



HOW TO **DERISK** DELIVERY OF SMART BUILDINGS

Unlocking better project outcomes with
our technology test labs

JUNE 2026



Smart building technologies are now business-critical infrastructure – interwoven with IT, Operational Technology (OT) and cyber security and increasingly forming the foundation of wider smart places that connect buildings, users and digital services across estates and portfolios. Yet across many projects, these systems are still designed, procured and deployed under delivery models that were not originally designed to address the current level of technical complexity or risk.

Through our work across commercial offices, healthcare, and complex estates, we consistently see the same challenges: late discovery of integration issues, limited visibility of real-world performance, technology choices driven by claims rather than evidence, and cyber security and IT approvals becoming programme-critical risks during construction.

We wrote this paper to illustrate how those challenges can be tackled at a building level, and as clients scale these solutions across multiple buildings and wider estates. It sets out a structured approach intended to help address uncertainty in technology delivery by focusing risk assessment earlier in the delivery lifecycle, including early-stage validation of systems, integrations and security assumptions, before time pressure and site constraints dominate decision-making.

This perspective is grounded in the experience of our building technology systems team, who work across strategy, design, systems integration and delivery. By testing smart building technologies in controlled environments, we help clients turn assumptions into evidence, and make informed decisions.



Mark Ince

Building Technology Services Director



RESHAPING THE BUILT ENVIRONMENT WITH SMART BUILDINGS

Technology is increasingly deployed across multiple buildings and integrated platforms to create smart places – where systems, data and services operate cohesively at campus, estate or portfolio scale. As the UK faces rising energy costs and higher expectations from occupiers, developers are increasingly looking to technology to meet these challenges.

Smart buildings use connected technologies to monitor and optimise building systems, providing real-time insight into performance and enabling issues to be addressed before they disrupt operations.

Key benefits can include:

- Reduced operating costs through more efficient energy use and system optimisation
- Greater building resilience by identifying faults early and minimising unplanned downtime
- Improved tenant experience through more reliable and comfortable environments
- More accurate measurement of energy use and carbon emissions across individual buildings and wider portfolios, enabling owners to track and demonstrate decarbonisation progress over time

This shift brings greater exposure to cyber security risks, highlighting the need for building systems to be securely designed, thoroughly tested and well integrated to ensure they perform as intended.



A FAST-EVOLVING CYBER LANDSCAPE

RISK IS GROWING

Research from the [UK Government](#) has uncovered that 43% of UK businesses and 30% of charities faced cyber attacks in 2024. These are mostly phishing incidents, with the goal of gaining access to the wider network and interfering with physical building systems.

In 2025, 204 nationally significant cyber incidents were reported, representing a 130% increase from the previous year, according to the [National Cyber Security Centre](#). The same report suggests four nationally significant cyber attacks occur on average every week in the UK — some causing disruption at a scale to become national news or impacting local authorities.

According to the [RICS UK Facilities Management Survey 2024](#), 27% of respondents revealed their building faced a cyber attack over the previous year.

These statistics highlight the growing threat landscape in the UK and the need for enhanced national cyber security measures.

THE COST OF CYBER COMPLACENCY

Deployment across multiple interconnected sites increases risk across Smart Places, increasing the importance of consistent governance across sites. Cyber security is increasingly vital for every organisation due to its significant impact on operational resilience and financial stability. In the UK, a significant cyber crime was projected to cost businesses £14.7 billion a year, according to 2025 research from the [UK Government](#).

Additionally, [another report](#) found that only 30% of businesses surveyed adhered to the UK Government's Cyber Essentials standards to defend against evolving online threats as of 2026. Building systems are increasingly targeted because they are perceived to have less defences than corporate networks.

These figures reinforce the urgent need for UK businesses to strengthen their cyber security measures, ensuring appropriate investment in people, processes and technology to mitigate risks and safeguard critical assets.



Buildings are more than just concrete and glass anymore, they rely on efficient, safe and modern functionalities enabled by a lot of digital technology in those buildings, that's why we call them smart. But this digital infrastructure needs to be protected and well managed over the lifespan of a building too – that is our cyber security offering. From secure-by-design to maintaining security during operation, we can help clients integrate digitally reliable solutions to shape resilient buildings.



