efi global®

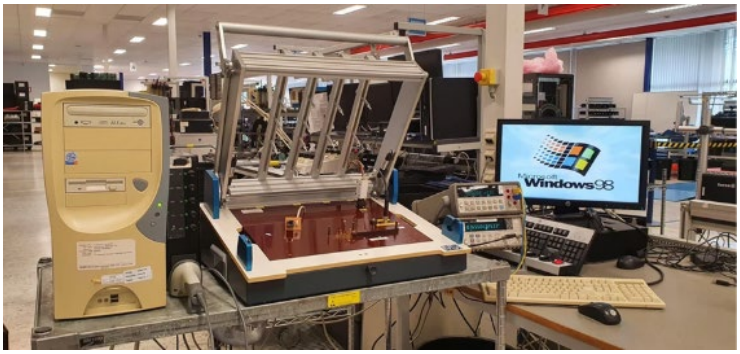
Why Plants Keep Old Computers Running

DOS, Windows 95, 98, and XP in Industrial Operations

Mitchell Duran[1], Amir Rubin[2]
[1]Service Line Principal, EFI Global, Columbus, OH 43026, Amir.Rubin@efiglobal.com
[2]Forensic Mechanical Engineer, EFI Global, Colton, CA 92324, Mitchell.Duran@efiglobal.com

Executive summary

In industrial environments, an old computer is rarely just an old computer. More often, it is the visible front end of a larger operational technology stack that includes a human-machine interface, controller communications, vendor-specific drivers, legacy interface cards, recipes, machine-vision libraries, historian links, alarm logic, and operator workflows. Replacing that computer can therefore trigger cascading changes that reach far beyond the desktop itself.



A legacy industrial workstation running Windows 98 alongside automated test equipment, illustrating how decades-old computers can remain embedded in modern production and laboratory environments. Credit: r/Taira Mai

This persistence is not simply a failure to modernize. Current National Institute of Standards and Technology (NIST) guidance states that operational technology (OT), the hardware and software that monitor or control physical equipment and industrial processes, has "unique performance, reliability, and safety requirements" [1, Abstract]. From an engineering perspective, retaining a stable legacy system is often a rational response to these unique requirements. NIST also states that availability is "generally the greatest concern for an OT" [1, Sec. 4.3.2 (Categorize)]. In NIST's OT-versus-Information Technology (IT) comparison, NIST explains that OT outages are often planned days or weeks in advance, that even momentary downtime may be unacceptable, and that software changes require careful handling because OT environments can involve proprietary operating systems, specialized control algorithms, and potentially modified hardware or software [1, Sec. 2.4, Table 1]. Research on digital retrofitting reaches a similar practical conclusion from a different direction: manufacturers frequently keep legacy systems in service because replacement is capital-intensive, compatibility is difficult, skills are scarce, and heterogeneous machines from multiple vendors are hard to unify without substantial engineering effort [4][5][6].

This white paper is intended as background and training material. It is a targeted synthesis of government guidance, selected peer-reviewed retrofitting literature, and industry references relevant to property-loss

scoping, not a systematic review and not a case-specific causation analysis. Its central point is simple: the age of the computer is often less important than the dependency chain wrapped around it.

Field proposition
For claims and engineering purposes, the correct question is not, "How old is the PC?" The correct question is, "What process, software, interfaces, validation burden, and period of interruption depend on that PC remaining functionally equivalent?"

The wrong mental model

Treating a plant-floor computer like an office desktop leads to poor conclusions. Office computers are usually replaced to restore user productivity. Industrial computers are often replaced, or deliberately not replaced, to preserve machine behavior. The distinction matters.

Operational technology interacts with the physical world. In NIST's OT-versus-IT comparison, "Human safety is paramount" [1, Sec. 2.4, Table 1]. The same comparison notes that even momentary downtime may be unacceptable, that outages are planned and scheduled days or weeks in advance, and that software changes must be handled carefully because OT systems can involve proprietary operating systems, specialized control algorithms, and potentially modified hardware or software [1, Sec. 2.4, Table 1].

