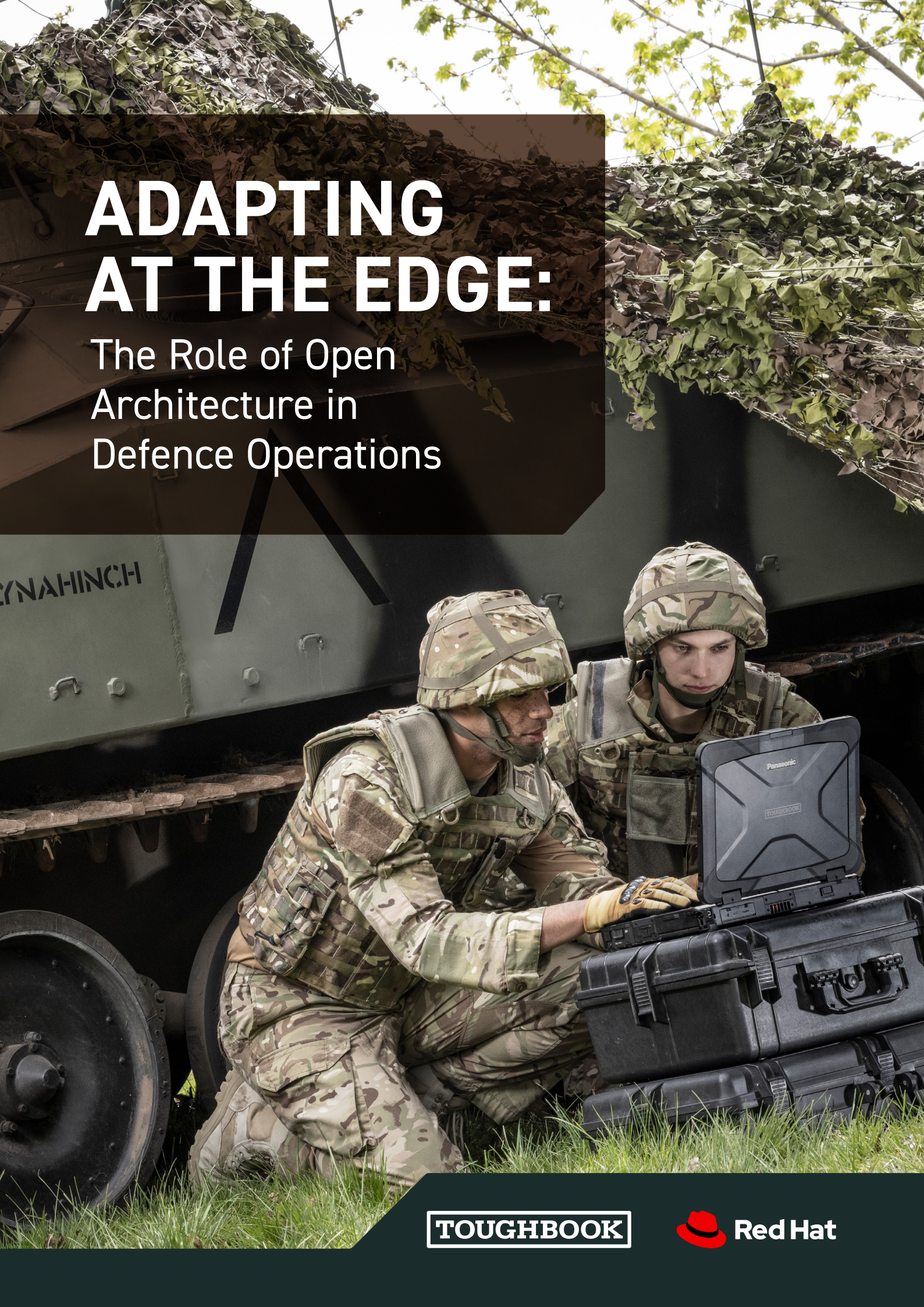

ADAPTING AT THE EDGE:

The Role of Open Architecture in Defence Operations

TOUGHBOOK

Red Hat

FOREWORD

As the UK MOD continues to modernise and evolve its digital infrastructure, the importance of secure, modular, and open systems has never been clearer. Our partners across the defence ecosystem, particularly system integrators, play a critical role in delivering solutions that align with this vision.