Betty Helienek
Global Digital Lead
Director OT Cyber Security

UNLOCKING BETTER OUTCOMES



SHIFTING FROM REACTIVE TO PROACTIVE APPROACHES

When delivering smart buildings for global organisations, technology and software must pass corporate approval processes and security gateways before they can be deployed into live IT and Operational Technology (OT) environments.

Any solution connected to a client's network is required to meet stringent cyber security standards and progress through formal client IT approval procedures.

This requirement is frequently underestimated within traditional construction delivery models and is often treated as a client-owned risk. In practice, this can result in significant delays to the installation, integration and commissioning of building technologies.

Our technology test lab addresses this challenge by providing a controlled environment where vendors, installers and client IT teams can collaborate early in the programme. Technical issues are identified and addressed earlier in the delivery process, enabling solutions to be tested and validated in a controlled setting. As a result, technology components can enter Stage 5 already validated, reducing uncertainty and enabling more efficient deployment.

We have developed a methodology in collaboration with client IT approvers to mitigate this risk, providing a dedicated environment for testing building technologies prior to on site deployment in Stage 5.

OUR PROCESS

INNOVATE

Establish a closed test environment to validate functionality isolated away from operational systems

INTEGRATE

Confirm that devices and systems deliver the expected functionality in practical scenarios

VALIDATE

Identify and resolve interoperability challenges, validate alignment with client IT requirements & building standards

OPTIMISE

Plan for operation, using data to drive continuous optimisation, moving to "Insights as a service"

SECURE

Test cyber security measures against client requirements and industry standards

REDEFINING POTENTIAL WITH OUR TECHNOLOGY TEST LABS

We deliver this work in collaboration with a Master Systems Integrator (MSI) with experience in implementing intelligent, automated and secure building systems.

The technology system architecture of the test lab mirrors the layered structure of the broader smart building system, including field equipment, network infrastructure, middleware and cloud-based analytics.

A typical testing sequence takes 6 to 8 weeks and provides an opportunity to test equipment and technologies as well as vendors' customer service and operational support in getting the devices integrated.

Working in this way also allows the client to be directly involved in the decision-making and validation process. IT, security and other teams like facility management can observe integrations as they happen, gaining early familiarity and provide immediate feedback on the configuration and vendor choices. This shared visibility helps avoid misunderstandings later in the programme.

The collaborative format enables the project team to see integration patterns and begin documentation in real time. As devices are onboarded, lessons learned are captured into updated technical specifications so the correct route to deployment can be replicated for the live environment scenario in later stages of the project.



[Watch this video](#) to see how we delivered this in collaboration with MSI partner Thanium Nine.

“

The technology test lab brings real-world integration into RIBA Stages 3 and 4, allowing us to specify systems using measured performance data rather than manufacturer claims. We see how devices communicate, measure parameters and, most importantly, how they integrate to the BMS and HVAC controls systems. This enables us to derisk the delivery, improving efficiency, and delivering a “smart building” which is truly smart.

