated by financial gain, political objectives, strategic coercion, or attempts to assess and exploit weaknesses in critical infrastructure. Potential attack vectors include kinetic actions, cyberattacks, sabotage, supply-chain manipulation, communication interference, and coordinated hybrid operations. These events can compromise process availability, integrity, safety, and confidentiality, while also producing cascading effects across interconnected infrastructure and supply networks. Owing to their intentional and potentially adaptive nature, such disturbances require integrated risk assessment, cybersecurity measures, physical protection, incident response capabilities, and organizational resilience planning [18]. Although cyber-security monitoring is usually done from centralized places like corporate headquarters or Security Operations Centers by external suppliers, in case of potential incidents close coordination with on-site control rooms is essential. Coordinating such disturbances accounts for an increasing share of the operator's responsibilities [19].

3.3. Asset Monitoring and Maintenance

The purpose of asset monitoring is to assess that assets such as motors, compressors, and sensors perform as designed. Assets can degrade slowly through wear and tear or fail abruptly. Although asset management is traditionally handled by a dedicated maintenance department, asset health is also critical to process operations. Control room operators therefore share responsibility, at least to some extent, for ensuring that assets remain functional and reliable. The resilience of autonomous plants depends strongly on the maturity of asset management and on the system's ability to continue operating safely in degraded conditions [20].

Many assets include self-diagnostic capabilities [21]. These include drift detection and various other diagnostic algorithms. Critical instruments are usually implemented redundantly. For example, the 2oo3 strategy means that at least two out of three redundant instruments need to report the same value. Assets like motors and pumps are often equipped with vibration sensors. Numerous machine-learning methods have been developed for fault

detection and diagnosis in electric motors [15]. However, deploying such solutions reliably at scale remains challenging. Industrial installations contain a wide variety of motor types and operating conditions and installation conditions—such as whether a motor is mounted on a rigid or flexible structure—can significantly affect model performance. The quality of a solution must therefore be assessed not only by the number of failures it does not predict, but also by the number of unnecessary inspections triggered by false alarms.

Maintenance activities incur costs and often require temporary reductions in plant productivity. Determining the appropriate balance between preventive maintenance expenditure and the risk of costly unplanned failures is therefore a central challenge. Diagnostic results are often uncertain or ambiguous, which further complicates maintenance decision-making. In practice, however, the available monitoring and diagnostic capabilities are not always fully exploited.

Condition-based maintenance is initiated when monitored indicators reveal a deterioration in equipment condition. Relevant information may be obtained from process measurements, inspections, vibration analysis, lubricant analysis, thermal imaging, or other diagnostic methods. Maintenance is therefore performed according to the actual condition of the asset rather than at fixed intervals. This approach can reduce unnecessary interventions and improve equipment availability [14].

Prescriptive maintenance extends condition-based approaches by recommending specific maintenance actions based on the estimated equipment condition, failure risk, operational constraints, and expected consequences. In addition to identifying an emerging fault or predicting its remaining useful life, prescriptive methods evaluate alternative interventions and determine when and how maintenance should be performed. Recommendations may include component replacement, operating-point adjustment, load reduction, inspection, or deferred maintenance. The objective is to select the action that best balances safety, availability, maintenance cost, production requirements, and asset lifetime. By considering asset condition together with production constraints, available resources, costs, and operational consequences, it supports the integration of maintenance and plant operation [16]. From a supervisory-control perspective, only recommendations requiring human judgement or coordination should demand human attention; routine responses should remain automated.

3.4. Cybersecurity and Physical-Security Monitoring

Cybersecurity monitoring in operational technology (OT) environments differs from conventional IT monitoring because cyber events may directly affect physical processes, equipment, safety, and production. Typical monitoring functions include the analysis of network traffic, system logs, device configurations, access activity, and anomalous communication patterns using mechanisms such as intrusion-detection systems, security information and event management systems, and behavior-based anomaly detection. For OT systems, such monitoring must take account of the normal operating state of the plant and of potential impacts on process performance and safety. It also emphasizes the importance of monitoring physical access, since unauthorized access to equipment, control cabinets, engineering stations, or removable-media interfaces can provide another path for compromising OT systems [18].

Rehman and Bahsi [22] highlight the growing importance of process-aware security monitoring. Process-aware attacks do not merely exploit communication or software vulnerabilities but deliberately manipulate the physical process or its control logic. Consequently, purely cyber-level indicators may be insufficient for detecting or interpreting such attacks. Process-aware monitoring therefore incorporates knowledge of the physical process and evaluates process measurements and dynamic behavior together with cyber information.

Their systematic review shows that this has developed into an important research direction for detecting attacks whose consequences become visible in the physical behavior of the plant.

From the perspective of plant supervision, cybersecurity, physical-security, and process monitoring should therefore not be regarded as completely independent information streams. An unusual network connection may have little immediate operational significance, whereas the same event occurring together with an unexplained process deviation or unauthorized physical access may require urgent attention. Conversely, an operational anomaly may provide evidence of a cyberattack that has bypassed conventional security mechanisms. The supervisory challenge is therefore not to present operators with all detected cybersecurity events, but to correlate information across domains and escalate those situations that have potential operational consequences or require local human judgement and coordination.