At TOUGHBOOK, we understand the pressures our defence partners face. From the need for rapid deployment to supporting secure environments at the edge, our focus is on helping integrators build confidently with platforms that are tested, flexible, and certified where it matters most.

This whitepaper brings together key considerations and practical guidance for those navigating MOD priorities around open architecture and interoperability. I hope it provides a useful reference as you plan, design, and deliver the next generation of defence capability.

Charlotte Langridge
UK Defence Lead, Panasonic TOUGHBOOK

ADAPTING AT THE EDGE:
THE ROLE OF OPEN ARCHITECTURE IN DEFENCE OPERATIONS

EXECUTIVE SUMMARY

Defence operations demand more than military grade solutions. They require systems that can evolve, integrate, and perform at the tactical edge without compromise. At the same time, the UK Ministry of Defence has set clear digital priorities: adopt open standards, enable modularity, and build systems that are secure by design and ready for future needs.

This whitepaper explores how system integrators can align with those priorities using open architectures and flexible hardware platforms. It looks at how the right building blocks, including certified Linux environments like Red Hat Enterprise Linux, support interoperability, resilience, and operational agility in complex defence settings.

By focusing on design principles that support adaptability and integration, system integrators can deliver solutions that are faster to deploy, easier to evolve, and better aligned with MOD expectations.

THE STRATEGIC IMPERATIVE – MOD'S EVOLVING DIGITAL PRIORITIES

The MOD's future-facing digital strategy creates new expectations for system integrators.

The Ministry of Defence is clear in its direction for the future of defence IT. Flexibility, security, and speed of integration are no longer optional. Open standards, modular architecture, and cyber resilience are now foundational expectations across programmes and platforms.

System integrators working with the MOD are increasingly expected to deliver solutions that can adapt to changing needs. This means avoiding vendor lock-in, supporting interoperability across new and legacy systems, and designing with long-term lifecycle value in mind.

MOD strategy documents frequently highlight the importance of:

- **Open architecture** to allow faster integration and better control
- **Secure-by-design systems** to reduce risk and protect classified environments
- **Modular technology** that can evolve without complete replacement
- **Interoperability across devices**, platforms, and command centres
- **Cost-effective lifecycle management** that balances innovation with reliability

For integrators, this presents both a challenge and an opportunity. The ability to assemble flexible, standards-based solutions is now a key differentiator. It is also a requirement for long-term success in the defence space.

These priorities define the strategic direction. But how do they translate into action for system integrators? That begins with architecture.

> **Key platforms will serve for decades, so we will focus on open physical, electronic and digital architectures, on commonality and modularity, and on working with industry to integrate iterative upgrades through-life.**

UK Ministry of Defence, Land Industrial Strategy, page 6
Source: https://assets.publishing.service.gov.uk/media/6284ad0ae90e071f67b27fc0/Land_Industrial_Strategy.pdf

OPEN ARCHITECTURE IN ACTION – FROM DATA CENTRE TO EDGE

Open standards are already delivering real benefits in modular, scalable defence systems.

Open architecture is more than a technical preference. It is a strategic approach that allows defence organisations to build systems that are adaptable, scalable, and resilient across a range of operating environments.

For system integrators, this flexibility is essential. Defence deployments rarely follow a one-size-fits-all model. They range from secure data centres to mobile command units and disconnected edge scenarios. Integrators must be able to mix and match components, integrate with existing infrastructure, and meet specific mission requirements without compromising security or control.

Open standards enable this by removing many of the barriers created by proprietary systems. They make it easier to incorporate new capabilities, extend system lifespans, and deliver consistent performance across multiple platforms.

Open standards give integrators the flexibility to respond fast and integrate with confidence.