For this reason, a 1990s or early-2000s computer can remain in service long after its consumer-era value has vanished. The machine around it may still be mechanically productive, the process may still be stable, and the plant may see more risk in changing the control environment than in preserving it.

Why one computer becomes a system issue

Legacy industrial computers persist because they are embedded in tightly coupled stacks. Digital retrofitting literature repeatedly describes factories as mixtures of machines, sensors, Programmable Logic Controllers (PLCs), and devices of different ages, different interfaces, and different manufacturers, all of which are complicated further by proprietary software and data structures [4][5]. In practice, that means a single replacement can implicate many dependencies at once:

- Human Machine Interface (HMI) or supervisory control software versions that only run on a specific operating system, runtime, or vendor library.
- PLC communication drivers, industrial data-exchange software, serial protocols, and proprietary interfaces that may not survive an operating-system change intact [4][5].
- Specialized interface hardware or fieldbus components that tie the workstation to the machine or line [4][5].
- Recipe databases, historians, label systems, vision applications, or peer workstations configured around a frozen software environment [4][5].
- Alarm handling, tested machine states, and commissioning baselines that may need to be re-established if the platform changes [5][6].
- Operator workflows and training assumptions that were built around the existing interface and software behavior [5][6].

The literature on integrated digital retrofitting is useful here because it explains the problem from the plant's point of view. Legacy machinery often is not "data ready," firms may lack capital to replace equipment wholesale, and proprietary interfaces make unifying information across the plant difficult [4]. More recent work adds that compatibility across hardware and software, limited technical competencies, and resistance to change can materially slow or complicate modernization [5][6].

Modernization is often nonlinear

A common claims assumption is that the old computer can be replaced with a new computer of greater capability and that the plant will therefore be "better off." In reality, modernization is frequently nonlinear. A modern operating system may not support the required driver set or interface hardware. A newer HMI version may require newer PLC firmware or a revalidated communications path. A firmware or software change may then require additional testing, backups, recipe review, and commissioning before the process can return to service [4][5][6].

This is one reason retrofitting is so common. The literature consistently frames retrofitting as a staged way to extend the life of productive assets while adding selective connectivity, sensing, or monitoring, instead of forcing an all-at-once replacement [4][6][7]. The MEP National Network guidance for manufacturers states this bluntly: firms can use current equipment, add after-market smart sensors, and start small rather than immediately purchasing entirely new systems [7]. That approach is not technological conservatism for its own sake. It is risk management.

Validation and regulated environments

In medical-device production and quality-management-system environments, the burden can be even heavier. Where production or quality-management software is subject to formal assurance or validation expectations, a platform change may require documented objective evidence that the automation still performs as intended [10]. FDA's February 3, 2026 guidance on Computer Software Assurance (which supersedes a September 2025 final guidance and builds on a risk-based framework in development since 2022) describes computer software assurance as a risk-based approach to establish confidence in automation used as part of medical device production or the quality management system, and it outlines methods and testing activities that may be used to generate that objective evidence [10].

This FDA guidance does not govern every industrial sector. But where formal validation, requalification, or documented change-control requirements exist, the same practical result often follows: plants may prefer containment, isolation, spare imaging, virtualization, or limited-scope retrofits over a fast platform migration. The older computer may be undesirable, but the change effort may be more disruptive than the legacy state it preserves.

Capital, skills, and downtime economics

The economics are rarely limited to hardware price. Digital retrofitting research identifies several recurring barriers to wholesale replacement: substantial investment cost, long amortization periods, difficulty quantifying return on investment, compatibility challenges, limited employee skill sets, and cultural resistance to change [5][6]. Those are not theoretical obstacles. They appear in real modernization programs as cost overruns, long schedules, and prolonged technical debt.

