ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1241

Control System Obsolescence Management a Proactive Framework for Reliability, Safety, and Operational Continuity

Nagore Hanifa Sikkandar Basha[1]

[1]Automation & Control Unit
SA RTR
Chennai, India

Publication Date: 2026/04/28

Abstract: Control system obsolescence management has become a critical aspect of industrial asset governance, particularly in process industries where operational continuity, safety, and reliability are essential. As automation platforms age, organizations face escalating challenges related to spare parts scarcity, vendor support discontinuation, cybersecurity vulnerabilities, and increasing maintenance complexity. This article presents a proactive framework for managing control system obsolescence through structured asset inventory, lifecycle monitoring, risk assessment, mitigation planning, cybersecurity integration, cross-functional governance, documentation, lifecycle extension planning, and workforce knowledge transfer. The framework supports systematic decision-making and aligns obsolescence management with proactive project control practices. The study concludes that obsolescence management should be treated as a continuous governance process embedded within organizational asset management strategies rather than as a reactive maintenance activity.

Keywords: *Obsolescence Management, Control Systems, Reliability, Cybersecurity, Lifecycle Management, Industrial Automation, Asset Governance.*

How to Cite: Nagore Hanifa Sikkandar Basha (2026) Control System Obsolescence Management a Proactive Framework for Reliability, Safety, and Operational Continuity. *International Journal of Innovative Science and Research Technology*, 11(4), 2264-2267. https://doi.org/10.38124/ijisrt/26apr1241

I. INTRODUCTION

Industrial control systems constitute the backbone of modern process operations, where they are responsible for maintaining operational continuity, protecting assets, and ensuring personnel safety. Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) platforms, and Emergency Shutdown Systems (ESD) serve as foundational technologies in environments requiring precision, resilience, and reliability. However, as these systems age, their continued operation becomes increasingly constrained by obsolescence-related risks.

Obsolescence typically manifests through several interdependent conditions, including limited availability of spare parts, withdrawal of vendor support, and increasing exposure to cybersecurity threats. Legacy systems are particularly vulnerable because they often lack current software updates, security patches, and manufacturer-backed technical assistance. In addition, organizations that defer obsolescence planning may encounter elevated costs and implementation complexity when forced into unplanned modernization after failures occur.

Accordingly, control system obsolescence management should not be viewed solely as a maintenance issue. Rather, it should be recognized as a strategic governance function that supports long-term reliability, safety, and operational continuity. The objective of this article is to present a structured framework for control system obsolescence management that integrates technical, operational, and governance perspectives.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1241

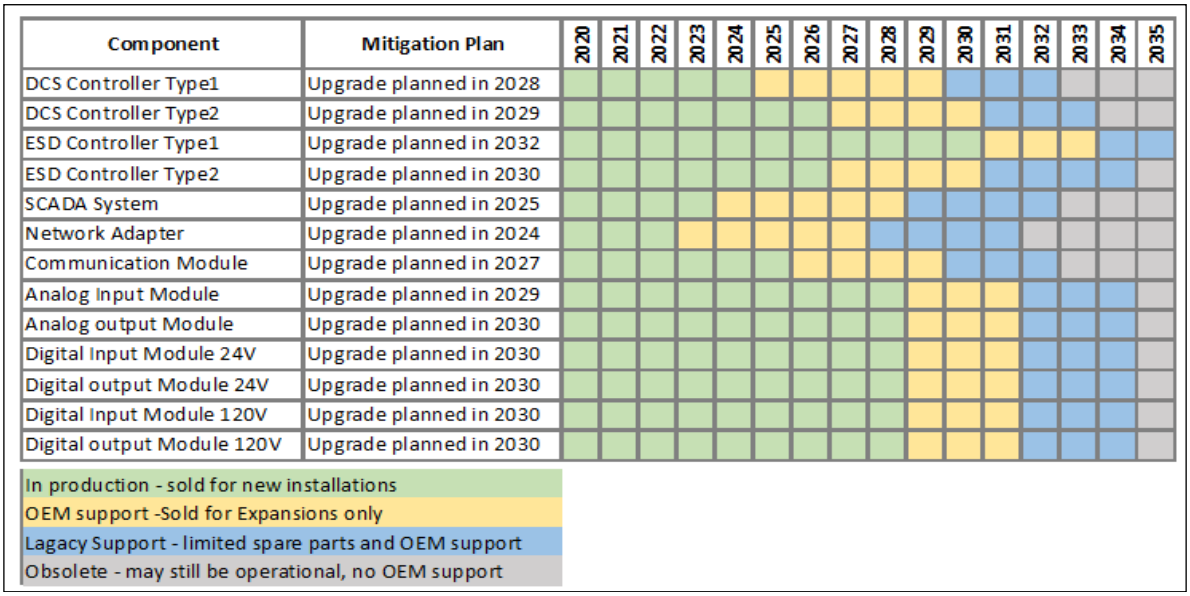

Fig 1. Life Cycle Progression of Control System Components

II. ASSET INVENTORY AND LIFECYCLE VISIBILITY

A complete and current inventory is the foundation of effective obsolescence management. The inventory should include system type, hardware configuration, software version, controller and I/O models, workstation and network architecture, redundancy arrangement, vendor support status, and operational criticality. This baseline enables organizations to maintain visibility over the installed base and identify assets approaching end-of-life or end-of-support conditions.