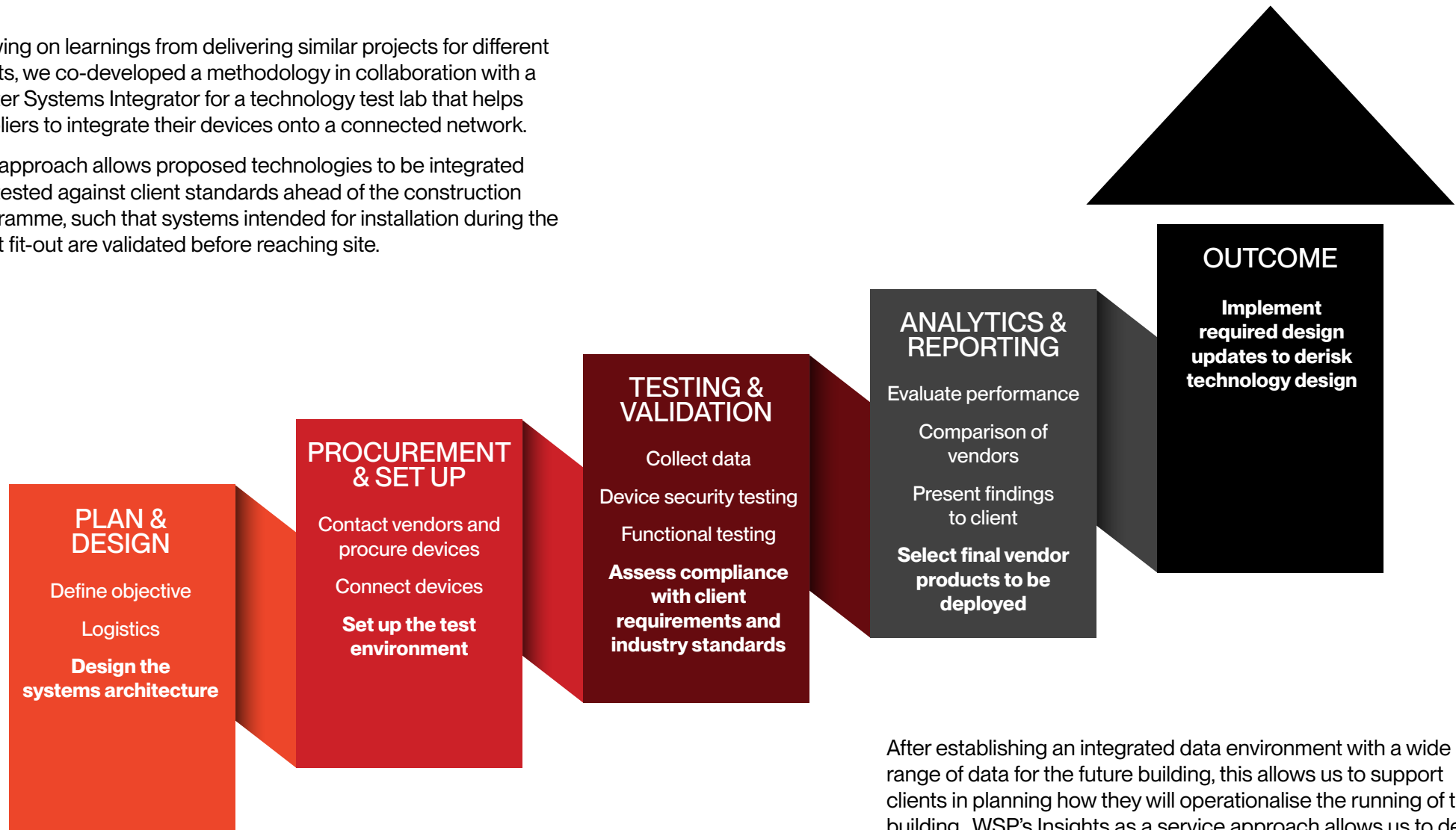


Nico Lomas
Associate Building
Technology Services

AN ITERATIVE PROCESS

Drawing on learnings from delivering similar projects for different clients, we co-developed a methodology in collaboration with a Master Systems Integrator for a technology test lab that helps suppliers to integrate their devices onto a connected network.

This approach allows proposed technologies to be integrated and tested against client standards ahead of the construction programme, such that systems intended for installation during the client fit-out are validated before reaching site.



After establishing an integrated data environment with a wide range of data for the future building, this allows us to support clients in planning how they will operationalise the running of their building. WSP's Insights as a service approach allows us to deliver post occupancy analytics, using live data to drive FM operational approach to building optimisation.

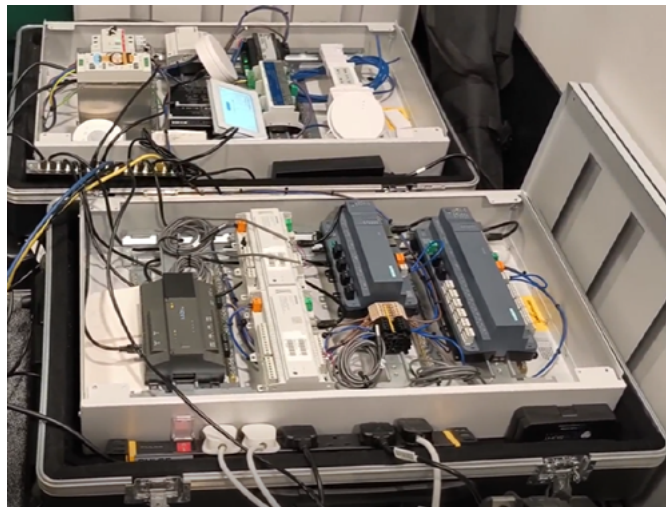
DERISK TECHNOLOGY DELIVERY WITH TECHNOLOGY TEST LABS

Commissioning our own in-house lab gave us insights into the performance of the individual devices/systems. It has also allowed us to better understand procurement and integration challenges and how to apply these learnings to other projects.