A proven example of this in action is the widespread adoption of Linux, particularly Red Hat Enterprise Linux, in secure defence environments. Red Hat's focus on security, long-term support, containerisation and seamless integrations with defence systems makes it a trusted choice for mission-critical workloads.

When combined with modular, open-compatible hardware, these environments give integrators the foundation they need to meet MOD expectations while maintaining control over how systems evolve over time.

EDGE-READY HARDWARE – TURNING OPEN PRINCIPLES INTO OPERATIONAL ADVANTAGE

The right hardware extends open architecture benefits to the tactical edge.

Operating at the tactical edge presents unique challenges. Devices must be rugged enough to survive harsh conditions, secure enough for classified environments, and flexible enough to adapt to different roles and missions. For system integrators, this adds another layer of complexity when selecting or recommending hardware platforms.

Modularity is key. Hardware that can be easily configured, upgraded, or repaired in the field reduces downtime and extends usability. It also allows integrators to tailor solutions to specific needs without starting from scratch for each deployment.

Equally important is compatibility with secure, open-source platforms like Red Hat Enterprise Linux. Choosing hardware that is officially certified for use with RHEL reduces compatibility risks and helps ensure long-term support and security compliance. For defence projects, where both uptime and cyber resilience are critical, this kind of assurance matters.

When open software runs on modular, certified hardware, this creates a platform purpose-built for operational flexibility, secure integration, and long-term performance.

To help clarify the difference, here is a comparison of Red Hat-certified versus non-certified hardware platforms:

Feature / Benefit	Red Hat-Certified Hardware	Non-Certified Hardware
Official validation by Red Hat	✔	✖
First line service support from Red Hat	✔	✖
Full support with new RHEL releases	✔	⚠ Risk of breakage or unsupported bugs
Lifecycle patching and security compliance	✔	⚠ Require manual testing and fixing

Red Hat certification is more than a badge. It assures system integrators that the hardware has been tested and approved for use with RHEL, reducing risks during deployment and support. This can be especially critical in defence environments where security compliance, uptime, and rapid deployment all matter. It becomes easier for system integrators to deliver solutions that align with MOD priorities and still meet the fast-paced demands of real-world operations.

FUTUREPROOFING DEFENCE IT – PRACTICAL STEPS FORWARD

Futureproofing requires smart, standards-driven choices today.

As MOD programmes evolve, the pressure on system integrators to deliver secure, modular, and interoperable solutions will only increase. Futureproofing is no longer about locking in a single platform or vendor. It is about choosing components that can grow, adapt, and integrate within a changing digital ecosystem.

For integrators supporting defence IT projects, a few key principles stand out:

- **Evaluate open standards** to maintain flexibility across evolving requirements
- **Select Red Hat-certified hardware** to reduce compatibility risks and simplify integration
- **Design for modularity** so individual components can be swapped or upgraded as needed
- **Build with lifecycle in mind**, considering support, security, and maintainability
- **Ensure edge-readiness** to support mission-critical applications in disconnected environments

These principles allow integrators to create value beyond initial delivery. By recommending systems that are easier to adapt, support, and secure, they become long-term partners in the MOD's digital transformation.

Whether deploying rugged edge platforms, securing infrastructure, or integrating new capabilities, the choices made today will determine how well defence systems perform tomorrow. With the right building blocks, system integrators can lead with confidence.

Your next project does not just need to be robust. It needs to be ready to adapt.

CONCLUSION

Open architecture is no longer a future goal. It is already shaping how defence projects are specified, procured, and delivered. For system integrators, aligning with this direction means more than just meeting technical requirements. It is about delivering solutions that are modular, secure, and ready for rapid integration.

By combining open-source platforms like Red Hat Enterprise Linux with certified, modular hardware, including platforms such as Panasonic TOUGHBOOK, integrators can help defence customers stay ahead of change while meeting the MOD's goals for resilience, interoperability, and long-term value.

EXPLORE RED HAT-CERTIFIED EDGE DEVICE OPTIONS

Start building your next MOD-ready solution with platforms that support open standards and secure integration.

Start

TOUGHBOOK

Red Hat