Global Academic Journal of Economics and Business

Available online at https://www.gajrc.com
DOI: https://doi.org/10.36348/gajeb.2026.v08i05.004

OPEN ACCESS

ISSN: 2706-9001 (P)
ISSN: 2707-2584 (O)

Original Research Article

Enhancing Process Safety in Smart Oil and Gas Facilities through Integrated SIS, DCS and Real-Time Instrumentation Analytics

Mohammed Juned Nijami[1*]
[1]Independent Researcher

***Corresponding Author**
Mohammed Juned Nijami
Independent Researcher

Article History
Received: 07.07.2026
Accepted: 02.09.2026
Published: 07.09.2026

Abstract: At present, intelligent oil and gas facilities are using safety instrumented systems (SIS), distributed control systems (DCS), connected field instrumentation, historians, edge computing, and advanced analytics. Although the large amount of data generated can improve process safety, this benefit can only be achieved if the analytical integration still satisfies the required standards concerning independence, determinism, and assurance for safety functions. This article looks at how the SIS, the DCS, and the real-time instrumentation analytics can be combined so as to establish an evidence architecture that helps in the early detection of abnormal conditions, the evaluation of barrier health, the contextuation of alarms, and the provision of risk-informed support for human decision-making. A structured integrative review has been carried out in line with the PRISMA 2020 and PRISMA-S reporting guidelines in order to summarise the peer-reviewed and credible literature published between 2020 and 2025. The evidence is divided into five areas: functional-safety architecture, control and alarm management, instrumentation data quality, fault diagnosis and dynamic risk analytics, and cyber-human assurance. The synthesis shows that the most defensible design is not one in which the analytics control the SIS, but rather a layered architecture in which both the SIS and the DCS keep their present operational roles while authenticated, time-aligned, read-only data are sent to an independent analytics environment. This setup allows for predictive and contextual insights absent creating an unverified actuation path into the protection layers. The paper suggests an assured integration architecture and a five-level implementation maturity model. It concludes that the future value for process safety will depend less on the novelty of the algorithms themselves and more on traceable measurements, validated models, secure interfaces, explainable outputs, disciplined management of change, and clear human authority over safety-critical decisions.

Keywords: Safety Instrumented Systems (SIS); Distributed Control Systems (DCS); Process Safety; Real-Time Instrumentation Analytics; Functional Safety.

1. INTRODUCTION

The production, processing, transport and refining of oil and gas rely on a number of closely interrelated physical processes, and if any deviations occur they can very quicklya lead to a loss of containment, a fire, an explosion, toxic exposure, an environmental release or a prolonged shutdown. In view of this, traditional safety measures have employed a number of layers: basic process control is responsible for making sure that the system functions normally, alarm systems notify the operators of any deviations, and separate protection systems such as

the SIS are put into operation when hazardous conditions have arisen and a safety response is needed. The shift towards digitalisation does not eliminate the layered approach to protection; instead it alters the quantity, speed and extent of the information available to each layer. Today's facilities are able to store process values, diagnostic codes, alarm sequences, valve signatures, maintenance records and equipment-health data, and analytical tools can identify relationships which are hard to spot when one only examines individual tags or relies on fixed thresholds. Reviews of digital process safety have shown that operational data can lead to faster monitoring, quicker fault identification and better risk management, but they also point out that they add cyber-physical complexity and increase the dependence on the quality of the data (Pasman *et al*., 2022; Amin *et al*., 2022).

The issue of process safety is not one of whether or not more data should be collected, but rather about the way in which the data should be used without weakening the safeguards it is meant to support. A DCS is designed for continuous regulation, sequencing, visualisation, and the management of alarms. In contrast, an SIS is based on safety instrumented functions, and the sensors, logic solvers, final elements, and proof tests it includes are all subject to a functional-safety lifecycle. On the other hand, analytics platforms are generally probabilistic, are continually updated, and rely on sizable datasets, software libraries, network services, or cloud-edge infrastructure. If these three environments are treated as if they were the same, the differences in their failure modes and assurance requirements would be hidden. In the case of the petroleum industry, research has cautions that greater connectivity can pose a threat to the security and independence of process control and safety systems, particularly when remote data access crosses the traditional architectural boundaries (Onshus *et al*., 2022; Zhu & Liyanage, 2021).

It is just as wasteful to keep the different systems completely separate, as in that situation useful safety data is lost. Instrumentation failures can occur gradually for a variety of reasons, such as drift, noise, stiction, broken communication links, fouling, blocked impulse lines, changes in calibration, or stress resulting from the environment. Data-driven techniques can detect patterns involving multiple variables before a normal high-high alarm or shutdown takes place. Research into the application of machine learning in engineering risk assessment and in the diagnosis of process faults shows an increasing capacity to identify abnormal states, classify faults, monitor how they develop, and help personnel to make decisions more quickly (Hegde & Rokseth, 2020; Arunthavanathan *et al*., 2021a). Moreover, big-data tools allow safety data to be examined across a range of incidents, assets, methods of operation, and time periods, rather than being analysed one at a time (Wang & Wang, 2021; Sattari *et al*., 2021). These advances are of great importance for intelligent oil and gas facilities, since the same process variables are used for control, alarm, maintenance, and protection decisions, but each of these applications demands a different level of trust in the data.

The review presents an integration model based on evidence and aims to incorporate all the findings that are typically observed, without selecting any single source as the basis for taking safety actions. In this model the SIS continues to be responsible for the deterministic safety functions; the DCS keeps the role it currently has in operational control and in handling alarms; and a separate analytics layer takes in curated versions of the process and device data in order to produce advisory safety intelligence. The architecture has to ensure that data provenance, synchronisation, quality, cybersecurity, model validation, and human interpretation are all observable. This approach goes beyond the existing body of research in the area of digital process safety by concentrating on the boundary conditions which allow a useful integration between the SIS, the DCS and the analytics system while at the same time preserving the functional independence of each component.