System connectivity plans, which had been drafted based on the information provided by vendors, had to be adjusted as we encountered installation issues. e.g. sensors where additional infrastructure and hardware were required and not communicated directly by vendors prior to installation.

It would be reasonable to assume if this type of equipment or information gap had surfaced on site during a pressured period of delivering the final fit out, it would be likely that unmanaged switches or similar would have been deployed as a quick fix. A thorough interrogation of all aspects of integration in a lab environment ahead of the final installation helps mitigate this risk.

The technology test lab also reinforces the integrity of the entire smart building programme by providing empirical validation of system performance, interoperability, and security compliance before committing to full-scale deployment. This protects the client's investment and ensures optimal return on smart building technology expenditure.



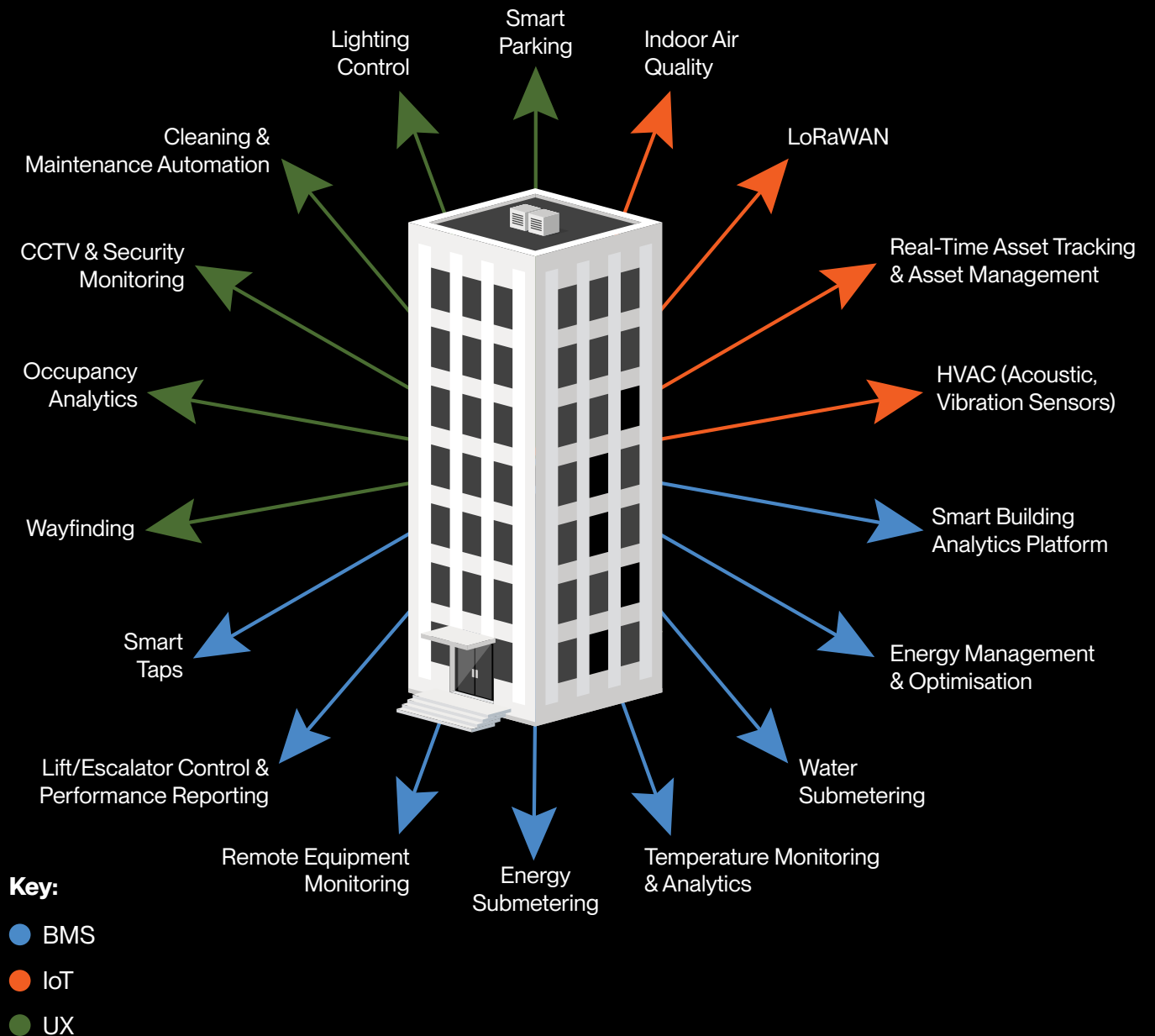
CANDIDATE TECHNOLOGIES SUPPORTED BY OUR TECHNOLOGY TEST LAB

Smart buildings depend on many interconnected technologies operating reliably as a single ecosystem.