4. Monitoring as a Supervisory Control Function

Within a broader supervisory control structure, monitoring represents the first step in a sequence that includes detection, diagnosis, decision-making, and corrective action [23].

Figure 2 illustrates monitoring as the first stage of a broader supervisory-control loop. Detected deviations are not an end in themselves, but provide the input for subsequent diagnosis, decision-making, and corrective action. The value of a monitoring system therefore depends not only on its ability to detect abnormal conditions, but also on whether the resulting information supports these later stages. Events presented to the operator should contribute to understanding the situation and deciding whether human intervention is required.

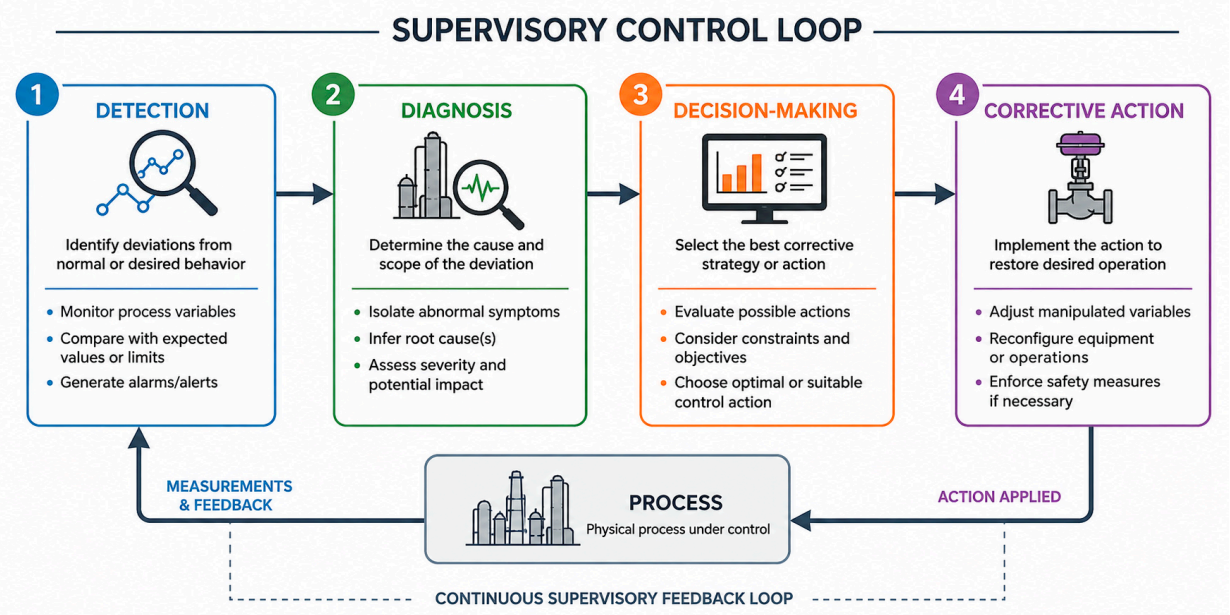


Figure 2. Supervisory control loop

This perspective also clarifies the role of the human operator. Continuous low-level detection can increasingly be performed by automation, whereas human attention is most valuable for interpreting ambiguous situations, assessing consequences, and selecting appropriate responses. The following sections therefore examine both the capabilities and limitations of humans in anomaly detection and the implications for the design of automated monitoring systems.

4.1. Human Capabilities in Anomaly Detection

Historically, anomaly detection relied heavily on human operators inspecting trend curves, alarms, and process indicators. Bliss et al. [24] link low alarm reliability to the "cry-wolf" effect [25]. Operators learn the statistical behavior of the alarm system and adjust their response accordingly. When many alarms are false or unimportant, they respond less frequently—even when a valid alarm eventually appears. For process monitoring, alarm reliability should therefore mean more than technical detection accuracy. An alarm should consistently indicate a condition that requires operator attention or action. Frequent nuisance alarms weaken the credibility of the entire monitoring system. The objective is not to detect and display every abnormal signal. It is to provide a small number of reliable, timely and actionable indications that remain effective even when the operator is under the greatest workload.

4.2. Limits of Sustained Monitoring

The increasing scale and complexity of modern industrial systems exceed the limits of sustained human vigilance. Bainbridge [26] describes this situation as one of the ironies of automation. As routine control tasks are transferred to automated systems, operators are increasingly left with passive monitoring and intervention during rare abnormal situations. However, reduced involvement in normal operation makes it more difficult for operators to maintain an accurate understanding of the process and preserve the diagnostic and manual skills required when automation fails. Automation may therefore remove tasks that humans can perform routinely while leaving them responsible for the most complex, unfamiliar, and time-critical situations, often with limited opportunity to practice the required response.

4.3. Automated Detection Approaches

Anomaly detection in modern industrial plants is increasingly performed by automated monitoring systems using statistical, model-based, and data-driven methods. Qin [27] provides a broad overview of data-driven process monitoring, in which multivariate statistical techniques such as principal component analysis and partial least squares are used to characterize normal operating behavior and detect deviations caused by process disturbances, sensor or actuator faults, control-performance degradation, or quality-related problems. These methods are particularly useful for large sets of correlated process measurements because they can identify relevant relationships without requiring detailed first-principles models.