2. Aim and Review Objectives

This review seeks to establish a conceptual framework which will guarantee safety whenever the SIS, DCS, and the real-time instrumentation analytics are used together in smart oil and gas facilities, on the understanding that analytical outputs that have not been verified must not be used in any safety-critical actions. The framework is built upon four objectives. The first of these is to make clear the separate roles and to specify the information flows that are allowed between the field instrumentation, the SIS, the DCS, the historians, the edge or cloud analytics, and the operator decision systems. The second objective involves assessing how much real-time analytics can enhance the leading indicators of process safety, such as sensor health, alarm context, the detection of abnormal conditions, the availability of barriers, and dynamic risk. The third objective is to determine the assurance conditions necessary for the reliable use of these analytics, with specific attention given to measurement quality, model validation, cybersecurity, explainability, human factors, and the management of change. The fourth objective is to suggest a staged maturity model that enables operators to take up analytical capabilities in a step-by-step way while at the same time maintaining unambiguous safety authority that can be audited.

3. METHODOLOGY

An integrative review based on a structured approach was chosen since the research question involves functional safety, process control, instrumentation, data analytics, cybersecurity, and human decision making rather than focusing on a single intervention that could serve as the foundation for a statistical meta-analysis. The report was prepared in line with the PRISMA 2020 guidelines and the PRISMA-S extension, with particular attention paid to defining clear eligibility criteria, documenting the search process, and ensuring that the synthesis could be reproduced (Page *et al*., 2021; Rethlefsen *et al*., 2021). The review period spanned from January 2020 to December 2025 so that all the evidence referred to in the text corresponds to the time frame specified for this study and also considers the rapid developments that have taken place in Industry 4.0 and in real-time process-safety research.

The search terms were drawn from the following expressions: "safety instrumented system", "SIS", "distributed control system", "DCS", "basic process control system", "oil and gas", "refinery", "petrochemical", "process safety", "instrumentation", "real-time analytics", "fault diagnosis", "dynamic risk", "alarm management", "digital twin" and "operational technology security". Where possible, the journal articles related to Scopus and the Web of Science were acquired directly from the publishers' own websites and scholarly databases, and in cases where a peer-reviewed source could not be used, authoritative technical guidance was used as a substitute for a normative security function. A source was only considered eligible if it dealt with the process industries or oil and gas operations and made a direct contribution to at least one of the five synthesis areas: safety-control architecture, DCS and alarms, instrumentation or data quality, real-time fault or risk analytics, or cyber-human assurance. Publications that were concerned solely with reservoir optimisation, those involving commercial analytics with no safety relevance, papers published before 2020, non-English materials and citations that could not be verified were excluded from being directly cited.

Thirty sources were used in the synthesis. Each of these sources was given a code according to its system layer, data type, analytical purpose, safety contribution, main limitation, and assurance implication. The evidence was compared thematically rather than being ranked solely on the basis of algorithmic accuracy since benchmark performance does not prove that a technology is suitable for use in a safety lifecycle. The review also makes a distinction between descriptive evidence and the proposed framework: the previously published studies provide information about capabilities and constraints, while the reference architecture and maturity model described in this paper are integrative constructions that have been developed from the patterns observed in the sources. Since the study designs, process contexts, datasets, and outcome metrics vary, no pooled effect size has been reported. This approach enables the review paper to be logically reproducible without making false claims about the relative safety value of different technologies.

4. Functional-Safety and Control Architecture

It is important when planning a smart facility to establish well-defined roles. The field instruments carry out the measurement of a number of parameters, including pressure, temperature, flow, level, composition, vibration, valve position and other values which indicate the state of the process and the condition of the equipment. The DCS or the basic process control system makes use of these measurements in order to regulate the process, carry out sequences, display graphics and handle operational alarms. The SIS on its own assesses the safety-related inputs and sets in motion the pre-determined actions when a hazardous situation goes beyond the logic set up for a safety instrumented function. These functions must remain separate since, in the event of a control failure, a software defect or a cyber incident, any protective measure which is regarded as one that reduces risk should not be quietly diminished. Research into the automation of the petroleum industry indicates that digital integration can cause these boundaries to become blurred when the safety and control networks are connected together for the purpose of data exchange, maintenance or remote engineering (Onshus *et al*., 2022).

The review thus supports asymmetric integration: even though the safety and control systems send data to a monitoring and analytics environment, analytical services should not be given regular write access to the SIS logic, the trip setpoints, the bypass states or the final elements. The NIST guidance on operational technology also stresses the importance of security measures that involve network segmentation, access control and the monitoring of interfaces, while at the same time taking into account the performance, reliability and safety requirements of OT (Stouffer *et al*., 2023). In practice, the architecture could make use of replicated historians, data diodes or closely controlled gateways, demilitarized zones, authenticated message brokers, and role-based engineering access. Whatever the specific technical mechanism may be, the principle remains unchanged: analytical convenience must not result in an unexamined common-cause path.

Another principle is that the meaning of the measurements should be kept separate from that of the decisions. For instance, even if the same reading from a pressure transmitter is shown in the DCS trend, is used to feed a predictive model, and is given as the reason for a safety trip, the level of validity required in each of these situations is different. In order to make safety decisions it is necessary to have traceable calibration, to know the failure characteristics, to carry out a proof-testing procedure, and to maintain configuration control. Analytics, by contrast, can make use of soft sensors, calculated features, inferred states, or a combination of data from a number of instruments. Although these derived variables can be very helpful for advisory diagnosis, they should not be regarded as equivalent to a certified safety input merely because they are correlated with a hazard. Research into the quality of decisions regarding emergency shutdown systems also indicates that the value of the data depends on how it is transformed into information for safety-critical maintenance and inspection decisions (Zhu *et al.*, 2021).

The third principle involves temporal context as the trips are intentionally designed to be deterministic and quick, in contrast to deterioration which generally occurs over hours, days or months. It is possible to identify drift, repeated excursions near the threshold, nuisance alarms, oscillation, control-valve stiction, or an increasing demand on the protective functions by means of DCS historians and device diagnostics. Analytics can therefore be used during the period before a trip is required, providing an early signal of the stress being placed on the barriers. These insights are most valuable when they result in confirmed human actions such as an inspection, a calibration, alarm rationalisation, a review of the operating envelope, or the management of change, rather than when they prevent the normal protection lifecycle from being followed. This separation allows smart analytics to improve the conditions surrounding the SIS while the SIS continues to function as the final independent automated protection against the specified scenarios.

