

WHITE PAPER

The Knowledge Continuity Crisis in Industrial Operations

Why experienced staff are an irreplaceable asset, what happens when they leave, and what must be done before the knowledge walks out of the door for good.

AUTHORED BY

Dr Chris White

PRODUCT MANAGER



The Problem

RIGHT NOW, IN CONTROL ROOMS ACROSS EVERY INDUSTRIAL SECTOR:

- Experienced colleagues who built their understanding of a specific plant over 20 or 30 years are retiring at a rate that has no historical precedent.
- The knowledge they carry, the mental models, the contextual judgements, the alarm response instincts built over decades, is not written down anywhere.
- The people entering those roles to replace them face alarm systems of increasing complexity with a fraction of the contextual understanding needed to manage them safely under pressure.
- And in most organisations, no structured plan exists to capture the knowledge that is walking out the door before it is gone permanently.

“In the USA alone, 10,000 baby boomers retire every single day. 70% of critical operational knowledge is undocumented. This is not a future risk. It is happening now.”

The six statistics below represent the scale of what industrial organisations are walking towards. Not one of them is projected or speculative. Each is drawn from published research conducted in 2023, 2024, or 2025.



This paper sets out the scale of the problem, the specific mechanisms through which knowledge loss degrades operational safety and performance, the structural reasons why organisations have repeatedly failed to address it, and the practical approach that ProcessVue offers to capture, preserve, and make accessible the institutional knowledge that industry cannot afford to lose.

1 The Scale of the Problem

Industrial operations across every major sector are facing a workforce transition of a kind not seen before. The baby boomer generation, which has provided the backbone of skilled operational expertise in utilities, oil and gas, chemicals, manufacturing, maritime, and power generation for four decades, is now leaving the workforce at a pace that outstrips the capacity of organisations to replace it. While emerging AI capabilities offer promising tools for preserving and accessing institutional knowledge, this essential knowledge foundation must first be built: and that requires a fundamentally different approach to how operational expertise is captured, structured, and maintained before it walks out of the door.



The scale of the demographic shift is documented and unambiguous. According to research from the Alliance for Lifetime Income, more than 4.1 million Americans reached retirement age in 2024, with that figure sustained through to 2027. In the United States alone, 10,000 baby boomers retire every single day. In UK manufacturing and frontline industry, more than 57% of the most experienced workers are expected to retire within the next five years, according to a 2025 study conducted by Flip and Workplace Intelligence across 1,500 frontline managers and employees. Of UK managers surveyed, 81% report that most of their technical expertise is concentrated in older employees.

The manufacturing sector illustrates the trajectory with particular clarity. According to the Manufacturing Institute and Deloitte's 2024 Digital Skills Report, 3.8 million manufacturing jobs will need to be filled by 2033. Of these, 2.8 million are direct replacements for retiring workers, and projections suggest that 1.9 million of those positions may remain permanently unfilled because the skills and the candidates do not exist in sufficient numbers. Currently, 25% of the US manufacturing workforce is aged over 55, a proportion that has nearly doubled since the year 2000. McKinsey has noted that retirement rates spiked during the COVID-19 pandemic and have remained elevated since, accelerating a transition already well under way.

What makes today's situation structurally different from previous workforce transitions is the absence of any meaningful replenishment pipeline. Thirty years ago, when organisations made comparable mistakes with workforce planning, a deep graduate talent pool provided the absorptive capacity to recover. That buffer no longer exists. Industry attractiveness has declined significantly. Deloitte's Digital Skills Report notes that applicant interest in manufacturing and process roles is shrinking, not growing, despite governments and industry bodies launching initiative after initiative to address the skills gap.

Critically, this demographic pressure is not confined to the USA and UK. The United Nations World Population Prospects report documents massive and sustained shifts in population age profiles across Germany, Italy, South Korea, Japan, and China, all of which are seeing the working-age pool contract at pace as decades of declining birth rates feed through into the workforce. India, often considered as not affected, is starting to see the very early signs of significant demographic change. Because this is a genuinely global and simultaneous transition, simply encouraging skilled workers to relocate from one country to another is no longer a viable response, hindered further by growing political pressure to reduce immigration. Every major industrial economy is facing the same cliff at the same time. There is no neighbouring talent pool to draw from. The capture, retention, and accessible management of operational knowledge will not only be essential to business continuity: it will provide a decisive competitive advantage to any organisation that addresses it before the crisis becomes unrecoverable.