Detection alone, however, is not sufficient. Once an abnormal condition has been identified, the monitoring system should support diagnosis, fault reconstruction, and ultimately root-cause identification. Qin [27] also points to several practical limitations, including ambiguous contribution plots, nuisance alarms caused by deviations with little operational relevance, and the difficulty of accounting for process dynamics, multiple operating modes, hierarchical plant structures, and gradual changes in normal operating conditions. More sophisticated methods may improve detection performance, but this additional complexity must be balanced against ease of implementation, interpretation, and maintenance.

Machine-learning methods extend traditional process-monitoring approaches by allowing complex and nonlinear relationships to be learned from historical plant data [10]. Their application to industrial processes is nevertheless challenging. Process data are strongly correlated and dynamic, influenced by feedback control, and generated under operating conditions that change over time. At the same time, representative data from abnormal situations is often scarce. Qin and Chiang [10] therefore argue that industrial machine-learning methods need to incorporate process characteristics and domain knowledge and

must provide results that remain interpretable in an operational context. Their value consequently depends not only on detection accuracy, but also on robustness in changing operating conditions and on whether the resulting information can support engineering and operator decisions.

Li et al. [9] illustrate this challenge for closed-loop industrial processes, where genuine faults must be distinguished from normal changes in operating conditions. Both may cause process variables to deviate from historical steady-state distributions, but their dynamic behavior can differ substantially. Feedback control may compensate for a legitimate operating change and establish a new stable condition, whereas a fault may result in persistent abnormal dynamics that the control system cannot suppress. The authors therefore propose considering static and dynamic characteristics separately, both within local process subsystems and at the plant-wide level. A persistent deviation in both static and dynamic indicators suggests that the process is no longer adequately controlled, whereas a static deviation followed by a return of the dynamic indicators to normal is more consistent with a controlled transition to a new operating state. Such distinctions can reduce unnecessary alarms and help determine whether operator intervention is indeed required.

The information available for automated monitoring has also expanded considerably. Earlier generations of field devices often provided little more than a single analogue process value, whereas modern digital field devices can communicate additional information about device status, detected faults, calibration, operating conditions, and measurement quality. Many devices also include self-diagnostic functions. Monitoring systems can therefore assess not only the behavior of the process variable, but also the condition and reliability of the instrument providing it. This additional information can improve anomaly assessment and help prevent instrument-related deviations from being presented to operators as process problems.

Figure 3 illustrates how large numbers of machine-detected anomalies can be transformed into a smaller, more manageable set of human-facing alarms. As industrial plants become increasingly automated, fewer human supervisors will be responsible for supervising larger plant areas, making their available cognitive capacity an increasingly scarce resource. Human supervisor attention should therefore be reserved for situations that require human awareness, judgement, coordination, or intervention, while duplicate, expected, or low-value events should be suppressed, correlated, or handled automatically. The objective is to use limited human attention where it provides the greatest operational value.

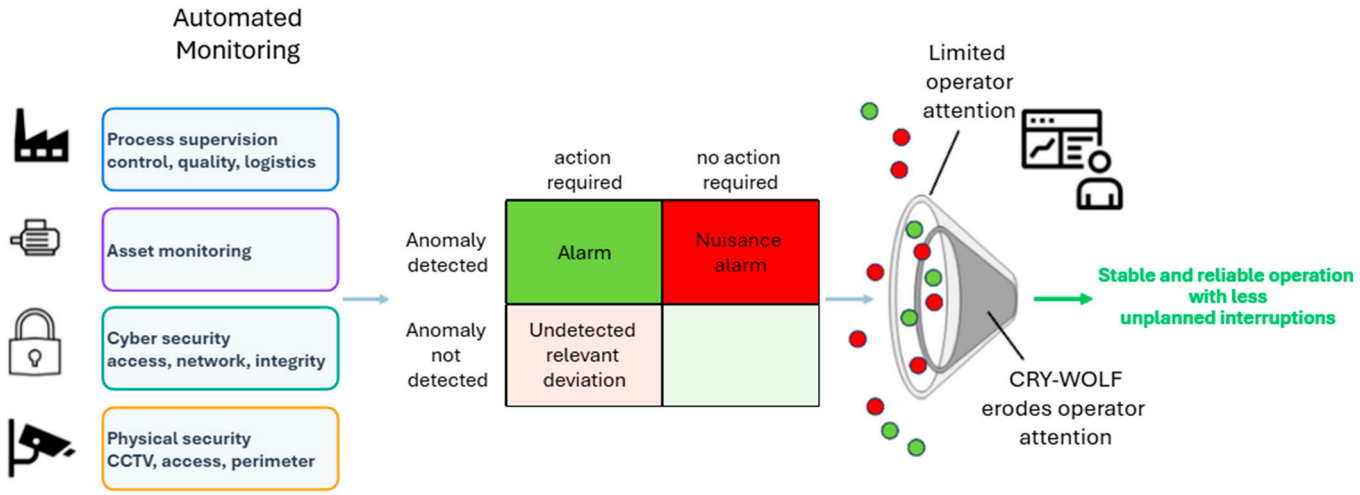


Figure 3. Nuisance alarms consume attention and increase the risk of missed alarms.