5. Real-Time Instrumentation Analytics for Process Safety

Real-time instrumentation analytics starts by making sure that the data is of good quality, not by choosing a model. The process data may contain missing values, have timestamp offsets, show discontinuities caused by maintenance, include frozen signals, suffer from sensor bias, involve changes in operating mode, be affected by compression, and exhibit relationships resulting from control loops. For this reason, data-driven research in the field of process safety puts a strong focus on preprocessing, synchronization, feature construction and taking the context into account before carrying out any statistical or machine-learning analysis (Bai *et al*., 2022; Wanasinghe *et al*., 2022). In the case of a safety application, these steps are not just ordinary data-science tasks. A model which is unable to tell the difference between a transmitter undergoing calibration and a real process deviation can lead to alarm fatigue, while a model trained on unlabelled abnormal operation might end up treating unsafe behaviour as though it were normal. Data-quality rules must therefore be regarded as assurance controls and should have clear ownership, defined thresholds, and procedures for managing exceptions.

Fault detection and diagnosis offers the most direct analytical link between the instrumentation and process safety. Unsupervised and cognitive methods have proven their ability to detect process faults that have not been seen before and to update fault categories as new states appear (Arunthavanathan *et al*., 2020). Bayesian-network methods are able to combine multivariate statistical reduction involving probabilistic dependency frameworks in order to identify fault conditions and the likely causal channels (Amin *et al*., 2021). Deep learning allows the acquisition of temporal signatures and the forecasting of fault progression, including the early symptoms that occur before complete functional failure (Arunthavanathan *et al*., 2021b). More recent research has gone even further in this direction by using multiscale convolutional and recurrent models, which can learn local transients and longer time relationships in complex industrial datasets (Zhao *et al*., 2024). The various studies referenced all indicate a move away from monitoring that depends solely on thresholds towards a type of surveillance that is pattern aware.

To regard accuracy with benchmark data as equivalent to safety integrity is a mistake. Actual plants vary in the type of feedstock, in their operating rates, in their equipment arrangements, in the condition of their catalysts, in the ambient conditions, and in their control strategies. In situations involving multimode behaviour, a normal transition may appear abnormal or a fault might be hidden if the model's baseline is not appropriate. Explainable artificial intelligence is relevant in this context since operators need to know which variables caused an alert and whether the explanation is in line with the principles of process physics. Bhakte *et al*., (2024) offer mode-specific explainability for deep fault-detection models, and Zhou *et al*., (2024) demonstrate that dynamic as well as non-Gaussian process characteristics require monitoring methods which take the temporal structure into account. As far as safety is concerned, explainability should be seen as part of alarm credibility: an advisory alert that

refers to plausible variables, trends, and failure mechanisms is more useful than one that has a high level of confidence yet no engineering basis.

Alarm analytics also offers a useful method of interaction. As DCS alarm systems usually result in operators being confronted with a series of repeated, continuous, important, or inappropriate alarms rather than simply activating an alarm when a threshold is reached, advanced alarm management aims to take into account the various operating states and the relationships between different sequences of alarms (Yang *et al*., 2022). Real-time analytics is able to group together related alarms, identify the most likely cause of the deviation, remove duplicate alarms from the advisory displays, and calculate various metrics concerning persistence or recurrence. However, the first alarm settings must still be traceable to the approved alarm philosophy. The analytics layer should be responsible for supplying context and setting priorities; it must not quietly delete or redefine alarms which have already been formally justified. This method assists to reduce the mental effort while at the same time preserving accountability for the configured protective actions.

Dynamic risk assessment does not limit itself to looking at the condition of the equipment; it also considers the performance of the barriers. Different from traditional quantitative risk assessment, which stays the same between formal reviews, the actual level of risk varies according to factors such as the availability of the equipment, the state of the process, the weather conditions, maintenance activities, the number of alarms, and degradation. Li *et al*., (2022) have described methods for updating operational risk as new process information becomes available. Furthermore, an analysis of incident data can reveal the dependencies that exist among the various elements of process-safety management and the recurring patterns of incidents; for instance, Sattari *et al*., (2021) applied machine learning and Bayesian analysis to prioritise the relationships in a large dataset of oil and gas incidents. The result in practice is that smart facilities are able to keep their safety situation continuously up to date, on the condition that the risk they show is used as a means of aiding decision-making instead than as a replacement for hazard analysis.

A good way of putting it is by means of the idea of barrier-health analytics. Rather than asking an algorithm to "predict an accident", a task which is statistically challenging and could result in misleading outcomes, the system can evaluate the observable precursors such as sensor drift, degradation of valve response, overdue proof tests, a higher frequency of SIS demands, longer bypass durations, alarm floods, abnormal control effort, or repeated operation near the safe limits. Since these signs are nearer to measurable evidence, they can be assigned to the specific parties responsible. Studies into autonomous fault diagnosis demonstrate how new faults and their root causes can be identified from process variables (Arunthavanathan *et al*., 2022), while process-safety reviews underline the importance of linking fault information to the management of abnormal situations and to risk assessment (Arunthavanathan *et al*., 2021a). Barrier-health dashboards can thus be incorporated into the existing process-safety workflows instead of setting up a separate digital safety programme.

