Salem Automation
Systems Integration Specialists

The Hidden Cost of 'Good Enough':

A C-Suite Guide to Legacy System Risk and the Path to Modernization

Custom Solutions for Industrial Automation

3909 Westpoint Blvd. · Suite C · Winston-Salem, NC 27103 · Tel: +1 336-661-0890 · www.salemautomation.com

Overview

Across manufacturing and industrial sectors, legacy control systems and software platforms continue to run quietly in the background — not because they are optimal, but because replacing them feels too risky, too expensive, or too disruptive. This posture carries a hidden and growing cost.

This paper makes the business case for proactive legacy system management. It outlines the financial and operational risks of inaction, describes a structured four-stage path from stabilization to full modernization, and explains how Salem Automation, which is now part of IT Service Alliance (ITSA), helps industrial organizations lower risks of this journey at every step.

Key Takeaway	*Legacy systems do not fail on a convenient timeline. The question for executive leadership is not whether to act, but whether to act on your terms — or in response to a crisis.*

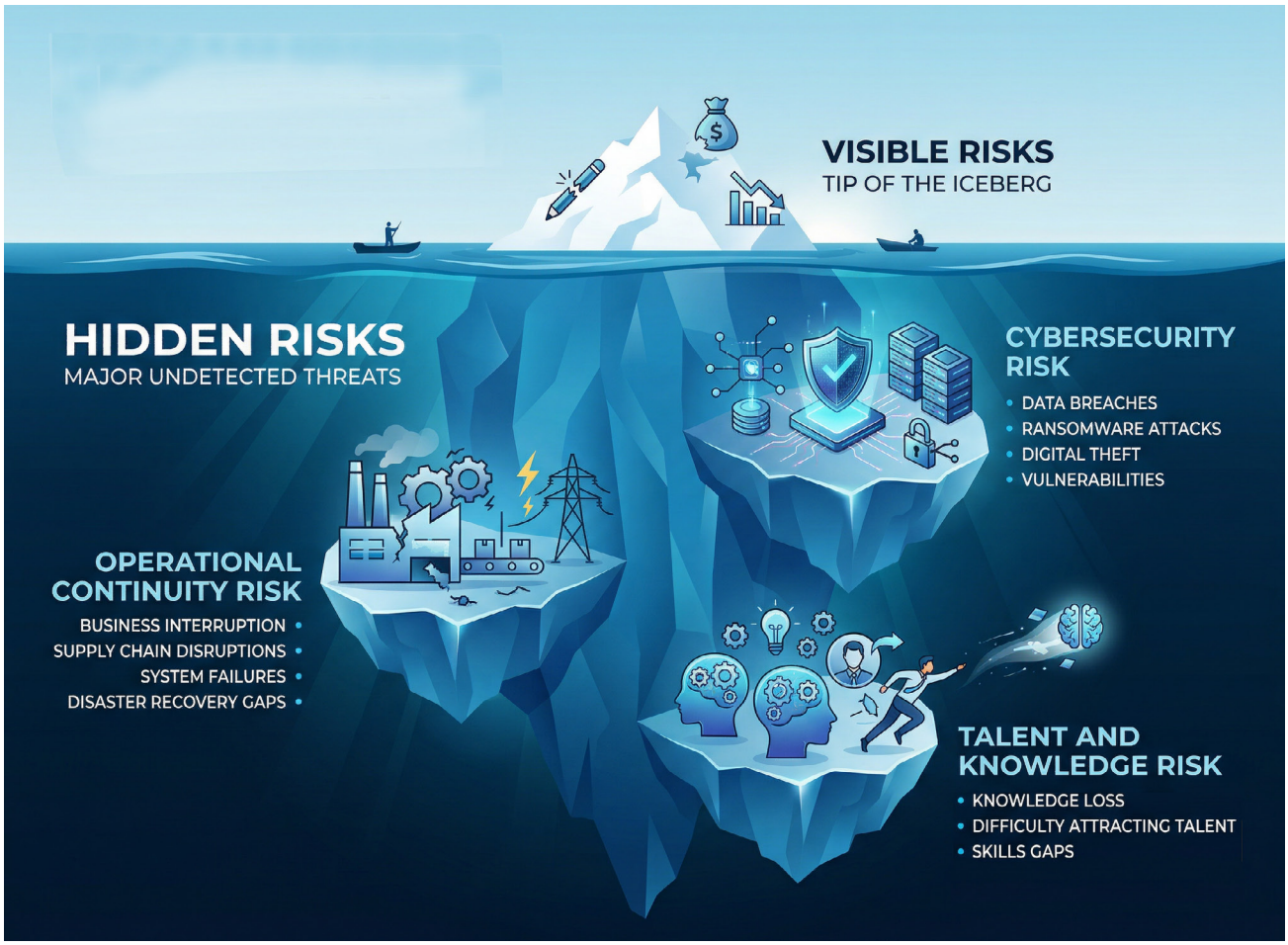
The Business Risk Hiding in Plain Sight

Legacy core processing systems,running on decade-old hardware are not relics. These architectures are active, load-bearing components of many industrial operations. And they are aging faster than most organizations realize.

What Executives Are Missing

Legacy system risk rarely surfaces in reports to the board, until something breaks. The day-to-day exposure accumulates quietly across three dimensions:

- Operational continuity risk: Aging hardware has no vendor support path. A single failed component can halt production with no commercially available replacement. The installed base of industrial control systems across North American manufacturing and utilities averages 15 to 25 years in age (Global Market Insights, January 2026).
- Cybersecurity risk: Legacy operating systems are no longer patched, representing exploitable gaps across OT/IT environments. Ransomware attacks against industrial organizations increased 87% year-over-year in 2024, with manufacturing accounting for more than two-thirds of all ransomware victims in 2025 (Dragos, February 2026). The average OT-related breach now costs $4.56 million per incident (Rosenblatt Securities, February 2026).