Our technology test lab enables a broad range of building, digital and operational systems to be integrated, tested and validated as a connected ecosystem.

This reduces risk and improves confidence before deployment.

By bringing candidate technologies into a shared, controlled environment, we can test integration pathways, data quality, cyber security and operational performance before solutions reach site.



PROJECT LEARNINGS & APPLICATIONS



INSIGHTS FROM REAL-WORLD TESTING

Having applied this approach across several sectors, we have seen first-hand how early testing surfaces technology integration challenges that would otherwise go undetected until deployment. The insights in this section reflect what we have learned from working on specific healthcare and commercial projects, each with its own pressures, priorities and complexities, with findings that are relevant to broader sectors.

Commercial

Rising occupier expectations, hybrid working patterns and increasing operational costs are placing new demands on commercial buildings. Owners need workplaces that respond to real-time conditions while delivering comfort, efficiency, resilience often in shared multi-tenant buildings environments.

Achieving this requires building management systems, user platforms and digital infrastructure to work together consistently, with occupier needs driving strict corporate IT and security requirements.

Testing these technologies and integrations before deployment allows us to validate performance, assess user experience outcomes and resolve issues early, reducing risk and supporting reliable operation from the outset.

Healthcare

Smart hospitals bring together data, automation and interoperable systems to improve clinical workflows, asset performance and estate operations, with an ultimate goal of improving patient outcomes. Moving from siloed technologies to a connected ecosystem demands a coordinated approach, ensuring data flows securely between systems in a highly regulated environment.

The imperative to protect patient data places particular scrutiny on how connected devices perform. Setting up and testing IT/OT networks and selected systems in a prototype environment allows us to demonstrate how each system operates, verify interfaces and identify interoperability issues before they impact live clinical settings.



Technology test labs have been delivered in the client's own ICT spaces, with isolated environments used to deliver POC testing of head-ends, servers and sensors with testing via remote terminals.

KEY FINDINGS

DEVICE CONNECTIONS

Additional hardware was required in some cases. Once identified, appropriate hardware for connectivity was updated in collaboration with client IT teams on the client system architecture.

CYBER SECURITY

Some devices showed insecure or unknown open ports. This could allow bad actors access to the device or network posing a significant risk to the building. Our testing allowed us to specify the closure of these ports allowing for a secure design.

INTEGRATION CHALLENGES

Integrating different devices proved difficult, as each device had unique requirements and did not always align with the expected standards or vendor claims. This often needed troubleshooting and collaboration with the vendors.

ACCURACY TESTING

Through structured tests team members validated the accuracy of data captured by devices and supplied to platforms such as occupancy and smart analytics. This helps identify the most accurate device or system currently on the market.

DATA USAGE

Some devices used significantly more data than devices from other vendors. This has the potential to result in higher cloud messaging costs for the client and was a useful metric for evaluation.

WHAT WE TESTED

A range of device and system parameters were evaluated to assess the functional and non-functional performance of the devices/systems (eg response times, error rates).

CASE STUDY - COMMERCIAL OFFICES

LONDON, UK | CONFIDENTIAL CLIENT

We provided multidisciplinary services for a global financial services company developing a new European Headquarters in London. We delivered smart building technology design from Stage 2 onwards, addressing both base build infrastructure monitoring and client fit-out requirements. This development delivers a smart building that leverages integrated data to deliver a frictionless occupant experience, efficient & highly resilient operations.

The smart building scope included strategy development, technology procurement design management and oversight through installation and operation. The client's aim was to deliver an exceptional building of the future, leading their standard for building deployments.

Base build infrastructure monitoring was an important aspect to validate that the client's desired building technology integrations could be achieved across procurement and responsibility boundaries, while meeting the client's robust requirements for IT resilience and information security. We worked with the project MSI to deliver a technology test lab where selected technologies were deployed, integrated and validated ahead of the construction installation.