Digital twins offer a more suitable environment for establishing this kind of connection since they are able to combine live data with engineering models and simulated scenarios. According to Keprate and Bagalkot (2022), a digital twin can be used to update the remaining service life and inspection data for safety-critical piping by making use of process parameters and likelihood-based modelling. Petrochemical research has also associated digital twins with instant interaction and with safety improvements that are meant for humans (Jia *et al*., 2024). In the oil and gas sector, Mazzuto *et al*., (2025) have developed a digital twin of an experimental transport system that makes use of actual plant data and predictive modelling to investigate anomalous behaviour and resilience. A systematic review by Belo *et al.,* (2025) points out the functionality, interoperability, synchronization, and other requirements that have to be specified if digital twins are to reliably support oil and gas production. The findings from these studies indicate that digital twins are only useful when their purpose, level of fidelity and uncertainty are clearly defined; a model that appears to look visually impressive but has no validated boundaries might lead to excessive confidence.

6. Integrated SIS-DCS-Analytics Reference Architecture

Figure 1 presents the review as a reliable reference architecture. At the field level, the instruments and the final control elements are connected to the DCS, and where necessary in accordance with the safety lifecycle, also linked to independent SIS channels. The DCS is responsible for continuous control, operator visualization, sequencing and alarms; the SIS carries out the safety instrumented functions. Both systems send selected read-oriented data to a protected integration layer which is made up of replicated historians, event logs, device diagnostics and time synchronization services. This layer functions as the evidence boundary since the data are copied, quality-tagged and given context before being passed on to the analytics. The analytics layer can include fault detection, soft sensing, alarm

sequence analysis, barrier-health calculations, dynamic risk models and digital-twin services. The results are provided to the operator, process-safety, reliability and maintenance interfaces together with clear information regarding provenance and confidence.

One of the main characteristics of the architecture is that it does not provide a set procedure by which the SIS carries out its actions on the analytics. If any future applications involve automated recommendations or closed-loop optimisation, these functions must be carried out in a separately validated control domain unless the applications have been specifically designed as part of the functional-safety lifecycle. Although the 2025 review of real-time process safety emphasises the increasing link between dynamic risk, fault diagnosis, safe control, and cyber-physical integration, it also notes that there are still unresolved issues relating to safe data-driven control and integrated demonstrations (Braniff *et al.*, 2025). The architecture therefore regards analytics as a way of improving human intelligence. This is in line with the ideas set out in Process Safety 4.0 that humans and artificial intelligence should work together rather than assume that autonomous AI can replace professional judgment within safety-critical operations (Arunthavanathan *et al.*, 2024).

Table 1 shows the architecture in the form of an evidence matrix, each layer supplying a varying degree of safety and carrying a corresponding level of assurance responsibility. The field instrumentation supplies physical evidence but is susceptible to drift and can be affected by environmental failures. The DCS data offer process context but may illustrate the effects of interactions inside control loops and defects in alarm design. The SIS data give direct evidence regarding protection demands, bypasses, and the outcomes of proof tests, even though they require more rigorous access and configuration controls. The analytics are able to combine patterns from all these different sources, but uncertainty caused by the models and distribution shift remains considerable. Hence, a defensible smart-safety programme looks at the entire evidence chain rather than focusing on the accuracy of a single model.

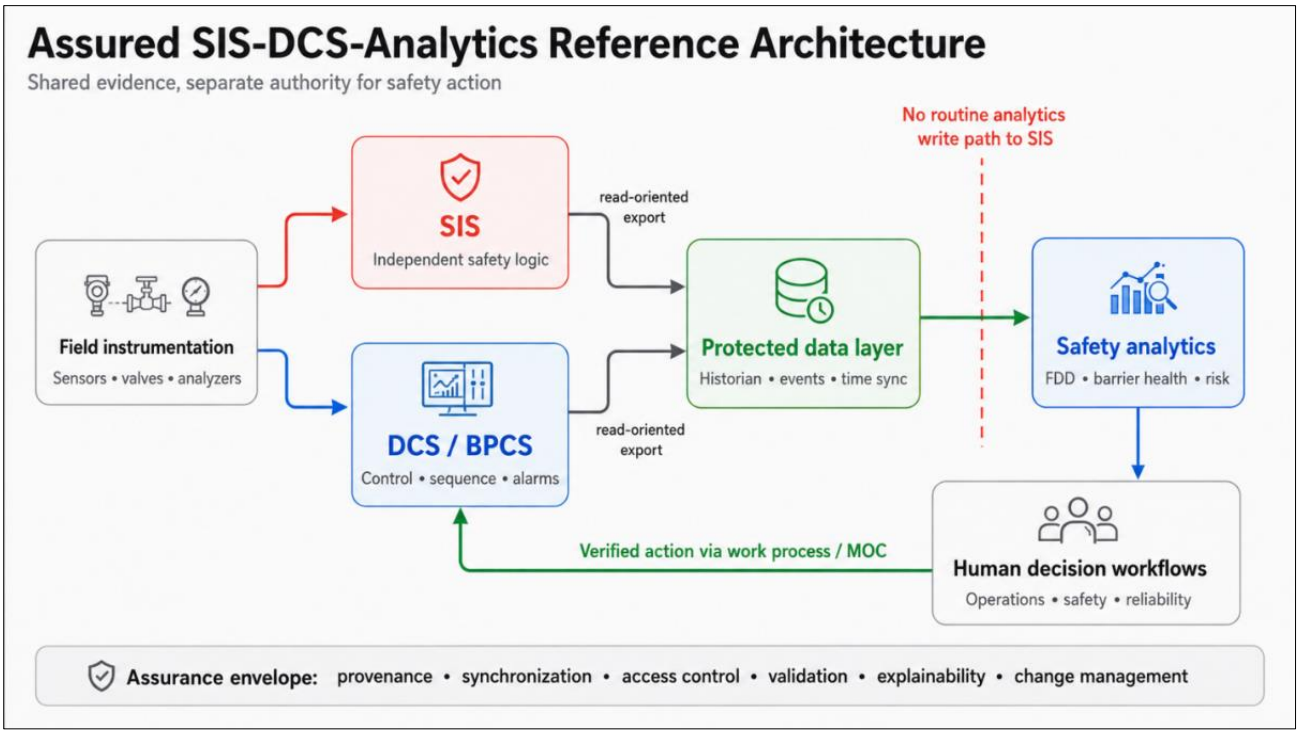

Figure 1: Assured SIS–DCS–analytics reference architecture.