It is also important to recognise that retirement is not the only driver of knowledge loss. Employee churn, experienced people leaving for better opportunities, creates exactly the same problem with none of the predictability that a retirement timeline provides. The most capable practitioners in any organisation are precisely those with the most options in the labour market. They are the ones competitors actively target, and in an environment where capable professionals routinely change roles every three to four years, the assumption that institutional knowledge is safe until retirement age is a dangerous one.

Research consistently shows that loyalty to a single employer has declined significantly across all age groups and sectors. The knowledge continuity challenge is therefore not a project with a defined start date tied to a retirement schedule. It is a continuous operational risk that demands a continuous response.

The personal dimension deserves equal emphasis. The author of this paper faced this problem directly at a previous organisation. On joining, the team had a combined operational experience of about 250 years. A timeline analysis showed that within ten years, the majority of that experience would retire. A hiring and knowledge transfer plan was developed, presented to corporate HR, and approved at board level three years running. Three years running, it was cut at budget time. The knowledge continued to walk out of the door regardless. That pattern, approved and deferred, recognised and ignored, is not unique to any one organisation. It is the norm.

2 What Actually Leaves When Experience Retires

When an experienced person retires, the organisation loses far more than a body to fill a position. It loses a body of knowledge that, in most industrial environments, has never been fully written down and cannot be reconstructed after the fact.

Research published in the **Manual.to Tribal Knowledge Crisis Report (2026)** describes operational knowledge as existing in three distinct layers. The table below shows what those layers contain, and what happens when they are lost.

KNOWLEDGE TYPE	WHAT IS IT	LOSS RISK
10% EXPLICIT KNOWLEDGE	Written procedures, checklists, alarm configurations. What is already documented.	Easy to capture. Most organisations stop here.
30% EXPLICIT KNOWLEDGE	Optimised sequences, personal adjustments, shortcuts developed over years. The difference between the SOP and how an expert actually does it.	Requires observation and video capture. Rarely documented.
60% TACIT KNOWLEDGE	Sensory diagnosis, contextual judgement, predictive intuition. What takes 15-30 years to develop.	Lost permanently when the expert leaves without structured capture.

In alarm management specifically, the loss of tacit knowledge carries particular operational weight. Veteran control room operators carry what practitioners describe as mental models of their plant: an intuitive understanding of how process variables interact, which alarm combinations are genuinely critical and which reflect instrumentation noise, how long a particular plant section takes to stabilise after an intervention, and which upstream conditions reliably predict a downstream event. These mental models are not documented anywhere. They are built by living through the process, responding to its upsets, and accumulating pattern recognition over years.

When those operators retire, the alarm system they leave behind is unchanged. The DCS configuration, the priority assignments, the response procedures all still exist on screen. But the human capacity to interpret it in context, to distinguish genuinely dangerous from routine, and to respond with the confidence that comes from experience, is gone. What remains is an alarm system that newer operators may follow procedurally without fully understanding, and that under pressure can become a source of confusion rather than clarity.

The Boeing case study from 2017 crystallises the position. The company was forced to rehire hundreds of retired engineers simply to maintain production schedules, because the institutional knowledge required to keep those lines running could not be quickly reconstituted from documentation alone. In the nuclear sector, the United States discovered it could no longer manufacture a critical warhead component because the engineers who understood the process had all retired. Recovering that capability required five years and \$69 million. NASA encountered the same phenomenon after Apollo: the Saturn V blueprints existed, but the practical knowledge of how to build the rocket had dispersed with the team.

Repeating the same mistake

These are not cautionary tales from distant industries. These are leading technology organisations. Every process plant where experienced operators retire without structured knowledge transfer is repeating the same mistake at smaller scale, with consequences proportional to the complexity of what they were managing.

3 The Consequences When It Goes Wrong

The consequences of knowledge loss in alarm management are not abstract. They are measurable in operational performance degradation, financial loss, and in the most serious cases, in injuries and fatalities. The data below is drawn from incident investigations, regulatory research, and operational performance studies.

3.1 | The Human Performance Ceiling

ASM Consortium research establishes that a fully competent operator requires approximately 49 seconds per alarm to complete the full response cycle: noticing the alarm, accessing supporting data, diagnosing the situation, and executing a corrective action. Three principal international standards govern alarm management practice: ISA 18.2, EEMUA 191, and IEC 62682. Together these frameworks define how alarm systems should be designed, managed, and maintained, and collectively set the manageable alarm rate at no more than 10 alarms in a 10-minute period.