Although human supervisors can tolerate and filter a certain number of nuisance alarms, excessive nuisance alarms increase workload and reduce responsiveness to subsequent alarms. As alarm reliability deteriorates, genuinely important alarms are more likely to be overlooked or acted upon too late. From the perspective of effective human supervision, nuisance alarms therefore carry a substantial cost of their own and must be considered alongside undetected relevant deviations when evaluating the performance of monitoring systems.

4.4. Alarm Management

Alarm management [13,17,28,29] treats alarms as the boundary between automated monitoring and human intervention: an alarm should be generated only when the automation cannot adequately manage a developing situation and timely operator action is required. As Goel et al. [30] emphasize, alarms are a primary communication channel between the automated control system and the operator and, together with timely operator intervention, form an important layer of protection against escalating process disturbances. Alarm-system quality depends less on the number of detectable deviations than on whether each alarm is relevant, timely, understandable, appropriately prioritized, and associated with a defined operator response [11].

Alarm-system performance should therefore not be assessed solely by alarm quantity. Dorgo et al. [12] show that conventional performance measures are strongly dominated by alarm-load metrics, whereas qualitative properties such as informativeness and actionability receive considerably less attention

The ease with which alarms can be configured in modern control systems has, however, led to a rapid growth in their number, often without a corresponding assessment of their operational value. Standing, chattering, repeating, redundant, poorly prioritized, or otherwise irrelevant alarms consume limited operator attention and can develop into alarm floods that exceed the operator's ability to detect, diagnose, and respond to critical events. Effective alarm management must therefore be maintained as a continuous lifecycle process involving systematic rationalization, appropriate limit and priority settings, documented design intent, performance monitoring, maintenance, management of change, and continuous improvement. Advanced techniques such as state-based suppression, alarm-flood analysis, and decision support can further reduce unnecessary operator load by identifying recurring alarm patterns, distinguishing initiating causes from consequential alarms, and providing validated diagnostic guidance. Such methods must remain robust, explainable, and governed so that safety-critical information is not inadvertently suppressed. The objective is not to present every detectable deviation, but to provide a manageable number of reliable and actionable alarms that direct operator attention to situations in which human assessment or intervention is required.

4.5. Changes over the Plant Lifecycle

Once commissioned, a control system gradually diverges from the assumptions on which its original design was based [13,17]. Over the plant lifecycle, equipment ages, instruments drift, production requirements change, raw-material properties vary, and environmental or regulatory constraints evolve. Components are replaced, process sections are modified, and new control strategies are added to existing automation. At the same time, operators and engineers gain practical knowledge that may reveal limitations in the original alarm design. These developments affect which alarms remain relevant, how they behave, and how they should be prioritized and presented. Without systematic monitoring, review, and management of change, even a carefully designed alarm configuration will deteriorate over time, leading to increasing numbers of nuisance, stale, and standing alarms.

4.6. Alarm Floods

During a propagating abnormal situation, numerous consequential, redundant, or chattering alarms may obscure the initiating alarm and compete for limited attention. This degrades operators' situation awareness—that is, their ability to perceive relevant process information, understand its significance, and anticipate how the situation is likely to develop—thereby delaying diagnosis and increasing the likelihood that critical alarms or process conditions will be overlooked [31]. Prolonged alarm floods also increase cognitive workload and fatigue, making inappropriate or incomplete intervention more likely. As a result, the alarm system can cease to support recovery with potential consequences for plant safety, availability, product quality, and production [13].

During the design of monitoring systems, alarms are often added according to a "better safe than sorry" principle, even when it is uncertain whether the detected condition will indeed require operator attention. However, once the limited availability of human attention and the cry-wolf effect are considered, this conservative approach becomes problematic. Nuisance alarms are not harmless: they consume attention, increase workload, and reduce confidence in the alarm system [32]. From the perspective of effective human supervision, nuisance alarms therefore cannot be treated as cost-free errors and should be considered alongside missed detections.

5. Discussion

Industrial plants are increasingly equipped with monitoring systems capable of detecting deviations across multiple domains, including process operation, asset condition, cybersecurity, and physical security. At the same time, increasing levels of automation allow fewer operators to supervise progressively larger and more complex plant areas. This creates an important shift in the monitoring problem. The technical capability to detect abnormalities is expanding rapidly, whereas the human capacity to interpret and respond to the resulting events remains fundamentally limited. Human attention therefore becomes a critical design constraint for future supervisory systems.

This has important implications for how monitoring performance should be evaluated. A monitoring system should not be considered effective simply because it detects a large fraction of abnormal conditions. Each event presented to the operator consumes cognitive resources and competes with other events for attention. Events that are technically correct but operationally irrelevant can therefore reduce overall supervisory performance. In particular, excessive nuisance alarms increase workload and may erode trust in the monitoring system. Consequently, monitoring systems should be optimized not only for high detection rates, but also for the quality, relevance, and actionability of the information presented to the operator.