Table 1: Evidence and assurance roles across the integrated process-safety architecture

Integration layer	Primary evidence	Process-safety contribution	Principal failure / misuse risk	Assurance requirement
Field instrumentation	PV/SV, diagnostics, valve position, analyzer status	Physical-state visibility and precursor detection	Drift, noise, frozen values, calibration or communication errors	Calibration traceability; quality flags; timestamp integrity; criticality mapping

Integration layer	Primary evidence	Process-safety contribution	Principal failure / misuse risk	Assurance requirement
DCS / BPCS	Trends, control effort, sequences, alarms, operator actions	Operating context, abnormal-situation recognition and alarm interpretation	Control interactions mistaken for faults; alarm overload; shared-resource failure	Approved alarm philosophy; state context; change control; historian validation
SIS	Trip inputs, demands, bypasses, diagnostics, proof-test and final-element status	Direct visibility of protection-layer demand and availability	Loss of independence; unauthorized change; common-cause cyber path	Restricted access; configuration control; read-oriented export; functional-safety lifecycle
Protected data layer	Historian replicas, event logs, time sync, asset metadata	Creates a governed evidence boundary for cross-system analytics	Stale data, tag mismatch, inconsistent clocks, unverified transformations	Data lineage; canonical tag model; synchronization; integrity monitoring
Analytics / digital twin	Derived features, fault scores, barrier-health and dynamic-risk estimates	Earlier diagnosis, prediction, prioritization and scenario support	Model drift, opaque inference, overconfidence, distribution shift	Independent validation; explainability; uncertainty; model versioning; no routine SIS write path
Human decision workflow	Evidence summary, confidence, recommended checks, work orders	Turns analytical insight into accountable operational action	Alarm fatigue, automation bias, unclear ownership or delayed escalation	Role-based interfaces; escalation rules; MOC; cross-functional review; audit trail

7. Cybersecurity, Governance, and Human Factors

Connectivity functions not only as a way of enabling integrated analytics but also as the most important new risk in this scenario. Experience in the process industry indicates that cyber incidents can gain access to operational technology and may in fact cause hazardous releases, fires, explosions, and disruptions to production (Iaiani *et al*., 2021). Studies conducted on offshore oil and gas show that the cybersecurity of the SIS is a major concern because the digitalisation of the assets results in remote access, software dependencies, and new ways in which corrupted information or commands might affect safety functions (Zhu & Liyanage, 2021). The appropriate approach is not to revert to complete information isolation, but instead to design an architecture in which each new connection has a specific purpose, a defined direction, an owner, an authentication method, a monitoring strategy, and a failure response plan.

Governance must not be confined to network security; instead, it is essential to put in place controls at all stages of the model's lifecycle with regard to the training data, versioning, validation, approval before deployment, records of changes, performance drift, and retirement. A predictive model may perform well at the start but can later deteriorate following a turnaround, after the sensors have been replaced, as a result of control tuning, or when the data feed changes. Safety governance therefore has to define the areas in which analytics can make recommendations, the situations in which an output must be checked by engineering, and the kinds of changes that result in the need for management of change. The model's confidence should never be the only factor considered; independent process evidence, engineering plausibility, and the consequences of an error all have to be taken into account. NIST OT guidance endorses the concept of balancing cybersecurity with availability and safety rather than applying information-technology controls without taking into account the physical operations (Stouffer *et al*., 2023).

It is the human factors that determine whether analytical insight results in safer action; if an operator has to cope with hundreds of tags, they will not get any benefit from an additional dashboard which simply shows scores and colours. The interface should clearly show what has changed, explain why this is important, indicate which barrier might be weakening, and state what verified action is needed. As the literature on alarm management demonstrates, there is a safety cost due to overload and because of announcements that are not properly contextualised (Yang *et al*., 2022). In the same way, research into explainable AI shows the value in identifying the contribution of individual variables rather than providing opaque classifications (Bhakte

et al., 2024). The goal is to create a brief decision narrative which includes the evidence, the interpretation, the uncertainty, the recommended check, and the escalation rule.

Disciplined ownership is just as important in all these fields—such as operations, instrumentation, process safety, reliability, cybersecurity, and data science—because no single department can be made responsible for the whole process. Although instrument engineers are familiar with calibration and failure modes, control engineers have an understanding of loops and alarm behaviour, process-safety experts are aware of credited barriers and hazard scenarios, information security experts know the access paths, data scientists have knowledge of model behaviour, and operators have a good understanding of the plant context. It has to be concluded therefore that cross-functional review extends well beyond being nothing more than a matter of administrative bureaucracy and is in fact a technical step meant for identifying the underlying assumptions. Smart safety can only be regarded as credible if all the disciplines work from the same configuration baseline and if the analytical recommendations can be traced to specific, accountable decisions.

8. Implementation Maturity Model

Table 2 outlines five stages for implementation. At level 0 you have isolated monitoring: even though the SIS, DCS, the historians and the maintenance records are available, they are usually only examined after an incident has taken place. At level 1 secure visibility is obtained through employing replicated data and synchronised event histories while at the same time retaining the system borders. At level 2 contextual analytics are applied regarding data quality, alarm performance and instrument-health indicators. At level 3 validated predictive systems, barrier-health indices and dynamic risk displays are introduced and are linked to both maintenance and process-safety workflows. At level 4 assured adaptive intelligence is involved, which means that the models are continuously watched for drift, that digital twins are used for scenario testing, that cybersecurity controls are combined with safety governance, and that human authorisation is explicitly required for any action which has safety significance.

Advancement must be based on evidence rather than on the availability of technology. A facility should not advance from Level 1 to predictive systems if the timestamps are unreliable, the tag identities are inconsistent, the proof-test records are incomplete, or ownership is not clear. In the same way, a high-performing model should not claim to be at Level 4 if the explanations are weak or if change control is missing. Because of this, the maturity model regards data governance and organizational readiness as necessary prerequisites, not as steps that come after. The literature on the Industry 4.0 process-data architecture draws attention to the need for layered sensing, data management, application, and networking functions (Wanasinghe *et al*., 2022), and research into digital-twin requirements stresses the importance of defined functionality and non-functional requirements in oil and gas applications (Belo *et al.,* 2025). By taking a staged approach, operators are able to obtain early benefits from improved visibility and contextualization while at the same time building up the assurance evidence required for more advanced applications.