Under alarm flood conditions, even a competent operator begins to lose situational awareness. For inexperienced operators, the breakdown occurs much earlier and more severely. Under-trained operators facing alarm floods exhibit significant self-doubt: they seek second opinions, delay responses that should be instinctive, and lose track of causal alarms within the noise of consequential ones. In environments where the response window is measured in minutes, that hesitation has consequences.

3.2 | The Cost of Getting It Wrong

The financial and safety costs are documented in the historical record.

- A major petrochemical explosion, heavily attributed to an operator missing critical path alerts during an unmanaged alarm flood, resulted in \$80 million in damages and 26 injuries. (CCPS)
- The Texas City Refinery disaster: the US Chemical Safety Board identified an over-reliance on a poorly rationalised alarm system, where a critical high-level alarm failed to alert an overloaded operator, as a material contributor to an explosion that killed 15 people and injured 170.
- The Viking Sky incident (2019): alarm flooding complicated crew response during engine failures in treacherous waters. The Costa Concordia grounding (2012): navigation alarms failed to alert the crew to deviation from course in time for corrective action. Legal proceedings arising from that disaster resulted in millions of dollars of damages.
- Knowledge gaps cost organisations an average of \$47 million annually through increased error rates, extended training periods, and duplicated problem-solving. (Helpjuice, 2023)
- Replacing a single experienced specialist costs between 1.5 and 4 times annual salary, with senior operational roles at the top of that range. (Forbes, 2023; UK Employee Statistics, 2026)

3.3 | Alarm System Performance Degradation

The table below shows what happens to the international alarm standards' performance benchmarks when the experienced workforce that maintained them retires without structured knowledge transfer.

KPI (ISA 18.2 EEMUA 191 / IEC 62682)	BENCHMARK	IMPACT OF EXPERIENCED WORKFORCE LOSS
Steady-state alarm	1 per 10 min (target)	Alarm creep from undocumented changes causes chronic overload
Time in flood conditionrate	< 1% of operating time	Inexperienced operators fail to resolve bad actors; flood states lengthen
Nuisance / chattering alarms rate	Zero tolerated	Alarm fatigue sets in; operators begin ignoring the system entirely
Alarms per day per positionrate	150 (target), 300 (max)	New operators lack context to challenge or reduce alarm load
Top 10 alarms % of total	< 5%, with action plans	Bad actors persist without experienced engineers to diagnose root cause

Figure 3: ISA 18.2 / EEMUA 191 / IEC 62682 performance benchmarks versus the impact of experienced workforce loss.
Sources: Rockwell Automation (2014); ASM Consortium (2011); EEMUA 191.

Rockwell Automation's research identifies poor alarm handling as one of the leading causes of unplanned downtime globally. McKinsey's workforce productivity research demonstrates that in highly complex roles, the productivity differential between experienced and inexperienced staff can reach 800%. Society of Petroleum Engineers data shows that implementing data-driven alarm rationalisation alongside operator competency validation reduced time spent in alarm flood conditions by more than 50%.

4 Why Organisations Keep Failing to Address It



The demographic transition described in this paper is not new. Nortel addressed it in the 1990s by removing older workers, realised its mistake eighteen months later, and paid the same consultant to advise on knowledge recovery. Nat-West bank followed a comparable pattern in the early 2000s, becoming a business school case study in the process. These failures have been documented, analysed, and taught in MBA programmes for twenty years. Organisations continue to make the same mistake.

The reason is structural. Knowledge retention is an investment whose benefits accrue over a five to ten year horizon. The risks of knowledge loss manifest gradually and become acute only after the knowledge has already departed. Research conducted by the Investor Responsibility Research Center Institute found that only 10% of long-term incentive plans for named corporate officers have a performance period of greater than three years, and that more than 85% of S&P 1500 companies have no metrics aligned to future value creation in their executive compensation design. Economic performance explains only 12% of CEO pay variance.

“Too often, the wrong performance measures and wrong incentives are used over too short a performance period.”

Jon Lukomnik, Executive Director, IRRCi

The structural consequence is predictable. For an executive whose performance is measured over a three-year horizon, the rational decision is to defer investment in knowledge infrastructure. The costs land on their successor's watch. This is not a character failing. It is a governance design problem, one that the IRRCi research documents across 1,500 publicly listed companies. As Deming observed: every system is perfectly designed to get the results it gets.