The design objective should therefore shift from maximizing detection toward maximizing the operational value of human attention. Automated systems should perform continuous low-level surveillance, correlation, filtering, and routine responses, while human operators should be involved primarily when contextual judgement, coordination, diagnosis, or intervention is required. This principle provides a common framework for integrating process monitoring, asset management, cybersecurity, and physical-security monitoring within increasingly autonomous industrial plants.

5.1. From Detection to Meaningful Escalation

Meaningful escalation is the supervisory allocation decision that determines whether, when, and to whom a machine-detected deviation should be escalated after its operational context has been assessed. The possible outcomes include no further action, automated resolution, deferred human review, or timely human attention. Meaningful escalation is

therefore not an alternative detection, diagnosis, correlation, or alarm-management method; rather, it uses the outputs of these functions to determine the appropriate recipient and mode of response (Table 2).

Table 2. Relating basic concepts to meaningful escalation.

Concept	Principal Question	Relationship to Meaningful Escalation
Anomaly detection	Is there a difference from normal?	Generates candidate events
Fault diagnosis	What is the root cause?	Provides context
Alarm rationalization	Should this be an alarm, which priority and action?	Design time mechanism
Alarm suppression and filtering	Should this alarm currently be hidden?	Runtime mechanism
Meaningful escalation	Does this warrant human attention, when, and by whom?	Integrative supervisory allocation decision

The focus of industrial monitoring needs to move from detection toward meaningful escalation. Reis and Gins [8] describe the development of process monitoring as a progression from detection, through diagnosis, toward prognosis. Earlier approaches concentrated primarily on identifying deviations as rapidly and reliably as possible. However, further reductions in detection time may provide limited operational benefit if the subsequent diagnosis, interpretation, and troubleshooting remain slow or uncertain. In many abnormal situations, determining what has happened, why it has happened, and what should be done is more difficult than recognizing that some deviation has occurred.

Monitoring should therefore not terminate with the detection of an abnormal signal. Detected deviations should be evaluated according to their operational relevance, likely consequences, persistence, relationship to other events, and the need for human intervention. Where possible, monitoring systems should correlate related deviations, identify likely initiating causes, suppress consequential or redundant events, and provide information that supports diagnosis and decision-making.

This distinction becomes increasingly important as advanced analytics and machine-learning methods make it possible to detect increasingly subtle deviations. Greater sensitivity can improve early fault detection, but it can also increase the number of marginal or uncertain events. A technically sensitive monitoring system may therefore perform poorly from a supervisory-control perspective if it continuously presents operators with conditions that do not require action. The relevant question is therefore not only whether an abnormality can be detected, but whether it should be escalated to the human operator. The system should determine whether the detected condition has sufficient operational significance to justify consuming scarce operator attention. Events that can be handled reliably by automation should remain within the automated control and monitoring layers, whereas situations involving uncertainty, conflicting objectives, unusual conditions, or significant operational consequences should be escalated.

5.2. Cross-Domain Integration of Monitoring Information

This requires monitoring information to be considered across traditional organizational and technical boundaries. Process disturbances, asset degradation, cybersecurity incidents, and physical-security events cannot always be interpreted independently because

similar symptoms may have different underlying causes. A change in process behavior may originate from raw-material variability, equipment degradation, an instrumentation fault, an incorrect control action, or malicious manipulation. Determining the appropriate response therefore requires both technical information about the deviation and contextual information about the current operating situation.

Reis and Gins [8] emphasize the value of integrating process and maintenance information, while Hu et al. [33] demonstrate the benefits of combining process measurements, alarm and event histories, and process-connectivity information.

The same principle should be extended beyond process and maintenance monitoring. Cybersecurity and physical-security information may provide important context for interpreting unusual plant behavior. For example, a process deviation accompanied by unexpected network activity or unauthorized access should be assessed differently from an identical process deviation occurring during normal operating conditions. Conversely, an apparent cybersecurity anomaly may have little operational relevance unless it affects systems or assets that are important to the current production state. The Stuxnet incident [34] illustrates why monitoring domains cannot always be treated independently. A cyber intrusion manipulated the industrial process and caused abnormal equipment failures, while simultaneously falsifying the information presented to operators. Consequently, the observable event was initially an asset/process anomaly rather than an identifiable cybersecurity event. Cross-domain integration does not imply that control-room operators should become cybersecurity specialists. Security Operations Center personnel or cybersecurity specialists should remain responsible for interpreting network and system-level indicators and coordinating cyber incident response, while control-room operators assess process consequences and determine safe operational actions. Maintenance specialists contribute asset condition information, and physical-security personnel investigate access or perimeter events. Cross-domain correlation should combine these partial views into a common situation representation and route the resulting event to the personnel capable of acting, with escalation to the control room whenever process safety, availability, or local intervention is affected. Future monitoring architectures should therefore move toward cross-domain event correlation. Rather than presenting operators with separate streams of process alarms, maintenance, cybersecurity and security alarms, the system should combine related information into a smaller number of operationally meaningful situations. Such aggregation can reduce duplicate information, improve causal interpretation, and provide operators with a more coherent representation of what is happening in the plant.