Each asset should also be evaluated with respect to its lifecycle stage and support status. A practical classification scheme may include fully supported, limited support, legacy support, and obsolete or unsupported. This classification assists decision-makers in determining whether an asset may continue in service, require targeted mitigation, or necessitate replacement or migration.

Asset Name	Model	Quantity	Location	Vendor Support	Spare Parts Available
DCS Controller Type1	C200	2	Control Room 1	No	No
DCS Controller Type2	C300	10	Control Room 2	Yes	Yes
ESD Controller Type1	Controller 800	2	Control Room 1	No	Yes
ESD Controller Type2	Controller 900	6	Control Room 2	Yes	No
SCADA System	Version 9	1	Control Room 3	Yes	Yes
Network Adapter	MTAP	3	Control Room 3	Yes	Yes
Communication Module	CATP	6	Control Room 3	No	Yes
Analog Input Module	AI200_1	4	Control Room 3	Yes	Yes
Analog output Module	AO200_1	3	Control Room 3	Yes	Yes
Digital Input Module 24V	DI200_1	20	Control Room 3	Yes	Yes
Digital output Module 24V	DO200_1	20	Control Room 3	Yes	Yes
Digital Input Module 120V	DI200_2	15	Control Room 3	Yes	Yes
Digital output Module 120V	DO200_2	15	Control Room 3	Yes	No

Fig 2. Asset Inventory Structure For Control System Component Life Cycle Management

This figure presents the principle data elements required to establish and maintain a comprehensive inventory of control system assets.

III. RISK-BASED OBSOLESCENCE ASSESSMENT

Risk-based assessment enables organizations to prioritize resources toward the most consequential obsolescence threats. Criteria may include spare parts availability, failure history, age relative to expected service life, production criticality, support horizon, and migration feasibility. By using defined criteria, organizations can reduce subjectivity and improve consistency in obsolescence decisions.

Table 1: Risk Based Assessment

Criterion	Description	Impact
Spare parts availability	Availability of replacement components	High
Vendor support	Remaining OEM support Duration	High
Failure History	Frequency and severity of failures	Medium

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1241

Production criticality	Consequence of system downtime	High
Migration feasibility	Ease of moving to a new platform	Medium

A structured risk assessment helps distinguish between systems that can be extended with controls and those that require replacement or migration. This step is particularly important in industrial environments where even short interruptions can create significant operational and financial consequences.

IV. MITIGATION AND LIFECYCLE EXTENSION PLANNING

For systems assessed as high risk, mitigation planning should include actions such as securing critical spares, establishing extended support agreements, retrofitting obsolete modules, sourcing approved third-party components, reusing parts from decommissioned systems, and planning phased migration to updated platforms. Where continued operation is justified, lifecycle extension must be supported by trend monitoring, maintenance planning, and formal risk acceptance.

Mitigation planning is most effective when it is initiated before failures occur or vendor support is withdrawn. Early intervention reduces the likelihood of unplanned outages and allows organizations to plan procurement, testing, and commissioning activities in a controlled manner.

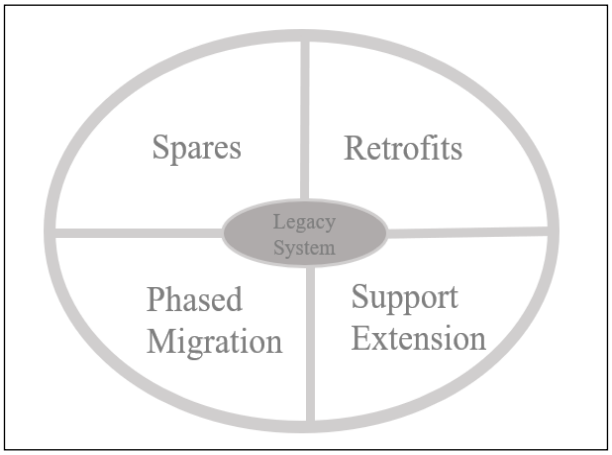

Fig 3. Migration Criteria for Legacy Systems

V. CYBERSECURITY INTEGRATION

Cybersecurity must be considered an integral component of obsolescence management. Legacy systems may present elevated exposure due to unsupported operating systems, unpatched software, weak access controls, and limited segmentation. Consequently, cybersecurity assessments should be conducted alongside lifecycle reviews, with compensating controls applied where immediate modernization is not feasible.