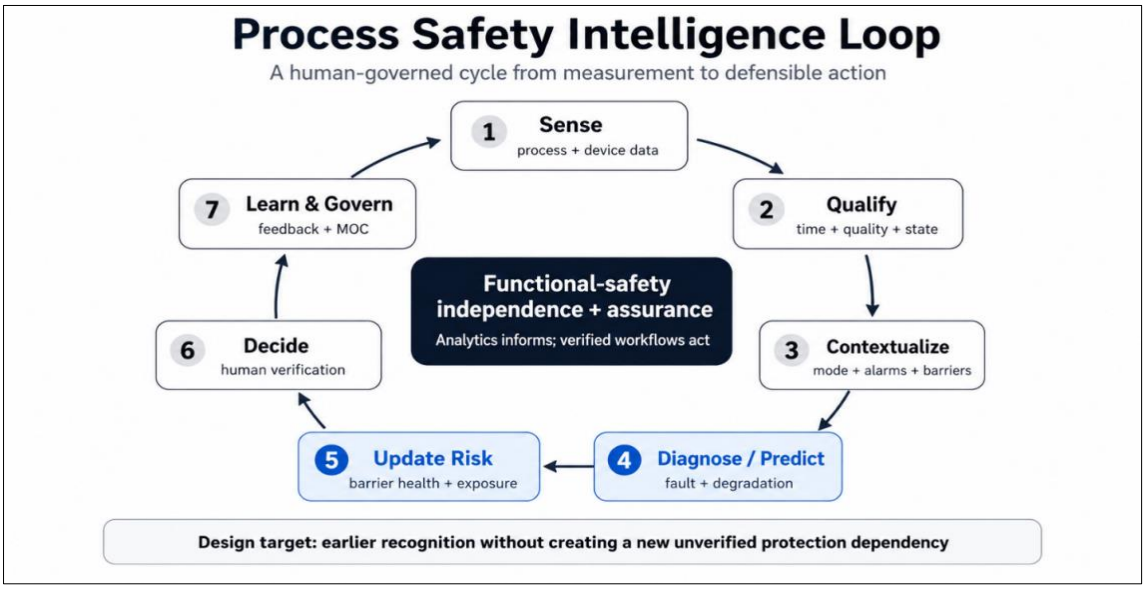

Figure 2: Human-governed process-safety intelligence loop

Table 2: Proposed implementation maturity model for SIS–DCS–analytics integration

Level	Architecture state	Analytical capability	Permitted safety use	Governance gate
0 — Siloed	SIS, DCS and maintenance data reviewed separately	Reactive trending and post-event analysis	Learning after deviations or failures	Basic configuration and record ownership
1 — Connected visibility	Protected historian/event replication and synchronized clocks	Cross-system timelines and dashboards	Situational awareness; no automated safety action	Network segmentation; identity/access control; data ownership
2 — Contextualized	Tag semantics, quality flags, operating modes and asset context	Data-quality, alarm and instrument-health analytics	Leading indicators and verified maintenance triggers	Validation rules; alarm governance; data-quality KPIs
3 — Predictive	Validated models linked to barriers and work management	Fault prognosis, barrier health, dynamic risk, selected digital twins	Advisory prioritization and scenario-informed intervention	Model lifecycle controls; explainability; MOC; performance monitoring
4 — Assured adaptive	Continuous model monitoring and cyber-safety co-assurance	Drift detection, resilient twins, role-specific decision intelligence	Human-authorized safety-significant action; controlled adaptation	Independent assurance; degraded-mode strategy; auditability; periodic revalidation

9. DISCUSSION AND RESEARCH GAPS

The section outlines the main points of the study and identifies the areas that need additional investigation. The results show that although there has been some progress in this field, certain questions still remain. The first of these is that the sample sizes in most of the studies are small, and this may prevent the findings from being widely applicable to bigger groups. A second issue is that the studies frequently employ different methods and measures, which makes it difficult to compare the results. Thirdly, there is a lack of long-term data, meaning that we do not know about the long-lasting effects. Fourthly, the majority of the research concentrates on a single group or region, so the results might not be applicable to other situations. Future studies should therefore use larger samples, standardise their methods, and gather data over longer periods, in order to establish a more firm foundation for future work in this area.

The literature strongly supports the possibility of detecting faults immediately and the application of digital process-safety analytics; however, the evidence concerning the complete integration of the SIS with the DCS and the analytics remains dispersed. A great deal of research focuses on the evaluation of algorithms using benchmark processes, pilot plants, historical records of incidents, or specific assets. Although these methods are helpful in developing the algorithms, they do not illustrate how the systems behave over long periods when exposed to changes in configuration, the replacement of sensors, different operating modes, network outages, and various human work practices as occur in large oil and gas facilities. The main research gap is therefore not one of greater accuracy; instead, it lies in the need for end-to-end assurance of the data-to-decision chain in real safety situations.

The first point to concentrate on is measurement provenance. Although smart analytics as a rule considers the values recorded by the historian to be accurate representations of physical reality, the instrument's calibration status, the sampling frequency, the signal conditioning, the quality of the communication, the condition of maintenance, and the context of the control loop can all have a significant impact on the interpretation. Subsequent research should develop data-quality metadata for use in safety analytics so that the models can reject or reduce the weight assigned to the evidence each time there is uncertainty regarding the measurement chain. In this way, instrumentation engineering can be more closely linked with data-centric safety and thus bridge the gap between sensor behaviour and model confidence.

