THE CHALLENGE OF OBSOLESCENCE
IN UK CRITICAL INFRASTRUCTURE

A paper by

ZIRCON
SOFTWARE ENGINEERING

Introduction

The UK's critical infrastructure – including its railways, highways, and industrial sectors – relies heavily on assets designed to last for decades, if not centuries. However, the digital systems and software that increasingly control and monitor these assets have a much shorter lifespan; often less than ten years.

This disparity creates significant operational, security, and financial risks, as software systems become obsolete far earlier than the physical assets they are designed to support.

Zircon Software has investigated the growing gap between the longevity of physical infrastructure and the rapid pace of software obsolescence. We draw on research from multiple fields and case studies, while also presenting statistical evidence of the challenges posed by ageing software and hardware systems.

Our expertise also gives us insight into the railways, highways, and industrial sectors we serve, where we outline possible solutions for managing obsolescence in the digital age.

Contents

- Operational lifespans of physical vs. digital assets ..... Page 2
- Software obsolescence in critical infrastructure ..... Page 3
- The drivers creating the challenges around software obsolescence ..... Page 4
- The challenges of making old assets work in a digital age ..... Page 4
- Potential solutions to obsolescence management ..... Page 5
- Final thoughts ..... Page 6
- References ..... Page 6

Operational lifespans of physical vs. digital assets

Physical assets

Historically, physical infrastructure assets (be they bridges, tunnels, or power plants) were designed with lifespans ranging from 50 to 100 years [1] – and a study from 2023 has found that at least 86 of the UK's critical road network structures are over 120 years old [2].

Similarly, the UK's rail network continues to use bridges and trackside infrastructure from the 19th century. In 2022, a £7.5 million maintenance project on Scotland's Forth Bridge (which has been in operation since 1890) was completed, securing the iconic structure for another 30 years [3]. Examples like this demonstrate the longevity of well-maintained physical infrastructure.

In stark contrast, digital assets – including the software used to monitor, control, and manage these physical infrastructures – have far shorter lifecycles.

Digital assets

Research from the European Union's Joint Research Centre indicates that the average software lifecycle is less than 10 years, with many systems becoming obsolete within six to eight years [4]. This could be due to a lack of updates, security vulnerabilities, incompatibility with newer hardware, or software engineers retiring or moving on.

This discrepancy creates a dangerous situation for critical infrastructure and systems: ageing software running on physical assets becomes a liability.

In a 2024 report by NTT DATA [5], 66% of UK organisations report that their network assets are mostly ageing or obsolete. The same report highlighted that 75% of UK executives believe legacy infrastructure significantly impairs their business.

This misalignment of lifecycles complicates maintenance and increases costs, as operators are forced to upgrade software more frequently than the physical infrastructure it supports, deploy physical teams to sites unnecessarily, or a mixture of both.

Software obsolescence in critical infrastructure

Railways

The UK's rail network is particularly vulnerable to software obsolescence.

A 2023 report from the Office of Rail and Road and Network Rail has mapped the remaining life of assets to the regional and national signalling programmes over the next 30 years.

The number of assets that are now being scheduled for renewal after their effective end of life is increasing - expected to peak nationally in 2037/2038. At this point over 25% of SEUs (Signalling Equivalent Units) will have less than five years to end of assets remaining life, and this will peak at over 35% in the North West and Central region [6].

Though not directly related to an issue of obsolescence, we can draw parallels to the potential scale of the fallout of failing to address weaknesses introduced via obsolescence to the ongoing damage caused by the CrowdStrike outage of 2024, which caused global transport chaos from a single miscoded security software update [7].

The rail industry also faces the challenge of migrating away from the Global System for Mobile Communications-Railway (GSM-R). This critical train radio system is currently based on 2G mobile network technology, which is fast becoming obsolete with the large-scale consumer shift toward 5G, and there are few engineers left with the skills to maintain it. GSM-R is so prevalent in the industry that they need to migrate to the Future Railway Mobile Communications System (FRMCS) to mitigate this problem [8].

Highways

The UK's highways sector faces a similar challenge. Take the rollout of smart motorways – which relied on digital monitoring and control systems to manage traffic flow and safety. It was severely hampered by software obsolescence.