The structural consequence is predictable. For an executive whose performance is measured over a three-year horizon, the rational decision is to defer investment in knowledge infrastructure. The costs land on their successor's watch. This is not a character failing. It is a governance design problem, one that the IRRCi research documents across 1,500 publicly listed companies. As Deming observed: every system is perfectly designed to get the results it gets.

The result is the pattern that operations managers and engineers will recognise immediately: the knowledge continuity plan that is approved in principle and cut at budget time, three years running. The concern that is raised at team level, escalated, acknowledged, and deprioritised. The experienced colleague who retires and whose replacement struggles for twelve months to reach a fraction of the operational confidence the predecessor had on day one.

That pattern has a measurable financial cost. The 2025 Flip research found that UK employees spend more than 12 hours per week, nearly four months annually, helping colleagues who lack critical skills, including correcting mistakes and troubleshooting problems that an experienced team member would resolve in minutes. 73% of managers report relying on a handful of experienced workers to keep operations running. When those workers retire, the bottleneck does not disappear. It becomes a crisis.

A recent conversation with a major data centre operator illustrates the churn dimension with particular clarity. The organisation had identified that its entire operational knowledge infrastructure effectively resided in a single specialist. That individual had threatened to resign eighteen months previously. The response was to increase their salary. When asked how sustainable that approach was, there was no comfortable answer.

“The pay rise response is the corporate equivalent of the budget deferral. It addresses the symptom, not the cause. It buys time but creates a more acute version of the same risk.”

The specialist still holds the knowledge exclusively. They are still a resignation, a better offer, or an unforeseen absence away from leaving. The organisation has spent money without reducing its exposure by a single percentage point. And it has signalled to that individual that their leverage is real and can be exercised again. Any organisation where critical operational knowledge sits with one or two individuals, rather than being captured in a structured and accessible system, faces the same vulnerability. The question is not whether that knowledge will eventually become unavailable. The question is whether the organisation will have captured it before that moment arrives.

The Cumulative Experience Loss Problem

The following table illustrates the cumulative impact on a real operational team in a high-technology software organisation, anonymised at the company’s request. The age profile at the time reflected patterns that are now common across industrial operations globally. The author reconstructed this data from direct personal experience as a member of that team.

PERIOD	EXPERIENCE LOST	EXPERIENCE GAINED	CUMULATIVE IMPACT
Year 1	25 yrs retire	+3 yrs retire	Net: -22 yrs
Year 2	40 yrs retire	+5 yrs retire	Net: -57 yrs
Year 3	55 yrs retire	+5 yrs retire	Net: -107 yrs
Year 5	90 yrs retire	+6 yrs retire	Net: -189 yrs
Year 7	120 yrs retire	+10 yrs retire	Net: -299 yrs
Year 10	150 yrs retire	+12 yrs retire	Net: -437 yrs

Figure 4: Cumulative operational experience loss in a real high-technology organisation. Each retiring team member carried decades of product, customer, and industry knowledge. Replacement hires started at zero relevant experience. The gap widened every year that action was deferred.

5 A Different Approach: Capture, Structure, and Access

The solution to a knowledge continuity problem is not primarily a technology problem. It is a discipline and process problem: identifying what knowledge needs to be captured, structuring it so that people who do not already possess it can access and apply it, and then creating the infrastructure that makes that possible before the knowledge has gone.

Technology, including AI, plays a genuine and important role. But AI cannot surface what has never been recorded. It cannot retrieve the alarm response rationale that existed only in a retiring operator’s head, or the contextual judgement that distinguished a manageable deviation from the precursor to a serious event. The sequence matters: capture and structure first, then intelligent access. A well-designed knowledge infrastructure is the foundation on which AI-assisted access becomes a genuine game changer rather than an interface to an empty knowledge repository.

ProcessVue’s approach to knowledge continuity in alarm management operates across four essential stages.

Stage 1 | Understand the Current Position

ProcessVue Analyser connects directly to PLC and SCADA systems, collecting alarm and event data and storing it in a time-sequenced database. It provides analysis across more than thirty report types, covering alarm frequency, flood events, bad actors, chattering and stale alarms, and performance against the international alarm standards (ISA 18.2, EEMUA 191, and IEC 62682). An organisation cannot plan a knowledge continuity programme without first understanding where its alarm management system actually is relative to where it should be. Analyser tells you where you are and what needs to be investigated.