OT network arrangements are also a key consideration for smart building design. The right arrangement varies significantly by project type (multi-tenant vs single tenant).

The collaborative efforts of the client's departments, including corporate IT, engineering and their global operations partner, was essential to establishing the successful design approach. The design accounted for repeatability across multiple sites to enable the client to apply portfolio wide in future

Key outcomes

- Through detailed **device testing** at a granular level, we were able to effectively assess the suitability of systems and devices in a simulated financial services environment.
- **A holistic approach** reinforcing cyber security requirements, developed with the client, ensured technology deployment was delivered in alignment with rigorous global corporate technology standards.

CASE STUDY - FRANKSTON HOSPITAL REDEVELOPMENT

MELBOURNE, AUSTRALIA | CLIENT: BAYSIDE HEALTH

Opened in 2026, Peninsula University Hospital, formerly known as Frankston Hospital is a landmark health infrastructure project delivering a new 12-storey clinical services tower and car park. Our team provided end-to-end technology services that ensured all digital systems met the client's brief and worked together seamlessly. We delivered multiple specialist disciplines, including Information and Communications Technology (ICT), electronic security, Audio Visual (AV) and nurse call/clinical communications.

As the lead MSI, we established the strategy for how all building systems and clinical technologies would connect and operate as a unified whole. This meant verifying that the new ICT, nurse call and security systems not only met performance requirements individually but also interoperated correctly with each other and with existing hospital systems.

Key outcomes

- Ensured that critical systems, from bedside nurse call alerts to security cameras, were delivered in an **integrated manner**, on time and in line with the hospital's strict operational requirements.
- Delivered **robust, Future Ready® digital infrastructure** for the hospital, achieved through our multidisciplinary technology consulting and diligent systems integration oversight.

\$1.1bn

AUD investment (total project value)

35,000

more patient episodes can be treated every year

130

more inpatient beds



To derisk the complex technology deployment, the project implemented an onsite prototype technology test lab (a full mock-up of the hospital's ICT network and critical systems) well before final installation. In the technology test lab environment, we worked with the project team to assemble the actual hardware and software for key systems (network switches, servers, nurse call controllers, security panels, etc.) in a controlled setting that mirrored the design. This forward-looking strategy gave the client confidence that when the new hospital wings opened, all the digital systems (from bedside call buttons to security cameras) would function harmoniously from day one, with no operational hiccups.



Manoj Indraharan
Director
Technology Systems

Delivered by: The Victorian Health Building Authority in partnership with Bayside Health Peninsula and the Exemplar Health consortium, comprising Lendlease, Honeywell, Compass Group and Capella Capital.

CASE STUDY - FRANKSTON HOSPITAL REDEVELOPMENT

PENINSULA UNIVERSITY HOSPITAL

What we learned

Prototype technology test labs enable early integration certainty

Establishing an on site technology test lab allowed complex clinical, ICT and security systems to be integrated and effectively pre-commissioned before site installation, significantly reducing late-stage integration risk.

Testing-based procurement reduces vendor and compatibility risk

Real-world testing of emerging and legacy technologies in the lab environment informed confident vendor selection decisions, avoiding deployment of unproven or incompatible solutions.

Early validation accelerates delivery and commissioning

Identifying and resolving interoperability issues early shortened on site commissioning, reduced programme risk and ensured all systems functioned seamlessly from day one.



CASE STUDY - DUNEDIN HOSPITAL REDEVELOPMENT

OTAGO, NEW ZEALAND |
CLIENT: TE WHATU ORA – HEALTH NEW ZEALAND

The New Dunedin Hospital is a landmark healthcare project in New Zealand – the nation's largest-ever health infrastructure investment to date. This redevelopment will replace the aging Dunedin Hospital with a state-of-the-art, fit-for-purpose facility designed to serve Otago and Southland for decades to come.

The redevelopment is expected to dramatically improve healthcare delivery for the region – offering modern medical technology, expanded capacity and enhanced patient experiences. Overall, the New Dunedin Hospital will usher in a new era of healthcare for the community, replacing outdated facilities with a future-proofed, digitally-enabled hospital that can adapt to evolving clinical needs and population growth.

We provided end-to-end technology consulting and design services covering a range of specialist disciplines, including ICT and communications infrastructure, hospital electronic security systems, audio-visual systems, clinical/nurse call communications and related digital health technologies.