Federal legacy-IT reporting shows the broader persistence of these challenges, even outside plant-floor OT. The U.S. Government Accountability Office's (GAO) July 2025 review of federal legacy systems found selected systems using outdated languages, operating with unsupported hardware or software, and carrying known cybersecurity vulnerabilities; of the eleven systems most in need of modernization, it found that two had no modernization plan, six had incomplete plans, and only three had complete plans [8]. The report is enterprise-IT evidence, not plant-floor OT evidence. It is cited here only for the narrower proposition that complex legacy environments can remain in service for years because modernization has real schedule, staffing, and interoperability costs.

For an insured plant, that reality directly affects the period of restoration. When a legacy controls computer is destroyed, the "computer replacement" line item may be the least significant part of the loss. The dominant exposure may instead be engineering labor, software recreation, OEM participation, control validation, and the lost production time associated with commissioning a new environment.

Cybersecurity is real, but replacement is not the only response

None of this makes legacy operating systems safe. Microsoft's lifecycle documentation lists Windows XP extended support ending on April 8, 2014 [9]. Unsupported platforms increase cyber risk, create patching limitations, and make vendor support harder to obtain; in fact, NIST explicitly identifies the use of legacy or outdated operating systems as a system vulnerability in SP 800-82r3 Appendix C (Table 15) [1].

But OT security guidance does not reduce the problem to 'replace everything old immediately.' NIST and foundational DHS guidance instead emphasize defense-in-depth, network segmentation, boundary protection, controlled remote access, inventory, monitoring, and compensating controls that respect OT performance and availability constraints [1][3]. NIST's 2020 manufacturing behavioral anomaly detection project is instructive as well: the report documented behavioral anomaly detection (BAD) approaches for manufacturing industrial control systems (ICS), and Appendix B included installation and configuration steps for Windows XP, Windows 7, and Windows Server 2012 endpoints [2].

In practical terms, plants often respond to legacy cyber risk by isolating vulnerable assets, restricting routable access, enforcing change control, preserving golden images, monitoring network behavior, using one-way data flows where appropriate, and limiting the legacy system's functional exposure. Those are not perfect answers, but they are rational operational answers when full replacement would create greater immediate risk to safety, availability, or business continuity [1][3].

Balanced engineering view
A legacy OT computer can be both a cyber weakness and a rational business decision. Good field analysis acknowledges both truths at once.

When replacement is the correct answer

A mature analysis should also identify the limits of legacy retention. Replacement or broader migration is often justified when the dependency chain can no longer be maintained safely or economically, for example when:

- The required application, image, or license cannot be recovered or transferred.
- Critical interface cards, drivers, or fieldbus components are unavailable.

- OEM support is unavailable and no technically sound migration path exists.
- The legacy platform cannot be adequately isolated from unacceptable cyber risk.
- Requalification requirements make piecemeal fixes more expensive than structured migration.
- Physical damage has already forced changes elsewhere in the control stack, making functional equivalence impossible to preserve.

In other words, age alone does not compel replacement, but age plus broken dependency chain often does.

Field application protocol (non-case-specific)

For claim-specific work, the safest use of this paper is not as a substitute for case-specific engineering judgment but as a disciplined background framework. The sequence below helps professionals apply the legacy-computer issue without reducing it to a commodity-IT replacement question.

Step		What to do	Typical evidence
1.	**Preserve the as-found environment**	Determine whether the existing system can be documented or imaged before any migration or teardown decision is made.	Disk image or backup, BIOS or CMOS photos, software version list, activation records, dongle inventory
2.	**Build the dependency map**	Identify the computer's links to PLCs, HMIs, fieldbus cards, printers, scanners, labelers, historians, recipe servers, and peer workstations.	Network topology, controller list, data-flow map, internal photos, communications settings
3.	**Test plausible recovery options**	Compare like-kind replacement, virtualization, selective retrofit, and staged modernization before assuming a full controls redesign.	OEM compatibility matrix, driver or fieldbus support notice, integrator proposal, spare-part availability
4.	**Define validation and commissioning burden**	Identify whether return to service requires approvals, scripted testing, objective evidence, or other controlled-change activities [10].	Validation protocols, commissioning plans, change-control records, SOPs, quality requirements
5.	**Build the critical path**	Translate the technical path into sequence, labor, testing, and shutdown-window assumptions that actually govern return to service.	OEM participation, plant outage window, staffing assumptions, task sequencing, lead-time quotations
6.	**Translate to BI and scope**	Tie the dependency chain and critical path to period of restoration, mitigation options, and the cost difference between restoration and modernization.	Schedule analysis, interim-workaround options, production constraints, period-of-restoration calculation