Stage 2 | Manage the Migration

ProcessVue Guardian is a master alarm database with full alarm rationalisation project management capability. It maintains the definitive record of what each alarm is, why it exists, what its priority is, what the required response is, and what the consequence of a missed response would be. Through its OPC connector, Guardian extracts current alarm configurations from the live DCS and compares them against the rationalised baseline, identifying where configuration has drifted from the intended design. The rationalisation process Guardian supports is itself a knowledge capture exercise: experienced operators externalising and documenting the contextual judgements that make an alarm system meaningful.

Stage 3 | Capture the Knowledge

Guardian's alarm manual capability is the centrepiece of a knowledge continuity strategy. The international alarm standards all require a documented alarm manual: a record of rationale, response procedures, and operational context for every significant alarm. In practice, most alarm manuals, where they exist at all, are incomplete, out of date, and inaccessible at the point of need. Guardian transforms the alarm manual from a compliance document into a living operational knowledge repository that is instantly accessible. When an experienced operator explains why a particular alarm behaves differently at start-up than during steady state, and that explanation is captured in Guardian's alarm record, it survives their retirement. The knowledge is no longer locked in one person's head. It becomes a structured knowledge library with instant access.

Stage 4 | Make Knowledge Accessible

ProcessVue has developed a set of APIs connecting to both Analyser and Guardian, enabling analysis to be triggered and results retrieved without extracting large data volumes. These APIs are integrated with an MCP server, making the ProcessVue data infrastructure accessible to AI agents. The current implementation uses Claude as the AI layer. The practical consequence is that a new starter or less experienced operator can query the system in plain language: asking why a specific alarm exists, what the intended response procedure is, what historical data shows about its frequency and behaviour, and what context the rationalisation record provides. Instead of requiring weeks of shadowing with a veteran operator, a new starter can access the structured knowledge that the experienced workforce accumulated and that Guardian preserved. The AI Gateway does not replace the experienced operator. It makes the knowledge

What Is Now Close To Reality

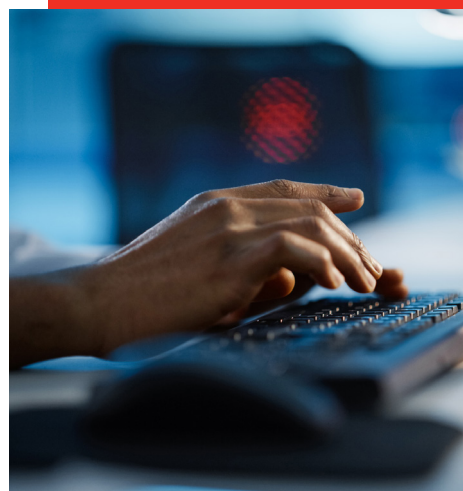
The architecture described above opens the door to something that is closer to reality than most people realise. Consider a technician standing next to a piece of equipment during a plant upset. They do not have time to leave the floor, locate a terminal, and search a manual. So they ask, out loud, over a headset. And the system answers, in plain language, drawing on every piece of knowledge that experienced operators contributed about that alarm. Speech-to-text and text-to-speech are mature, accessible technologies today. The ProcessVue AI Gateway already provides the governed connection to the knowledge repository. Connecting those capabilities is not a distant ambition. It is close to reality.

Add translation, and the implications multiply further. An experienced engineer whose first language is German, Japanese, or Portuguese contributes their knowledge in the language they think in. A new starter on a site in Korea, Brazil, or Poland queries the system in theirs. The knowledge base serves everyone. The effective resource pool for both knowledge contribution and knowledge access is no longer constrained by geography or language, which directly addresses the immigration and emigration barriers described in Section 1.

This concept may feel familiar. It should. The universal translator that captured imaginations in science fiction for decades is today a feature on a smartphone. The difference in an industrial context is that the technology is only as useful as the knowledge sitting behind it. That knowledge is what Guardian provides. And it must be captured now, while the people who hold it are still available to contribute it.

This concept may feel familiar. It should. The universal translator that captured imaginations in science fiction for decades is today a feature on a smartphone. The difference in an industrial context is that the technology is only as useful as the knowledge sitting behind it. That knowledge is what Guardian provides. And it must be captured now, while the people who hold it are still available to contribute it.