5.3. Human Attention as a Design Constraint

Human attention should be treated explicitly as a limited system resource [35]. In highly automated plants, operators are expected to supervise large numbers of control loops, assets, and increasingly also events originating from cybersecurity and physical-security systems. While automation can increase the amount of information that is monitored, it does not increase the cognitive capacity of the human operator.

At the same time, the nature of the information generated by automation has changed. Earlier field instrumentation primarily provided individual process measurements. Modern systems increasingly add interpretation at several levels: smart field devices provide self-diagnostics, condition-monitoring systems assess vibration and equipment health, advanced control systems monitor constraints and control performance, and data-driven and machine-learning methods detect anomalies, diagnose faults, and generate predictions. Asset-management, cybersecurity, and physical-security systems contribute additional event streams. Consequently, modern automation does not merely provide more measure-

ments; it produces an increasing amount of derived and interpreted information that may potentially be escalated to a human operator (Figure 4).

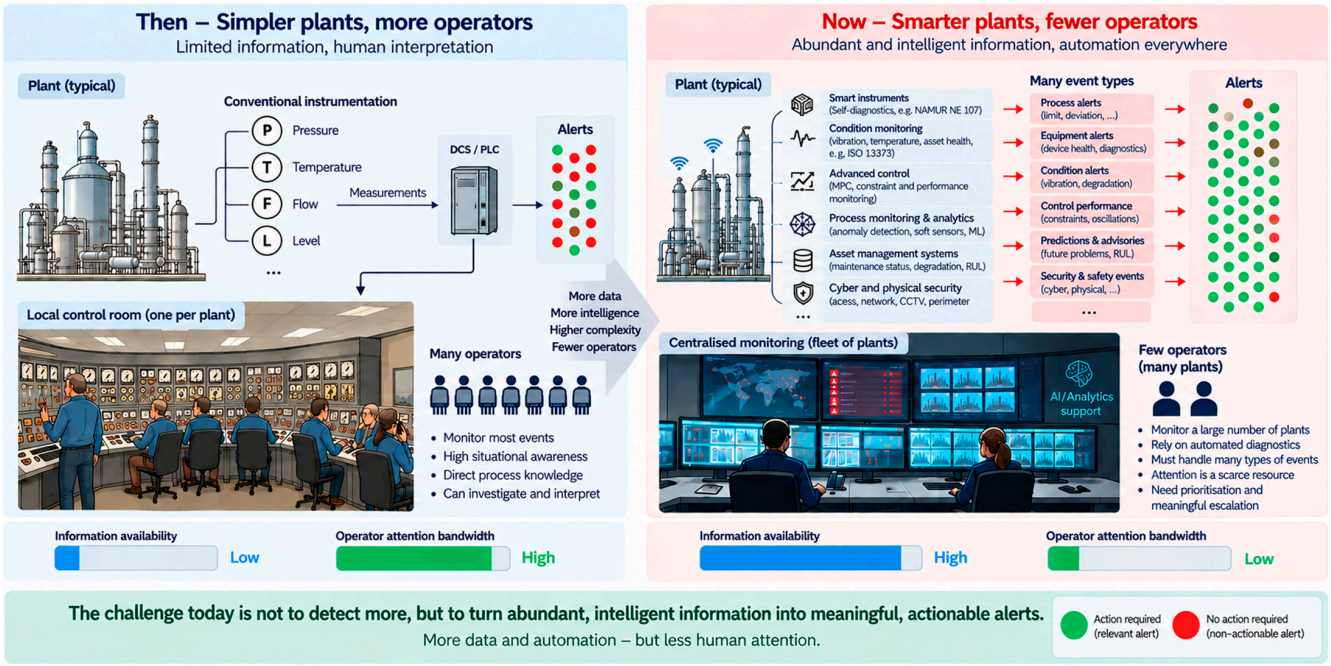


Figure 4. From information scarcity to attention scarcity in industrial supervision.

This development creates a fundamental asymmetry between machine-based monitoring and human supervision. Automated systems can continuously evaluate thousands of measurements and derived indicators, whereas a human operator can actively assess only a limited number of concurrent situations. The limiting factor therefore shifts from the ability to acquire and detect information toward the ability to determine which information deserves human attention. A monitoring architecture that transfers increasing amounts of machine-level output directly to the operator merely moves the monitoring bottleneck from the automation system to the human supervisor.

Alarm floods further intensify this problem by overwhelming the operator's capacity to perceive, understand, and project the development of the situation, thereby degrading situation awareness [31].

5.4. Implications for Future Monitoring Systems

The principal challenge for future industrial monitoring systems is therefore not simply to detect more abnormalities, but to determine which detected abnormalities deserve human attention. This requires a stronger separation between machine-level detection and human-facing event generation. Detection algorithms may operate with relatively high sensitivity internally, provided that subsequent processing evaluates context, combines related information, suppresses duplicates, and determines whether escalation is justified.

Such systems should ideally support several levels of response. Routine and well-understood deviations should be corrected automatically where this can be done safely. Events that require no immediate action may be logged for maintenance, engineering analysis, or later review without interrupting the operator. Only situations requiring timely human awareness, judgement, coordination, or intervention should generate human-facing events.