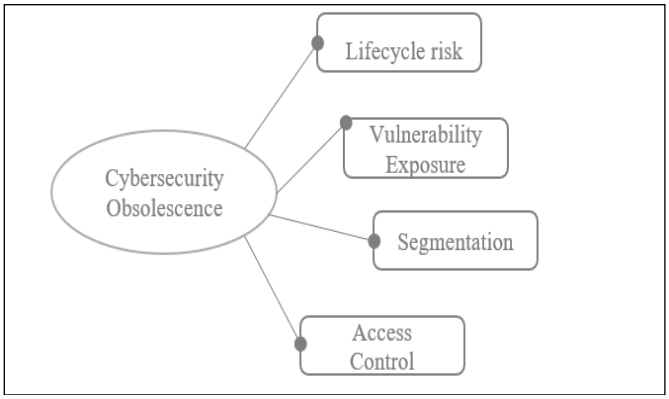

Fig 4. Cybersecurity and Obsolescence Integration Model

This integrated approach ensures that lifecycle decisions address both operational resilience and cyber risk. In practice, cybersecurity considerations should be embedded in the same governance process used for reliability and maintenance planning.

VI. CROSS-FUNCTIONAL GOVERNANCE

Successful obsolescence management depends on collaboration among maintenance, reliability, operations, engineering, procurement, cybersecurity, and vendor representatives. A cross-functional governance model enables integrated evaluation of technical feasibility, operational risk, cost implications, and implementation timing. Such collaboration is essential for sustainable decision-making.

Documentation should be maintained throughout the lifecycle of the obsolescence management process, including asset records, assessment results, support statements, failure trends, mitigation plans, and migration schedules. Training and knowledge transfer are equally important, as they reduce dependence on a limited number of personnel and preserve organizational memory.

VII. PROJECT CONTROL ALIGNMENT AND IMPLEMENTATION

Control system obsolescence management should also be aligned with project control practices so that material procurement, schedule forecasting, vendor commitments, and implementation planning are addressed early and systematically. This alignment allows organizations to anticipate risks, minimize delays, and improve resource utilization.

The proposed implementation model is organized into sequential stages. First, a baseline asset survey should be conducted to establish a reliable inventory of all control system components. Second, assets should be classified according to criticality and support condition. Third, a structured risk scoring method should be applied to identify high-priority obsolescence concerns. Fourth, a multidisciplinary governance team should review the results

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr1241

and determine the appropriate mitigation path for each critical system.

Implementation activities should be coordinated with planned outages, budget cycles, procurement lead times, and maintenance windows. Where necessary, migration projects should be phased to reduce operational disruption. Cybersecurity reviews should be embedded throughout the process to ensure that systems awaiting replacement remain protected through appropriate compensating measures. Documentation and training should be sustained throughout implementation to support continuity and organizational learning.

VIII. DISCUSSION

The proposed framework contributes to several important operational outcomes. First, it improves asset visibility by allowing organizations to identify aging systems earlier and more accurately. Second, it enhances risk prioritization by introducing consistency into obsolescence-related decision-making. Third, it reduces the likelihood of unplanned failure by enabling proactive intervention before critical degradation occurs.

The integration of cybersecurity into obsolescence planning is particularly significant, as legacy systems often remain in service beyond their intended lifecycle. By addressing vulnerability exposure, patch limitations, and access control deficiencies, organizations can strengthen their resilience against cyber threats. Additionally, lifecycle extension becomes more defensible when supported by formal governance, structured spares strategies, and disciplined monitoring.

From an organizational perspective, cross-functional governance and knowledge transfer promote continuity by improving coordination and reducing reliance on isolated expertise. When aligned with project control, the framework also contributes to improved schedule predictability, material readiness, and resource optimization. Collectively, these benefits demonstrate that obsolescence management should be treated as a strategic governance process that supports both immediate operational requirements and long-term enterprise resilience.

IX. CONCLUSION

Control system obsolescence management is an essential requirement for sustaining safe, reliable, and efficient industrial operations. The framework presented in this manuscript emphasizes asset inventory, lifecycle tracking, risk assessment, mitigation planning, cybersecurity integration, cross-functional governance, documentation, training, and project control alignment as mutually reinforcing components of effective practice.

By implementing this framework, organizations can improve asset visibility, reduce exposure to unplanned failure, strengthen cybersecurity posture, extend the useful life of legacy systems where appropriate, and improve coordination across functional domains. The findings support the conclusion that obsolescence management should be embedded within routine governance processes rather than triggered only by failure or support termination. Future research may extend this work through quantitative risk models, predictive analytics, and implementation benchmarking across industrial sectors.

REFERENCES

[1]. Purna Kiran 2024, A guide to obsolescence studies on control systems.
[2]. Thomas E. Herald, Obsolescence Management Forecasting: for Strategic Operational System Sustainment Decision Making, 2012.
[3]. Guidance on managing obsolescence and upgrading industrial automation and control systems, first Edition published by Energy Institute, London.
[4]. Bjoern Bartels , Ulrich Ermel , Peter Sandborn and Michael G. Pecht, Strategies to the Prediction, Mitigation and Management of Product Obsolescence (Wiley Series in Systems Engineering and Management) First Edition.
[5]. Book of Obsolescence Management Includes EU Automation's seven steps to obsolescence management.