An undercover investigative journalist found that many smart motorway systems, implemented only recently, are already facing significant security and safety risks due to obsolete hardware and software failures [9].

It's worth noting that in 2023, all new smart motorways were scrapped, as public confidence dropped; safety and reliability came under heavy scrutiny, as did the mounting costs of the project.

As the shift towards autonomous and connected vehicles along with the adoption of predictive traffic management systems (PTMS), there is growing concern about the compatibility of current infrastructure with future digital needs.

Industrial

Software obsolescence is of particular concern in military and defence manufacturing, where project lifecycles can exceed 25-30 years [10] – especially when many software systems become obsolete within six to eight years [4].
These systems, many of which are no longer supported by their original developers, present significant risks of failure. The shift towards the Industrial Internet of Things (IIoT) has further exacerbated the problem.

Older machines, while still operational, were not designed to communicate with modern IIoT platforms, leading to a lack of real-time data visibility and control. Documentation may be scarce, leading to an increased burden of reverse-engineering old systems to find out how they work.

This means that the cost of retrofitting old machinery with modern sensors and connectivity can be prohibitive, leading some companies to defer necessary upgrades – increasing the likelihood of operational disruptions.

The drivers creating the challenges around software obsolescence

There are several key drivers creating the challenges around software obsolescence:

Hardware

When hardware becomes obsolete, the software usually needs to change with it. This is often due to increasing system complexity – but also, old system architectures may not be compatible with modern programming; a transition from 32-bit to 64-bit architecture is an example of this.

Cybersecurity

Operating systems and software packages need to be patched to fix cybersecurity issues. At a certain point in the software lifecycle, security updates stop being supported – and exploitable vulnerabilities can become known by attackers.

Older software lacks the latest security measures; this increases the impact of vulnerabilities, makes exploitation more likely to succeed, and makes detection of any exploitation more difficult. High-impact security incidents are more likely with obsolete software, and there are limits on the security measures that will be effective – even against relatively low-skilled attackers.

Compatability

There may be compatibility issues with newer digital systems, like remote monitoring, smart city data platforms, and predictive maintenance to improve efficiency.

The challenges of making old assets work in a digital age

Analogue-to-digital transition

One of the most significant challenges in managing obsolescence is the transition from analogue systems to digital control. Research by the Institution of Civil Engineers (ICE) highlights the difficulty in integrating modern digital solutions with legacy infrastructure, particularly in sectors like railways and energy [11].

In the railway sector, much of the existing infrastructure was designed in an era when analogue systems were the norm. Modernising this infrastructure requires significant investment in retrofitting analogue assets with digital systems capable of interfacing with software solutions.

This process can take years, and involve complex engineering work – adding to the cost and risk of obsolescence.

Fragmented asset management

Another challenge is the fragmented nature of asset management across the UK's infrastructure sectors.

Many organisations use a combination of legacy and modern systems, leading to a patchwork of technologies that are difficult to integrate and manage.

This lack of standardisation is a key barrier to effective obsolescence management. Fragmentation complicates efforts to modernise systems and adds to the risk of software obsolescence.

Potential solutions to obsolescence management

Software obsolescence management

A key solution to the challenge of obsolescence is adopting proactive software lifecycle management. The UK's National Cyber Security Centre (NCSC) recommends that critical infrastructure operators develop comprehensive obsolescence management strategies [12], which include:

Lifecycle planning

Aligning software updates with the expected operational life of physical assets. For example, integrating software upgrade cycles into the routine maintenance schedules for physical assets could reduce the likelihood of system failure.

Modular software design

Developing modular software that can be easily updated or replaced without disrupting the entire system.

Cloud-based solutions

Moving to cloud-based infrastructure management systems, which are more scalable and adaptable to new technologies.

Digital twin technology

Digital twin technology offers a promising solution for managing the integration of old physical assets with modern software. Digital twins can help infrastructure operators predict when physical components will fail, and even have the potential to predict software failures, allowing for more efficient maintenance and upgrades. In some cases, digital twins can cut fault detection costs in critical infrastructure by 66% [13].

By creating virtual replicas of physical assets, infrastructure operators can simulate software updates and test their compatibility before deploying them – reducing the risk of failure and operational downtime.