The following stage involves carrying out validation every time there are changes in the way the system is operating. Even though deep fault-diagnosis techniques are still being developed, a distribution shift is inevitable. Any changes to the operating modes, to the characteristics of the feed, to the equipment configuration, and to the control strategies all affect the baseline against which 'normal' is determined. Methods that take into account the operating mode and also offer

explanations look promising (Bhakte *et al*., 2024; Zhao *et al.,* 2024), but the validation tasks should not simply concentrate on the detection rate and the number of false alarms; they must also take into account how long it takes to issue a warning, behaviour during transitions, tolerance to missing data, interpretability, and the consequences of giving incorrect advice. When it comes to applications related to barrier health, the cost of creating a false sense of security may be higher than the average level of classification correctness.

The third priority is safety-security co-assurance. In order to allow centralised analytics, it is necessary for petroleum systems to have data connectivity without at the same time compromising the independent credibility of their safety functions. Current research has documented both cyber incidents in the process industry and the specific difficulties linked to SIS connectivity (Iaiani *et al*., 2021; Onshus *et al.,* 2022). Future research needs to focus on architectures that incorporate unidirectional data flow, secure gateways, signed data, anomaly detection, and recoverable degraded modes. Safety cases must clearly describe what happens when the analytics are not available, have been compromised, have become stale or are in conflict. A safe design should make sure that it depends on the existing SIS and DCS functions rather than having those functions depend on the analytical service.

It is just as important to present the evidence in a way that focuses on people. Even if an analytical system is very effective, it will still not work at an organisational level if the people who use it do not trust it, misunderstand it, or are overwhelmed by the number of alerts they receive. As the scholarship linked to Process Safety 4.0 points out, intelligence augmentation and joint effort between people and AI while taking risk into account should take place, not for human expertise to be replaced (Arunthavanathan *et al*., 2024). The research carried out therefore needs to examine different interface designs, the amount of explanation given, the criteria for escalation, and the specific information needs depending on role. Although process-safety engineers may need trend data on barriers and the consequences of various scenarios, operators will require immediate causal context together with a verified procedural action. The same model output should not be presented in the same way to all users.

In the end, digital twins and dynamic risk models should include clear statements about the limits of their scope; they can be used for what-if scenarios and for resilience studies, and recent work in the oil and gas industry has shown credible progress in the assimilation of real data (Mazzuto *et al*., 2025). It is certain, however, that the twins will simplify the real physical behaviour. If they are being used for safety purposes, it is essential to state the degree of fidelity, the frequency of the updates, the uncertainty present, and the situations in which the model is not valid. Likewise, dynamic risk displays should not suggest that a single, continuously changing figure replaces HAZOP, LOPA, proof testing, operating discipline, or engineering judgment. The most promising area for research is integration: analytics should make the existing safety barriers more observable, more anticipatory, and more actionable, without changing the formal responsibilities linked to those barriers.

10. CONCLUSION

Process safety can be considerably enhanced through integrating the SIS, DCS, and real-time instrumentation analytics, on the condition that the system integration is based on evidence rather than on shared control authority. The review shows that data from the field and the control system can lead to the earlier identification of faults, provide alarms with better context, help in the monitoring of barrier health, permit dynamic risk assessment, support predictive maintenance, and assist with decision-making through means of the use of digital twins. The benefits mentioned are most clear when the measurements are traceable, time-aligned, quality-tagged and are interpreted in the context of the process state. The proposed architecture therefore keeps the SIS as independent, clearly defines the DCS's responsibilities, and places the advanced analytics in a separate advisory environment with controlled data exchange.

In the case of sophisticated oil and gas installations, it is essential not only to be able to make autonomous predictions as well as to have assured decision support. With regard to all the issues involved—cybersecurity, the management of the model over its whole lifecycle, explainability, the control of changes, and the maintenance of human authority—the development of the algorithms must proceed hand in hand with these aspects. The maturity model outlined here provides a realistic route along which one can go from secure visibility to assured adaptive intelligence. When assessing future implementations it is necessary to determine whether they make the dangers more apparent and allow decisions to be more defensible without bringing in new common-cause vulnerabilities. It is for this reason that the principle provides a reliable foundation for applying digital intelligence to high-hazard operations while at the same time retaining the functional-safety discipline on which those operations depend.