Key outcomes

- Project team **simulated and trialed** the integration of systems early, before actual installation in the new hospital buildings.
- On site prototype test lab helped **derisk integration**, validate system performance and guide smarter procurement.

10,000m²

approximately of clinics and day surgery facilities

\$100m

NZD estimated annually injected into the local economy during peak build phase



Following our successful approach on similar hospital projects, we established a dedicated mini-network and systems lab at the project site during the design/testing phase. In this lab environment, key elements of the hospital's ICT network and various subsystems were set up and connected exactly as they would be in the real hospital but on a small scale and in a controlled setting.



Manoje Indracharan
Director
Technology Systems

CASE STUDY - DUNEDIN HOSPITAL REDEVELOPMENT



The prototype and staging lab became one of the most important safeguards for the overall project's success. It gave us a controlled environment where clinical, engineering and facility, digital and operational systems could be built, integrated, tested and validated exactly as they would function in the hospital, but without the risks of touching a live environment. By reproducing the full end-to-end workflows, network conditions, user interfaces, security controls and device behaviours, the lab allowed us to uncover issues early, validate design intent and refine configurations long before deployment.



Roneel Singh
Director
Technology Systems

DUNEDIN HOSPITAL

What we learned

Master Systems Integration (MSI) provides technology governance at scale

Appointing a lead MSI created a single point of accountability for how clinical, ICT and building systems connect, reducing coordination risk across multiple vendors and disciplines.

Prototype environments expose critical issues while there is still time to act

The on site technology test lab identified integration and firmware issues (including RTLS performance risks) early enough to influence system design, vendor selection and mitigation strategies.

Rehearsed testing and commissioning lowers delivery risk

Using the technology test lab to develop and validate test scripts, acceptance criteria and commissioning processes reduced the risk of delays, rework and operational disruption during live deployment.

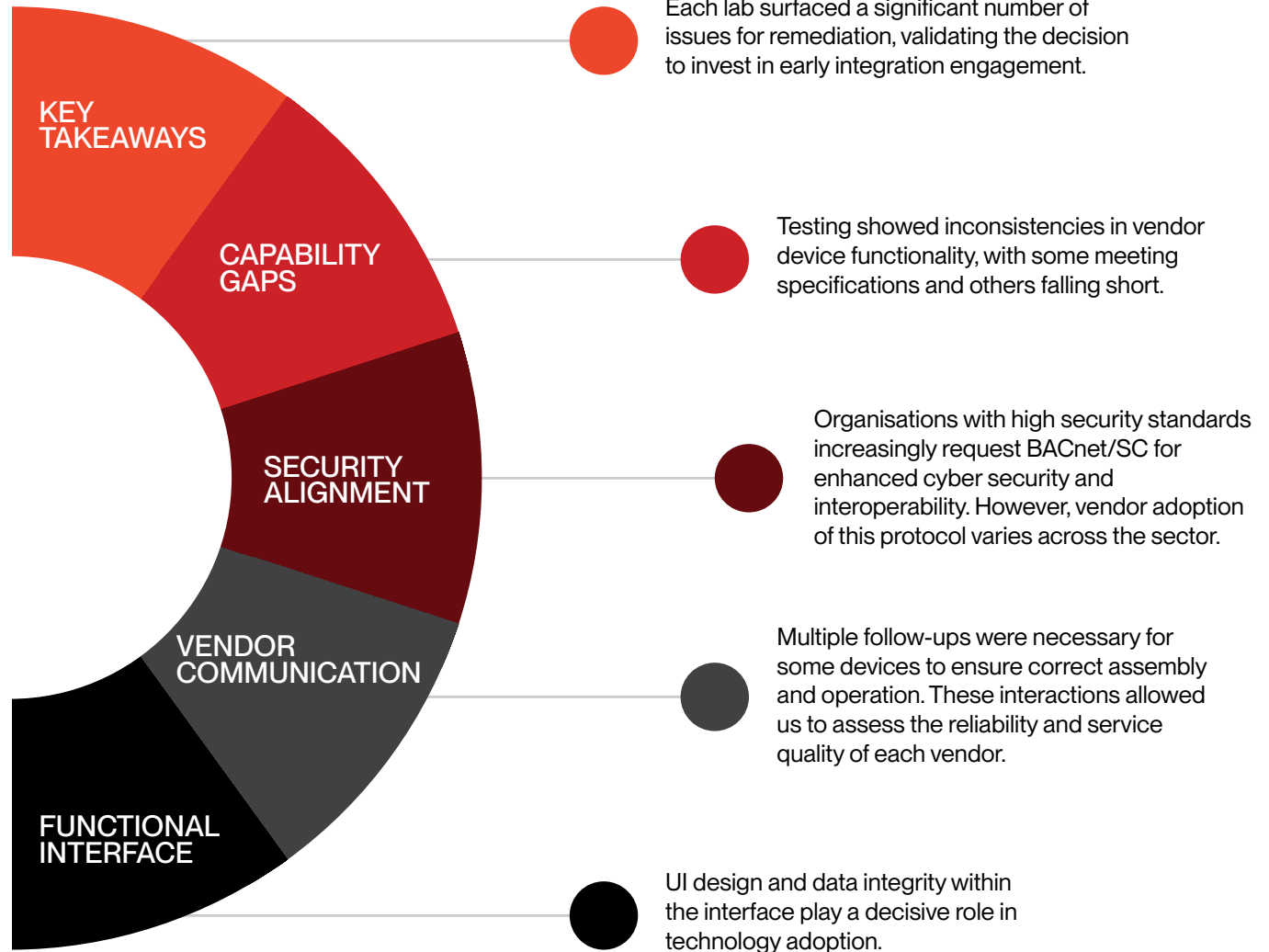
EARLY ACTION. LASTING IMPACT.