This approach also changes how monitoring-system quality should be assessed. Performance metrics such as sensitivity, specificity, precision, and detection delay remain

important, but they are insufficient on their own. A monitoring system ultimately contributes value only if it improves the ability of the plant to remain safe, reliable, and available. Operator workload, alarm rate, actionability, diagnostic value, trust, and the probability that critical events are successfully recognized should therefore also be considered.

The long-term objective should be an attention-aware supervisory architecture in which automated monitoring systems protect rather than consume human cognitive resources. As plants become more autonomous, the operator's role will increasingly concentrate on situations that are unusual, ambiguous, consequential, or difficult to automate. Monitoring systems should consequently be designed to ensure that, when such situations occur, the operator's limited attention remains available for the events in which human judgement provides the greatest value.

6. Conclusions

Monitoring of industrial plants is becoming increasingly automated, while human supervisors remain responsible for situations that require judgement, coordination, and intervention. As monitoring capabilities expand across process, asset, cybersecurity, and physical-security domains, the central challenge is no longer only to detect deviations, but to decide which deviations deserve human attention. Avoiding human-facing events without operational value is therefore a key design objective. In highly automated plants, nuisance alarms are no longer merely inefficient; they are incompatible with the need to protect scarce human attention. Monitoring systems should suppress, aggregate, defer, or automatically handle events whenever possible and escalate only those situations that require timely human involvement. Treating human attention as a limited supervisory resource provides a common design principle for monitoring and alarm systems in increasingly autonomous plants.

Future research should focus on cross-domain monitoring architectures that integrate process, asset, cybersecurity, and physical-security information. This will become increasingly important as critical infrastructure faces growing security threats while fewer human supervisors are responsible for larger and more automated facilities. The central challenge is not merely to detect more anomalies, but to correlate and interpret them sufficiently well to escalate only those situations that genuinely require human attention. Empirical studies in highly automated and normally unattended plants are also needed to determine how meaningful-escalation strategies affect workload, trust, situation awareness, and the probability of successful intervention.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding author.

Acknowledgments: The author would like to thank his colleague Ruomu Tan and the anonymous reviewers for their valuable feedback and constructive suggestions, which helped to improve the quality of this manuscript. I also gratefully acknowledge the MDPI editorial staff for their professional editing support and their assistance throughout the publication process. During the preparation of this manuscript, the author used ChatGPT for the purposes of generating Figures 2 and 4 from text prompts and to check spelling, grammar and language. The author has reviewed and edited the output and take full responsibility for the content of this publication.

Conflicts of Interest: No additional competing interests exist apart from the institutional affiliation.