The combination of Guardian's structured knowledge repository and AI-assisted access transforms institutional knowledge from a personal asset that retires with its owner into an organisational asset that endures.



6 What Good Looks Like

Organisations that address knowledge continuity proactively, before the demographic transition reaches its most acute phase, achieve measurable outcomes across seven dimensions.

Reduced time to operational competency

Research consistently shows that the time for a new hire to reach full operational productivity in complex industrial roles is between six and twelve months, with some estimates extending to two years in highly specialised environments. A structured knowledge repository, accessible at the point of need, compresses that learning curve significantly. The new operator is not starting from scratch: they have access to the institutional knowledge that would previously have required months of mentoring with an experienced colleague to acquire. That operator carried available to whoever is standing at the console.

A structured foundation for training

The knowledge captured through Guardian's rationalisation process and alarm manual is not only an operational reference tool. It is a structured training resource. A new starter working systematically through the alarm manual for their specific plant section receives a plant-specific education: what every significant alarm means, why it exists at its configured setpoint, what the correct response sequence is, and what the consequence of a delayed or incorrect response would be. This is operationally grounded training that no generic induction course can replicate, because it is specific to the plant, the process, and the accumulated experience of the people who have operated it. Organisations that have historically relied on informal knowledge transfer through mentoring and shadowing now have a documented, auditable, and scalable alternative.



Maintained alarm system performance through workforce transition

Without a knowledge continuity strategy, alarm system performance typically degrades during workforce transitions. Alarm creep accelerates as changes are made by engineers who lack the operational context to assess their cumulative impact. Nuisance alarm rates rise, flood frequency increases, and the performance gap against the international alarm standards widens. A maintained rationalisation record in Guardian, regularly updated and used as an active reference, preserves the institutional understanding of why the system is configured as it is.

Regulatory compliance continuity

ISA 18.2, EEMUA 191, and IEC 62682 all require documented alarm rationale and response procedures. The regulatory requirement does not diminish because key personnel have retired: it intensifies, because the audit trail that demonstrates a managed and maintained alarm system is precisely what regulators and insurers examine when investigating incidents. Guardian's maintained record provides that audit trail and the demonstrable evidence of a responsible, systematic approach.

Dramatically Reduced System Learning Curve

There is a dimension to AI-assisted access that goes beyond operational knowledge retrieval, and it is one that organisations frequently overlook when evaluating new software systems. The traditional barrier to extracting value from a sophisticated platform like Analyser or Guardian is the training investment required to use it effectively. Reports need to be configured, query logic needs to be understood, interfaces need to be learned. In resource-constrained operational environments, that training burden frequently limits deployment to a handful of designated users, leaving the broader workforce unable to access the system's capability.

With the AI Gateway in place, that barrier collapses. An engineer, a shift supervisor, or a new starter can ask in plain language what they want to know and receive a meaningful, contextualised answer drawn from the full depth of the ProcessVue data infrastructure. No configuration, no report-building, no prior system knowledge required. The practical effect is that the value of Analyser and Guardian becomes accessible to anyone in the organisation who needs it, not just those who have been formally trained. This directly addresses one of the most common objections in any software procurement conversation: the concern that there is insufficient bandwidth to train people on a new system.

A workforce that stays

Operations environments where less experienced staff are given access to structured knowledge, where the learning curve is shortened by good tooling, and where new operators are not left to manage alarm systems they do not fully understand, are environments where people are more likely to stay. UK employee research for 2026 finds that 90% of workers describe themselves as disengaged or actively disengaged. New operators in knowledge-poor environments, facing alarm systems under pressure without adequate support, are disproportionately likely to leave. The investment in knowledge continuity is therefore also an investment in retention, which in turn reduces the frequency and cost of the replacement cycle.

Proven real-world impact

ProcessVue has recently supported a major data centre operator to complete a full rationalisation project covering over 1.5 million alarms. This work established standard alarm configurations based on data centre size and type. The result was that the time required to configure the alarm system for a new data centre reduced from over one month to three days. This standardised approach has since been deployed across 36 data centres worldwide, delivering millions of dollars of operational savings and, critically, creating a consistency of alarm configuration that means expertise developed in one centre can be rapidly applied to support operations in any other. That is knowledge continuity in practice: captured, structured, and made transferable at scale.

7 Conclusion

The knowledge continuity crisis in industrial operations is real, it is quantifiable, and it is already under way. The demographic data is unambiguous. The financial costs are documented. The safety consequences are on the historical record. And the structural governance problem that has caused organisations to repeatedly defer the investment required to address it is well understood, even if rarely named directly.