Conclusion

Manufacturing plants and other industrial operators keep old computers because those computers often preserve something more valuable than the computer itself: stable machine behavior. The older system may be the last environment in which the software, interfaces, licenses, timing characteristics, and validated workflows all coexist without forcing a larger modernization event. That condition is fragile, but it is not irrational.

For adjusters and consultants, the key lesson is that legacy control computers should be investigated at the system level. A DOS, Windows 95, 98, or XP machine may represent obsolete information technology in a consumer sense, but in an industrial sense it may represent the functional hinge of a much larger process. The decision to retain it, replace it, or migrate away from it should therefore be analyzed through the lenses of safety, availability, interoperability, validation, and business interruption, not age alone [1][4][5][8][10].

References

1. National Institute of Standards and Technology, Guide to Operational Technology (OT) Security, NIST Special Publication 800-82 Rev. 3, September 2023. (Note: NIST issued a pre-draft call for comments on Revision 4 in January 2026; Revision 3 remains operative as of April 2026).
2. J. McCarthy, M. Powell, K. Stouffer, C. Tang, T. Zimmerman, W. Barker, T. Ogunyale, D. Wynne, and J. Wiltberger, Securing Manufacturing Industrial Control Systems: Behavioral Anomaly Detection, NISTIR 8219, July 2020.
3. National Cybersecurity and Communications Integration Center (NCCIC) and Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, U.S. Department of Homeland Security, September 2016. (Note: ICS-CERT functions were absorbed into the Cybersecurity and Infrastructure Security Agency [CISA] in 2018, and these principles are largely incorporated into current NIST guidance).
4. S. S. V. K. Kolla, D. M. Lourenço, A. A. Kumar, and P. Plapper, “Retrofitting of legacy machines in the context of Industrial Internet of Things (IIoT),” Procedia Computer Science, vol. 200, pp. 62-70, 2022.
5. L. Lidén, A Model-Based Approach to Digital Retrofitting and Success Factor Analysis for Legacy Machinery: A Case Study at an Essity Test Center, Gothenburg, master’s thesis, Luleå University of Technology, Luleå, Sweden, 2024.
6. D. Sanchez-Londono, G. Barbieri, and L. Fumagalli, "Smart retrofitting in maintenance: a systematic literature review," published online August 29, 2022; Journal of Intelligent Manufacturing, vol. 34(1), pp. 1-19, 2023. doi: 10.1007/s10845-022-02002-2.
7. MEP National Network, Manufacturers' Guide to Industry 4.0 Technologies, no publication date printed on PDF; NIST server metadata indicates September 2022 upload; NIST-hosted PDF, accessed March 2026.
8. U.S. Government Accountability Office, Information Technology: Agencies Need to Plan for Modernizing Critical Decades-Old Legacy Systems, GAO-25-107795, July 2025.
9. Microsoft, Windows XP lifecycle page, showing extended support end date April 8, 2014, accessed March 2026.
10. U.S. Food and Drug Administration, Computer Software Assurance for Production and Quality Management System Software, Guidance for Industry and Food and Drug Administration Staff, February 3, 2026.

Legal disclosure

This white paper is provided for general informational and training purposes only. It does not constitute legal advice, coverage advice, code-compliance advice, or a substitute for asset-specific engineering analysis. Coverage determinations depend on policy language, jurisdiction, and claim-specific facts. Any restoration, replacement, cybersecurity, validation, or re-energization decision should be based on qualified inspection, applicable standards, manufacturer information when available, and the requirements of the authority having jurisdiction. Mention of specific standards, publications, manufacturers, or operating systems does not imply endorsement. EFI Global reserves the right to revise technical opinions as additional facts, testing, or documentation become available.