REFERENCES

- Hegde, J., & Rokseth, B. (2020). Applications of machine learning methods for engineering risk assessment – A review. Safety Science, 122, 104492. https://doi.org/10.1016/j.ssci.2019.09.015
- Arunthavanathan, R., Khan, F., Ahmed, S., Imtiaz, S., & Rusli, R. (2020). Fault detection and diagnosis in process system using artificial intelligence-based cognitive technique. Computers & Chemical Engineering, 134, 106697. https://doi.org/10.1016/j.compchemeng.2019.106697
- Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., et al. (2021). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. BMJ, 372, n71. https://doi.org/10.1136/bmj.n71
- Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., Koffel, J. B., & PRISMA-S Group. (2021). PRISMA-S: An extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews. Systematic Reviews, 10, 39. https://doi.org/10.1186/s13643-020-01542-z
- Sattari, F., Macciotta, R., Kurian, D., & Lefsrud, L. (2021). Application of Bayesian network and artificial intelligence to reduce accident/incident rates in oil & gas companies. Safety Science, 133, 104981. https://doi.org/10.1016/j.ssci.2020.104981
- Arunthavanathan, R., Khan, F., Ahmed, S., & Imtiaz, S. (2021a). An analysis of process fault diagnosis methods from safety perspectives. Computers & Chemical Engineering, 145, 107197. https://doi.org/10.1016/j.compchemeng.2020.107197
- Amin, M. T., Khan, F., Ahmed, S., & Imtiaz, S. (2021). A data-driven Bayesian network learning method for process fault diagnosis. Process Safety and Environmental Protection, 150, 110–122. https://doi.org/10.1016/j.psep.2021.04.004
- Arunthavanathan, R., Khan, F., Ahmed, S., & Imtiaz, S. (2021b). A deep learning model for process fault prognosis. Process Safety and Environmental Protection, 154, 467–479. https://doi.org/10.1016/j.psep.2021.08.022
- Wang, B., & Wang, Y. (2021). Big data in safety management: An overview. Safety Science, 143, 105414. https://doi.org/10.1016/j.ssci.2021.105414
- Iaiani, M., Tugnoli, A., Bonvicini, S., & Cozzani, V. (2021). Analysis of cybersecurity-related incidents in the process industry. Reliability Engineering & System Safety, 209, 107485. https://doi.org/10.1016/j.ress.2021.107485
- Zhu, P., & Liyanage, J. P. (2021). Cybersecurity of offshore oil and gas production assets under trending asset digitalization contexts: A specific review of issues and challenges in safety instrumented systems. European Journal for Security Research, 6, 125–149. https://doi.org/10.1007/s41125-021-00076-2
- Zhu, P., Liyanage, J. P., Kumar, R., & Panesar, S. S. (2021). Decision quality related to emergency shutdown system in the oil and gas industry: Influences from data and information. International Journal of Decision Sciences, Risk and Management, 10(1/2), 131–159. https://doi.org/10.1504/IJDSRM.2021.117568
- Pasman, H., Sun, H., Yang, M., & Khan, F. (2022). Opportunities and threats to process safety in digitalized process systems—An overview. Methods in Chemical Process Safety, 6, 1–23. https://doi.org/10.1016/bs.mcps.2022.05.007
- Amin, M. T., Arunthavanathan, R., Alauddin, M., & Khan, F. (2022). State-of-the-art in process safety and digital system. Methods in Chemical Process Safety, 6, 25–59. https://doi.org/10.1016/bs.mcps.2022.04.001
- Bai, Y., Xiang, S., Zhao, Z., Yang, B., & Zhao, J. (2022). Data-driven approaches: Use of digitized operational data in process safety. Methods in Chemical Process Safety, 6, 61–99. https://doi.org/10.1016/bs.mcps.2022.04.002
- Wanasinghe, T. R., Don, M. G., Arunthavanathan, R., & Gosine, R. G. (2022). Industry 4.0 based process data analytics platform. Methods in Chemical Process Safety, 6, 101–137. https://doi.org/10.1016/bs.mcps.2022.04.008
- Yang, F., Wang, J., Asaadi, M., Hu, W., Wang, Z., & Zhang, Y. (2022). Alarm management techniques to improve process safety. Methods in Chemical Process Safety, 6, 227–280. https://doi.org/10.1016/bs.mcps.2022.04.009
- Li, X., Zhang, L., Khan, F., & Chen, G. (2022). Dynamic operational risk assessment in process safety management. Methods in Chemical Process Safety, 6, 309–351. https://doi.org/10.1016/bs.mcps.2022.04.004
- Keprate, A., & Bagalkot, N. (2022). Use of digital twins for process safety management. Methods in Chemical Process Safety, 6, 561–589. https://doi.org/10.1016/bs.mcps.2022.05.001
- Onshus, T., Bodsberg, L., Hauge, S., Jaatun, M. G., Lundteigen, M. A., Myklebust, T., Ottermo, M. V., Petersen, S., & Wille, E. (2022). Security and independence of process safety and control systems in the petroleum industry. Journal of Cybersecurity and Privacy, 2(1), 20–41. https://doi.org/10.3390/jcp2010003
- Arunthavanathan, R., Khan, F., Ahmed, S., & Imtiaz, S. (2022). Autonomous fault diagnosis

and root cause analysis for the processing system using one-class SVM and NN permutation algorithm. Industrial & Engineering Chemistry Research, 61(3), 1408–1422. https://doi.org/10.1021/acs.iecr.1c02731

- Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). Guide to Operational Technology (OT) Security (NIST SP 800-82 Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
- Arunthavanathan, R., Sajid, Z., Amin, M. T., Tian, Y., Khan, F., & Pistikopoulos, E. N. (2024). Process safety 4.0: Artificial intelligence or intelligence augmentation for safer process operation? AIChE Journal, 70(7), e18475. https://doi.org/10.1002/aic.18475
- Zhao, S., Duan, Y., Roy, N., & Zhang, B. (2024). A deep learning methodology based on adaptive multiscale CNN and enhanced highway LSTM for industrial process fault diagnosis. Reliability Engineering & System Safety, 249, 110208. https://doi.org/10.1016/j.ress.2024.110208
- Bhakte, A., Kumawat, P. K., & Srinivasan, R. (2024). Explainable AI methodology for understanding fault detection results during multi-mode operations. Chemical Engineering Science, 299, 120493. https://doi.org/10.1016/j.ces.2024.120493
- Jia, J., Wang, X., Xu, Y., Song, Z., Zhang, Z., Wu, J., & Liu, Z. (2024). Digital twin technology and ergonomics for comprehensive improvement of safety in the petrochemical industry. Process Safety Progress, 43(3), 507–522. https://doi.org/10.1002/prs.12575
- Zhou, S., Zhou, X., & Liu, H. (2024). Process monitoring and fault diagnosis method combining bagging DPCA-ICA with moving window Kolmogorov–Smirnov test. The Canadian Journal of Chemical Engineering, 102(7), 2495–2510. https://doi.org/10.1002/cjce.25211
- Braniff, A., Akundi, S. S., Liu, Y., Dantas, B., Niknezhad, S. S., Khan, F., Pistikopoulos, E. N., & Tian, Y. (2025). Real-time process safety and systems decision-making toward safe and smart chemical manufacturing. Digital Chemical Engineering, 15, 100227. https://doi.org/10.1016/j.dche.2025.100227
- Mazzuto, G., Pietrangeli, I., Ortenzi, M., Ciarapica, F. E., & Bevilacqua, M. (2025). Leveraging Digital Twin for operational resilience in the oil and gas industry. Array, 27, 100443. https://doi.org/10.1016/j.array.2025.100443
- Belo, R. C., Pimenta, M. S., Salvador, T. T., Petry, R. H., & Abel, M. (2025). Fundamental requirements of Digital Twins for production system in Oil and Gas Industry: A systematic literature review. Information and Software Technology, 184, 107742. https://doi.org/10.1016/j.infsof.2025.107742.