This approach is a significant step forward in derisking technology delivery by bringing all proposed sensors and major technology components together in a technology test lab to be deployed, integrated and tested much earlier in the construction programme than is usually done.

It allows client teams to test the customer support of vendors under consideration as well as the data that is output from sensors.

The advance testing makes it possible to test multiple vendors for each proposed device and incorporate findings before taking procurement decisions. This offers significant value to clients by allowing cyber security and IT stakeholders to validate requirements are met.

This early technology test lab approach fundamentally strengthens project certainty by transforming assumptions into evidence long before systems reach site. It enables the project team to uncover integration challenges, interoperability constraints and performance limitations at a stage when they are inexpensive and simple to resolve.



GLOBAL BUILDING TECHNOLOGY COMMUNITY

WSP is one of the world's leading professional services firms, uniting its engineering, advisory and science-based expertise to shape communities to advance humanity.

From local beginnings to a globe-spanning presence today, WSP operates in over 50 countries and employs approximately 83,000 professionals, known as Visioneers. Together they pioneer solutions and deliver innovative projects in the transportation, infrastructure, environment, building, energy, water, and mining and metals sectors.

WSP is publicly listed on the Toronto Stock Exchange (TSX:WSP).



UNITED STATES



Jay Wratten
Senior Vice President
Jay.Wratten@wsp.com

MIDDLE EAST



Iftikhar Zubair
Director, Building Technology Systems
Iftikhar.Zubair@wsp.com

UNITED KINGDOM



Mark Ince
Director, Building Technology Systems
Mark.Ince@wsp.com



Nico Lomas
Associate, Building Technology Systems
Nico.lomas@wsp.com

CHINA REGION



Alex Y Y Cheung
Director, Smart Solutions
& Advanced Engineering
Alex.YY.Cheung@wsp.com

AUSTRALIA



Manoj Indrahara
Director, Technology Systems
Manoj.Indrahara@wsp.com



Disclaimer

The Corporation has obtained industry data, market data and other statistical information presented in this report from a variety of third party publications and reports. Although the Corporation believes that these publications and reports are reliable as of the date of this report, such information and statistical data should not be construed as having been reviewed, verified or endorsed by the Corporation, and the Corporation makes no representation or warranty as to the accuracy or completeness thereof. The Corporation has not independently verified the information or other statistical data contained therein, nor the underlying economic or other assumptions relied upon by these sources. The Corporation has no intention and undertakes no obligation to update or revise any such information or data as a result of new information, future events or otherwise.

This report is a work protected by copyright and constitutes the intellectual property of WSP, subject to third party rights. Subject to applicable laws, excerpts from this report may be quoted, reproduced or transmitted for informational or non commercial purposes, provided that the source is clearly identified and that WSP is acknowledged as the author. Any full reproduction or use for other purposes is prohibited without the pr obtaining of required authorisations.

For additional queries, please contact:

Mark Ince +44-7920-250-630

Mark.Ince@wsp.com

