Control system obsolescence

Scalable solutions
From simple modifications to major EPC/MAC contracts

Full lifecycle services
Including concept, feasibility, FEED, design, manufacture, installation, commissioning to ongoing support

Key technologies
DCS, PLC, SCADA, HMI, RTU and Telemetry

How does control system obsolescence impact your operations?

Increased downtime

Outdated systems can cause equipment failures and are vulnerable to cyber attacks, resulting in increased costs and lost revenue.

Rising maintenance costs

As parts become scarce, the costs of maintaining obsolete systems rise. Additionally, specialised expertise may be necessary to manage legacy systems, further increasing expenses.

Regulatory compliance and safety issues

Older systems may not meet current safety, cybersecurity and environmental standards, exposing companies to compliance risks and potential fines.

Unrealised efficiencies

Ageing control systems often lack the ability to integrate with modern technologies, making it harder to gain efficiencies using data analytics and operational insight.

Managing obsolescence

Prioritising a technology modernisation strategy in alignment with investment and regulatory demands is challenging. Immediate replacement of obsolete systems isn't always feasible due to funding, operational and resource constraints.

With many legacy assets nearing obsolescence, automation and control system upgrades must balance financial considerations and acceptable risk levels.

Wood's expertise ensures effective, pragmatic, fit-for-purpose solutions for automation and control system obsolescence at every stage.

Short-term mitigation

Perform obsolescence mapping and evaluation

- Automation system component overview
- Risk analysis and classification of criticality
- End-of-life (EOL) assessment

Protect vulnerable legacy systems from cyber threats

- Firewalls, OT segmentation and intrusion detection
- Patch management and monitoring

Secure reliable access to parts and support

- Critical spare parts inventory
- Knowledge base for operations troubleshooting

Long-term mitigation

Manage replacement of obsolete systems

- Replacement plans prioritising high-risk systems
- Explore modular upgrade options

Adopt new technologies for future-readiness

- Introduce Industrial Internet of Things (IIoT) sensors, cloud-based SCADA and edge computing
- Leverage AI-driven predictive maintenance
- Integrate digital twins to simulate and system test
- Implement virtualisation to enable hardware independence

Ensure compliance to national and international safety, cybersecurity and operational standards

- ISO 55000, IEC 61508, IEC 62443, ISO 13849, NIST / NIS2

Outdated control systems are particularly vulnerable to cyberattack as they often lack modern security protocols

How Wood can help

Criticality assessment and lifecycle management 01

Wood can perform a complete audit of infrastructure system health, evaluating the risk profile and developing a proactive approach to managing the lifecycle of automation components.

Upgrade or replace vulnerable systems 02

Where systems are defined as high risk, Wood will develop a managed migration plan to upgrade with modern, compatible and secure alternatives.

Phased replacement strategy 03

Wood can develop a phased approach, upgrading critical components first while planning for a full replacement over time. We review interoperability to ensure partially upgraded systems remain functional.

Technology assessment and selection 04

As an independent systems integrator, we will review and assess the most appropriate upgrade or replacement solution using industry experience and knowledge.

Virtualisation and simulation tools 05

Wood can virtualise older systems, decoupling software from the hardware, and employ simulation tools to test new upgrades, extending the asset life of legacy equipment while minimising risks.

Network segmentation 06

We can isolate legacy operational technology systems to add an extra layer of OT security, reducing the potential impact of infiltration and cyber attacks.

Cybersecurity layering 07

Our digital and network specialists can design and deploy modern firewalls, encryption and intrusion detection systems to safeguard legacy equipment.

Security patching 08

For systems that cannot be replaced immediately, Wood can collaborate with technology vendors to assess, manage and monitor updates and patching routines.

Employee training 09

Wood can assess the training requirements for operational staff and maintenance personnel for any new control systems or upgrades and provide simulation, training and documentation support.

About us

Multi-sector
expertise

$200M+
revenue (2024)

500+
automation and integration specialists

Top 5
independent systems integrators in the world

Consulting and engineering expertise in automation, control and cybersecurity to enhance operational efficiency and security across your OT and IT environments

We have the solutions.

Asset Health
Extending assets through real time data-driven insights

Digital-led Decarbonisation
Accelerating the transition to a low-carbon future

Digital Assets & DataOps
Developing the building blocks of digital transformation

Process Optimisation
Boosting production and efficiency to maximise return

Automation & Systems Integration
Designing secure, reliable and operable digital ecosystems

As one of the largest independent systems integrators, Wood will guide and support you through every step of managing operational technology obsolescence.

See how we can help
woodplc.com/digital