Invest in innovation to address obsolescence

To effectively tackle obsolescence and prevent major operational and safety incidents, upfront investment and strategic planning are crucial. The UK government's Industrial Strategy [14] allocates substantial funding and resources for research and development in infrastructure technologies, particularly aiming to enhance the integration of digital and physical systems.

This investment is vital for developing the next generation of software and hardware solutions, which will help extend the lifespan of the UK's critical infrastructure.

An active strategy must be put in place to assess existing assets for hardware and software obsolescence. Following this assessment, a comprehensive roadmap should be created, detailing the priorities and timelines for addressing these issues, and ensuring they are seamlessly integrated into operational planning.

Implementation may require systems that support over-the-air updates or incorporate equipment upgrades into regular maintenance schedules. To facilitate the seamless replacement of components, a suitable testing environment must be developed, or existing facilities enhanced, to accommodate these updates effectively.

Final thoughts

Software obsolescence poses operational, financial, and security risks.

The obsolescence of software systems in the UK's critical infrastructure is a growing concern, particularly as physical assets continue to operate for decades while the software controlling them becomes outdated within a few years. The number of clients engaging with us to resolve obsolescence issues has increased, and we expect this trend to continue.

Addressing obsolescence requires proactive lifecycle management, investment in modern technologies like digital twins, and continued R&D.

By adopting these strategies, the UK government, infrastructure providers, and essential industries can ensure that critical systems remain resilient, secure, and future-proofed for a digital age.

References:

[1] **Highways Magazine, 2020**
Extending the life of bridges with integrated solutions
Available at https://www.highwaysmagazine.co.uk/ as of November 2024

[2] **Johnson, T. 2023**
Exclusive: 86 structures in operation on Strategic Road Network over 120 years old
Available at https://www.newcivilengineer.com/ as of November 2024

[3] **Network Rail, 2024**
Safeguarding the Forth Bridge
Available at https://www.networkrail.co.uk/ as of November 2024

[4] **Youth Award, 2019**
Average Expected Lifespan of Custom Software Solutions in 2019
Available at https://www.youthaward.org/ as of November 2024

[5] **Williams, S. 2024**
UK's outdated tech hampers business progress – report
Available at https://itbrief.co.uk/ as of November 2024

[6] **Office of Rail and Road, Network Rail. 2023**
Independent Report #35840 Conventional Signalling and Obsolescence Management
Available at https://www.orr.gov.uk/ as of November 2024

[7] **Atack, P.R. 2024**
Global transport systems struck by IT failure
Available at https://www.railway-technology.com/ as of November 2024

[8] **Darlington, P. 2023**
Migrating from GSM-R to FRMCS
Available at https://www.railengineer.co.uk/ as of November 2024

[9] **Coen, S. 2021**
Rebellion breaks out over smart motorways as roads chief tries to play down probe into 'death trap' system
Available at https://www.dailymail.co.uk/ as of November 2024

[10] **Rajagopal, S. Erkoyuncu, J.A. Roy, R. 2015**
Impact of Software Obsolescence in Defence Manufacturing Sectors
Available at https://pdf.sciencedirectassets.com/ as of November 2024

[11] **Institution of Civil Engineers**
Civil engineering insights into digitally retrofitting infrastructure assets and networks
Available at https://www.ice.org.uk/ as of November 2024

[12] **The National Cyber Security Centre**
Technology assurance
Available at https://www.ncsc.gov.uk/ as of November 2024

[13] **Martins, L.D. 2023**
Digital twin technology to slash grid fault detection costs by 66%
Available at https://www.current-news.co.uk/ as of November 2024

[14] **Gov.uk, 2023**
£360 million to boost British manufacturing and R&D
Available at https://www.gov.uk/ as of November 2024

About Zircon Software

Zircon is a UK software engineering company, founded in 1999. We are the trusted global partners to blue-chip companies, government agencies, and infrastructure providers.

We solve the biggest software challenges in critical infrastructure and systems engineering. Our mission is to build the software that enables the world to work, and engineer solutions that bridge the gap between legacy and next-gen technologies.

Email:
enquiries@zirconsoftware.co.uk

Phone:
+44 (0) 1225 764 444

Web: https://zirconsoftware.co.uk/

Address:
Bellefield House
Hilperton Road
Trowbridge
BA14 7FP

ZIRCON
SOFTWARE ENGINEERING