- Talent and knowledge risk: The engineers who built and maintain these systems are approaching retirement. Deloitte and the Manufacturing Institute project that 1.9 million manufacturing jobs could go unfilled by 2033, and 70% of manufacturers already report difficulty finding qualified automation engineers and technicians (Global Market Insights, January 2026).



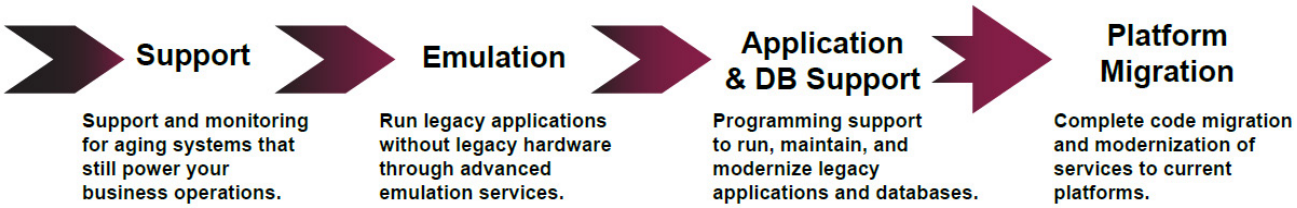
Industry Context

The installed base of industrial control systems in North American manufacturing averages 15–25 years in age. Many run on unsupported operating systems including Windows XP, embedded Windows, and Windows CE — platforms that can no longer be patched against modern exploits. Source: Global Market Insights, January 2026.

The financial consequences are well documented. Unplanned downtime across industrial segments averages $92,000 per hour, with a typical outage lasting 40 hours and costing $3.6 million per incident (Rockwell Automation, February 2026). Compounding this, 60–80% of IT budgets in legacy environments are consumed simply maintaining outdated systems — leaving little capital for proactive investment (Emkay Research, February 2026). A phased modernization program is nearly always less expensive than the reactive alternative.

A Four-Stage Path from Stability to Modernization

Salem Automation and ITSA take a pragmatic, phased approach to legacy system management. Rather than forcing a disruptive, cost-prohibitive strategy, we meet organizations wherever they are in their journey and build a logical path forward.



Support *Keep systems running*	**Emulation** *Eliminate hardware risk*	**App & DB Support** *Extend application life*	**Migration** *Modernize on your terms*
Expert monitoring and support for VAX, Alpha, OpenVMS, Oracle Solaris, and other legacy platforms —without replacing them	Run legacy applications on modern infrastructure using vtVAX, vtAlpha, and vtSparc virtualization—no rewrite required.	Programming support for C/C++, Pascal, Fortran, Java, and VB6 applications. Database continuity for RDB and Oracle Database environments.	Full code migration to current platforms: VB6 to .NET, SQL database migration, PLC upgrades, and modern SCADA deployment.