The window for acting is narrow and is ever decreasing. The knowledge that needs to be captured exists now, in the heads of experienced operators who are still at work. Once they leave, the opportunity to capture it in any structured form is substantially diminished. Every year of deferral is a year of knowledge lost permanently and a year of widening gap between what the alarm system requires of its operators and what those operators are equipped to provide.

ProcessVue's combination of Analyser, Guardian, and AI Gateway provides the practical framework for action. Analyser establishes the baseline. Guardian captures and maintains the knowledge. The AI Gateway makes it accessible to everyone who needs it, without the training burden that has historically limited the reach of operational software. Together, they transform institutional knowledge from a personal asset that retires with its owner into an organisational asset that endures.



The experienced operators who built your organisation's operational knowledge are retiring. The time to capture what they know is now, while they are still there to be asked.

8 Sources

The following sources were drawn upon in the preparation of this paper.

- Bullemer, P.T., Tolsma, M., Reising, D.V.C., Laberge, J.C. (2011). Towards Improving Operator Alarm Flood Responses: Alternative Alarm Presentation Techniques. ASM Consortium / ISA Automation Week.
- Dearden, H.T., Brazier, A. (2023). Jump to it! A New Model for Safety Alarm Operator Response Time Requirements. Hazards 33 Symposium Series No.170. IChemE.
- Rockwell Automation (2014). Getting Started: Performance Benchmarking and Alarm Philosophy Development. Process White Paper Series.
- EEMUA Publication 191 (3rd Ed.). Alarm Systems: A Guide to Design, Management and Procurement. Engineering Equipment and Materials Users Association.
- ISA-18.2-2016. Management of Alarm Systems for the Process Industries. International Society of Automation.
- IEC 62682:2022. Management of Alarm Systems for the Process Industries. International Electrotechnical Commission.
- American Bureau of Shipping (2025). Alarm Management Fundamentals and Industry Challenges. ABS.
- ABB / Water Online (2024). Prioritizing Alarm Responses for Better Workforce Management. Water Online.
- Flip / Workplace Intelligence (2025). Frontline Skills Crisis Research. Survey of 1,500 frontline managers and employees across US, UK, and Germany.
- Manufacturing Institute / Deloitte (2024). Digital Skills Report: 3.8 Million Manufacturing Jobs by 2033.
- Manual.to (2026). The Tribal Knowledge Crisis in Manufacturing.
- FP360 (2025). The Industrial Brain Drain: How Retirements Are Leaving Knowledge Gaps in Manufacturing.
- TSET / McKinsey (2025). How Retirements Undermine Manufacturing Productivity and What to Do About It.
- Wallace, L. / Forbes EQ (2023). Five Hidden Costs of Employee Attrition. Forbes.
- Dennison, K. / Forbes via IR Global (2023). The Silver Tsunami Is On The Way: How Companies Can Prepare.
- IRRCi / Organizational Capital Partners (2014). The Alignment Gap Between Creating Value, Performance Measurement, and Long-Term Incentive Design.
- Alliance for Lifetime Income Retirement Income Institute (2024). Peak 65 Zone Analysis.
- King's College London (2024). Analysis: Peak 65 Boom.
- United Nations Department of Economic and Social Affairs (2024). World Population Prospects 2024.
- MOL Learn (2026). Key UK Employee Statistics 2026.
- Bloomfire (2025). How Knowledge Mismanagement is Costing Your Company Millions.
- US Chemical Safety Board. Investigation Report: Texas City Refinery Explosion (2005).

© ProcessVue 2026. This paper may be shared freely for non-commercial purposes with attribution.

About ProcessVue

ProcessVue is a specialist alarm management and operational analytics platform designed for asset-intensive industries. Its capabilities are built around the EEMUA 191 and ISA 18.2 alarm management standards and are deployed across water, utilities, and process industries. ProcessVue helps control room teams move from reactive alarm handling to proactive operational awareness.

About The Author

Dr Chris White is a Product Manager at Processvue. He has worked in high tech and software product management position for over 25 years. Prior to his current role he held roles at NEC, GEC Marconi, Bookham Technology and Sopra Banking Software.



Contact ProcessVue to discuss your
Alarm Management requirements

Get In Touch

■ sales@processvue.com

processvue.com