References

1. Hollender, M. *Collaborative Process Automation Systems*; ISA: Triangle Park, NC, USA, 2010; ISBN 978-1-936007-10-3.
2. Gamer, T.; Hoernicke, M.; Kloepper, B.; Bauer, R.; Isaksson, A.J. The Autonomous Industrial Plant—Future of Process Engineering, Operations and Maintenance. *J. Process Control* **2020**, *88*, 101–110. [CrossRef]
3. Hollender, M. Process Automation: Industrial Process Operation 4.0. In *ISA Intech*; ISA: Triangle Park, NC, USA, 2019.
4. Wilhelm, J.; Freitag, M. Operator Role Classification in Human-Automation Interaction: A Systematic Review. *IFAC-PapersOnLine* **2024**, *58*, 1276–1281. [CrossRef]
5. Sheridan, T.B. *Telerobotics, Automation, and Human Supervisory Control*; MIT Press: Cambridge, MA, USA, 1992; ISBN 978-0-262-19316-0.
6. Parasuraman, R.; Sheridan, T.B.; Wickens, C.D. A Model for Types and Levels of Human Interaction with Automation. *IEEE Trans. Syst. Man Cybern.-Part Syst. Hum.* **2000**, *30*, 286–297. [CrossRef] [PubMed]
7. Leach, P.; Wright, M.; King, S. *A Guide to Enhancing Process Safety and Plant Efficiency through the Competence of Control Room Operators (CROs)*; Institution of Chemical Engineers Symposium Series; Institution of Chemical Engineers: Edinburgh, UK, 2014.
8. Reis, M.S.; Gins, G. Industrial Process Monitoring in the Big Data/Industry 4.0 Era: From Detection, to Diagnosis, to Prognosis. *Processes* **2017**, *5*, 35. [CrossRef]
9. Li, S.; Zhou, B.; Shang, J.; Chen, X.; Yu, J. Review of Recent Applications and Future Perspectives on Process Monitoring Approaches in Industrial Processes. *J. Manuf. Syst.* **2025**, *82*, 509–530. [CrossRef]
10. Qin, S.J.; Chiang, L.H. Advances and Opportunities in Machine Learning for Process Data Analytics. *Comput. Chem. Eng.* **2019**, *126*, 465–473. [CrossRef]
11. Mustafa, F.E.; Ahmed, I.; Basit, A.; Alvi, U.-E.-H.; Malik, S.H.; Mahmood, A.; Ali, P.R. A Review on Effective Alarm Management Systems for Industrial Process Control: Barriers and Opportunities. *Int. J. Crit. Infrastruct. Prot.* **2023**, *41*, 100599. [CrossRef]
12. Dorgo, G.; Tandari, F.; Szabó, T.; Palazoglu, A.; Abonyi, J. Quality vs. Quantity of Alarm Messages—How to Measure the Performance of an Alarm System. *Chem. Eng. Res. Des.* **2021**, *173*, 63–80. [CrossRef]
13. Hollender, M.; Manca, G.; Isaksson, A. Modern Methods for Alarm Management. In *Process Control*; Elsevier: Amsterdam, The Netherlands, 2026; pp. 191–211. ISBN 978-0-443-44103-5.
14. Jardine, A.K.S.; Lin, D.; Banjevic, D. A Review on Machinery Diagnostics and Prognostics Implementing Condition-Based Maintenance. *Mech. Syst. Signal Process.* **2006**, *20*, 1483–1510. [CrossRef]
15. Gangsar, P.; Tiwari, R. Signal Based Condition Monitoring Techniques for Fault Detection and Diagnosis of Induction Motors: A State-of-the-Art Review. *Mech. Syst. Signal Process.* **2020**, *144*, 106908. [CrossRef]
16. Giacotto, A.; Marques, H.C.; Martinetti, A. Prescriptive Maintenance: A Comprehensive Review of Current Research and Future Directions. *J. Qual. Maint. Eng.* **2025**, *31*, 129–173. [CrossRef]
17. *ISA 18.2*; Management of Alarm Systems for the Process Industries. ISA: Triangle Park, NC, USA, 2016.
18. Stouffer, K.; Pease, M.; Tang, C.; Zimmerman, T.; Pillitteri, V.; Lightman, S.; Hahn, A.; Saravia, S.; Sherule, A.; Thompson, M. *Guide to Operational Technology (OT) Security*; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023.
19. Butrimas, V. *Defending Critical Infrastructure: The Challenge of Securing Industrial Control Systems*; The European Centre of Excellence for Countering Hybrid Threats: Helsinki, Finland, 2022.
20. Litjens, R.; Henkel, H.-J.; Opmeer, J. Achieving Autonomous Operations: An End-User Focussed Approach and Maturity Model by WIB/NAMUR. *ATP Mag.* **2025**, *67*, 77–81.
21. *NAMUR NE107*; Self-Monitoring and Diagnosis of Field Devices. NAMUR: Monheim, Germany, 2017.
22. Rehman, M.U.; Bahşi, H. Process-Aware Security Monitoring in Industrial Control Systems: A Systematic Review and Future Directions. *Int. J. Crit. Infrastruct. Prot.* **2024**, *47*, 100719. [CrossRef]
23. Isermann, R. *Fault-Diagnosis Systems*; Springer: Berlin/Heidelberg, Germany, 2006; ISBN 978-3-540-24112-6.
24. Bliss, J.P.; Dunn, M.C. Behavioural Implications of Alarm Mistrust as a Function of Task Workload. *Ergonomics* **2000**, *43*, 1283–1300. [CrossRef] [PubMed]
25. Breznitz, S. *Cry Wolf: The Psychology of False Alarms*; Lawrence Erlbaum Associates: Mahwah, NJ, USA, 1984.
26. Bainbridge, L. Ironies of Automation. *Automatica* **1983**, *19*, 775–779. [CrossRef]
27. Qin, S.J. Survey on Data-Driven Industrial Process Monitoring and Diagnosis. *Annu. Rev. Control* **2012**, *36*, 220–234. [CrossRef]
28. *EEMUA 191*; Alarm Systems—A Guide to Design, Management and Procurement. EEMUA: London, UK, 2024. Available online: https://www.eemua.org/Products/Publications/Print/EEMUA-Publication-191.aspx (accessed on 15 October 2019).
29. *IEC 62682*; Management of Alarms Systems for the Process Industries. IEC: Geneva, Switzerland, 2022.
30. Goel, P.; Datta, A.; Mannan, M.S. Industrial Alarm Systems: Challenges and Opportunities. *J. Loss Prev. Process Ind.* **2017**, *50*, 23–36. [CrossRef]
31. Endsley, M.R. Toward a Theory of Situation Awareness in Dynamic Systems. *Hum. Factors* **1995**, *37*, 32–64. [CrossRef]
32. Parasuraman, R.; Riley, V. Humans and Automation: Use, Misuse, Disuse, Abuse. *Hum. Factors* **1997**, *39*, 230–253. [CrossRef]

33. Hu, W.; Shah, S.L.; Chen, T. Framework for a Smart Data Analytics Platform towards Process Monitoring and Alarm Management. *Comput. Chem. Eng.* **2018**, *114*, 225–244. [CrossRef]
34. Zetter, K. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*; Crown: New York, NY, USA, 2014; ISBN 978-0-7704-3617-9.
35. Wickens, C. Multiple Resources and Mental Workload. *Hum. Factors J. Hum. Factors Ergon. Soc.* **2008**, *50*, 449–455. [CrossRef] [PubMed]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.