Each stage is a decision point, not a mandate. Some organizations stabilize at Stage 1 or Stage 2 while planning a longer-term migration. Others move through all four stages over a defined program timeline. The architecture is designed to flex with your operational realities and capital planning cycles.

Risk Comparison: Inaction vs. A Managed Strategy

The following table summarizes how key executive-level risk categories compare between an unmanaged legacy environment and one supported through a structured program.

Risk Factor	Without a Strategy	With Salem and ITSA
Hardware Failure	Unplanned downtime, costly emergency sourcing	Monitored proactively; emulation removes dependency
Cybersecurity Exposure	Legacy OS gaps unpatched, audit failures	Isolated environments, ISO 27001 / SOC controls
Talent Attrition	Institutional knowledge lost permanently	Documented, supported by our engineering team
Compliance	Increasing audit risk as systems age	Structured migration path with traceable records
Cost Trajectory	Escalating emergency spend	Predictable, phased investment model

CFO Perspective

Phased modernization converts unpredictable emergency capital expenditures into structured, manageable investments. The market is already moving: brownfield modernization in existing facilities rose from 14% to 32% in early 2026 (JPMorgan Research, February 2026). Organizations that act proactively will modernize on their own terms — those that wait will do so in response to a crisis.

Why Salem Automation and IT Service Alliance

Salem Automation was built around one core capability: deep expertise in the legacy platforms that industrial organizations still depend on. Our firm brings together deep legacy platform expertise and modern industrial automation capability. We are purpose-built for the OT/IT infrastructure challenges that generalist firms aren't equipped to solve.

Our acquisition by IT Service Alliance expands that capability across the full automation and technology stack, from PLC programming and SCADA deployment to enterprise IT integration. The combined organization provides continuity across the entire OT/IT boundary.

Our Differentiators

- Platform depth: Hands-on expertise in VAX, Alpha, Integrity, OpenVMS, Oracle Solaris, and OSES—not just familiarity, but engineering-level support capability.
- Emulation without rewriting: vtVAX, vtAlpha, and vtSparc allow organizations to eliminate hardware dependencies while preserving existing application logic, reducing migration risk and cost.
- Modern automation delivery: Certified integrators for Rockwell ControlLogix, Siemens S7, Emerson, Ignition, and Movicon SCADA — so modernization leads to a supportable, future-ready platform.
- Compliance and security posture: ISO 27001 certified and AICPA SOC compliant, providing the governance framework that regulated industries and enterprise IT departments require.
- Rockwell Encompass Product Partner: Formal recognition within the Rockwell Automation ecosystem, supporting customers through a structured, validated integration pathway.

CIO/CISO Note

Our ISO 27001 certification means we operate under a documented information security management system. For organizations navigating OT/IT convergence, this provides a structured, auditable governance foundation — not just technical capability.

What to Do Now: Three Questions for Executive Leadership

Before initiating a formal program, we recommend that executive teams address three foundational questions about their legacy environment:

- **Do you have a current inventory?** Legacy systems are often undocumented. Without knowing what you have, you cannot assess exposure or prioritize action.
- **What is your failure tolerance?** If a critical legacy system failed tomorrow, what would the production and financial impact be? This single number often reframes the entire modernization conversation.
- **What is your planning horizon?** Modernization does not need to happen in a single project. With the right phasing, it can align to your capital planning cycle and operational schedule.

Salem Automation and ITSA offer a complimentary discovery engagement to help answer these questions and build a prioritized risk profile for your environment. Our structured, diagnostic process gives your team the information needed to make an informed decision.

Conclusion

Legacy systems have served industrial organizations well. But the window for proactive, cost-controlled modernization is narrowing. Hardware availability, cybersecurity exposure, and workforce transitions are all compressing the timeline for decision-making.

The organizations that act now — through a structured, phased approach — will modernize on their own terms, with manageable risk and predictable investment. Those that wait will eventually modernize in response to a crisis, at significantly greater cost.

Salem Automation and ITSA exist to make the first path available to every industrial organization, regardless of where they are starting from.

Contact Us: salemautomation.com | itserviceaalliance.com