hildebrand



CHERI

Market Benefits of CHERI-Enabled Devices in the Energy Sector

2026 Position Paper

by Hildebrand Technology Limited

Executive Summary

Memory safety vulnerabilities are the single largest class of exploitable software defect, accounting for approximately 70% of all common vulnerabilities and exposures (CVEs) assigned by Microsoft and Google and up to 75% of zero-day exploits tracked by Google Project Zero. The consequences of a memory-safety-related breach extend far beyond immediate remediation cost for the energy sector which operates critical national infrastructure and deploys connected metering devices at scale. Risks include regulatory fines, reputational harm, risk of device recalls and the potential for disruption to grid operations.

CHERI (Capability Hardware Enhanced RISC Instructions) and its embedded variant CHERIoT represent a fundamentally different approach: rather than patching software after the fact, CHERI eliminates entire classes of memory-safety vulnerability at the hardware level. Spatial and temporal memory safety, pointer integrity, and fine-grained compartmentalisation are properties of the silicon itself, not of any individual software component.

This paper sets out the commercial and regulatory case for CHERI-enabled devices in the GB energy market. It demonstrates that CHERI is not merely a security improvement; it is driven by converging regulatory pressure from the EU Cyber Resilience Act (CRA), the UK Product Security and Telecommunications Infrastructure (PSTI) Act, and the Network and Information Systems (NIS2) in conjunction with the operational economics of running connected device fleets over decade-long deployment horizons.

The cost of not adopting CHERI expressed through breach liability, compliance overhead, firmware update logistics, and constrained product architectures is increasingly more significant than the cost adopting it. After 15 years of development CHERI production silicon is available today, enabling energy sector device manufacturers to build hardware-enforced memory safety into their products. The next step is to demonstrate that certified, commercially viable products can be built on this foundation, showing that CHERI-secured devices can achieve cybersecurity certifications such as CPA more quickly and at lower cost than conventional alternatives.

As part of the CHERI Adoption programme, Hildebrand will deliver two fully certified metering products: the cSAPC, a certified smart metering device and the cCOP11 a compliant asset meter enabling participation in the GB flexibility market as well as the CHERI Pi, a microcontroller development board. All will be built on SCI Semiconductor's ICENI silicon. This will be the first range of products commercially available that are UK-made, CHERI-secured and ready for deployment.



What is CHERI?

Memory safety and more

Modern computing systems are predominantly written in C and C++ — languages that offer direct memory access, pointer arithmetic and high performance, but they provide no automatic protection against memory errors. The risk of a memory error is that when a programme reads or writes outside the bounds of an allocated buffer, or accesses memory that has already been freed, the result can range from a 'silent crash' to a fully exploitable attack chain.

Memory safety vulnerabilities have been the dominant class of exploitable defect for over thirty years. The Morris Worm of 1988 — the first major internet incident — exploited a buffer overflow. Heartbleed in 2014, a memory bounds error in OpenSSL, cost an estimated US$ 500 million to remediate across the global internet infrastructure. Decades of investment in static analysis tools, fuzzing, sandboxing, Address Space Layout Randomisation (ASLR), and memory-safe language rewrites have all failed to eliminate the problem. They mitigate: they do not cure.

The reason is structural: software mitigations are incomplete by design. ASLR makes exploitation probabilistically harder, but not impossible. Fuzzing finds some bugs but cannot enumerate all possible inputs. Memory-safe languages address new code but leave legacy codebases untouched. Critically, IoT and embedded devices often cannot run the heavyweight runtime overhead that these mitigations demand.

15 years of **R&D**

CHERI is a processor architecture extension developed over 15 years at the University of Cambridge and SRI International. Major investors include the UK government's Digital Security by Design (DSbD) programme, US Defense Advance Research Projects Agency (DARPA), and industrial partners including Microsoft and Google. It embeds security by design an aims to significantly strengthen system security through the use of memory safe pointer architecture and secure compartmentalisation of memory. Rather than adding software checks after compilation, CHERI augments every processor pointer with a capability: a hardware-enforced descriptor that encodes the memory address, the valid bounds, and the permissions (read, write, execute) that apply to that pointer.

The hardware enforces these capabilities on every memory access, every cycle, without exception. A programme — even one written in standard C — cannot read beyond the bounds it was granted, cannot forge a pointer it was not given, and cannot use a capability that has been revoked. These properties are architectural: they apply regardless of compiler settings, software configuration, or attacker sophistication.

UNIVERSITY OF CAMBRIDGE

UK Research and Innovation

National Cyber Security Centre

September 2026

CHERI Properties

CHERI introduces hardware-enforced memory protection that addresses the root causes of many software vulnerabilities without changes to the application design.

01

Spatial memory safety

Spatial memory safety ensures that software can only access memory within the valid bounds of an allocated object. Every CHERI capability carries hardware-enforced bounds that prevent reads or writes beyond the permitted memory region. Attempts to exceed these limits generate an immediate hardware exception, preventing exploitation. This directly mitigates common vulnerabilities including buffer overflows, stack overflows and out-of-bounds accesses, addressing weaknesses such as CWE-787 (Out-of-bounds Write) and CWE-125 (Out-of-bounds Read).

02

Temporal memory safety

Temporal memory safety prevents software from accessing memory after it has been released or reallocated. These use-after-free (CWE-416) vulnerabilities are frequently exploited to execute malicious code or corrupt application state. CHERI capabilities retain provenance information that enables supporting runtime mechanisms to identify stale references and prevent invalid memory access. This significantly reduces the opportunity for attackers to exploit dangling pointers and improves overall software robustness.

03

Pointer integrity

Unlike conventional processors, CHERI represents pointers as protected capabilities rather than ordinary memory addresses. Each capability includes permissions, memory bounds and integrity information enforced directly by hardware. Capability tags cannot be forged or modified using normal instructions, preventing attackers from creating arbitrary pointers or redirecting software to unintended memory locations. This provides strong protection against pointer injection, pointer substitution and pointer forging attacks.

04

Compartmentalisation

CHERI enables fine-grained compartmentalisation by allowing software components to operate with only the capabilities required for their intended function. Hardware enforcement ensures each compartment remains isolated from others unless access is explicitly authorised. Should one component become compromised, the attack is contained within that compartment, preventing unauthorised access to neighbouring software or system resources. This substantially reduces lateral movement and limits the impact of successful exploitation.

Available in a chip

ICENI

World's first production silicon implementation

In March 2026, SCI Semiconductor achieved a significant milestone: the first production silicon implementation of CHERIoT. Their ICENI microcontroller runs the CHERIoT-Ibex RISC-V core at up to 250 MHz and brings capability-based security and strong memory safety to production embedded hardware for the first time. The first ICENI chips will be made available in September 2026.

CHERIoT

Embedded and IoT devices



CHERIoT is the embedded variant of CHERI, originally developed by Microsoft Research and now maintained as a cross-vendor open-source project with contributions from Microsoft, Google, SCI Semiconductor, lowRISC, and others. It is specifically designed for resource-constrained microcontrollers, the device class used in smart meters, industrial controllers, and other connected embedded systems

CHERIoT extends the core CHERI guarentees with:

Deterministic use-after-free protection: temporal memory safety at hardware level

Lightweight compartment model: isolated software components with hardware-enforced boundaries, within a single address space and without an MMU

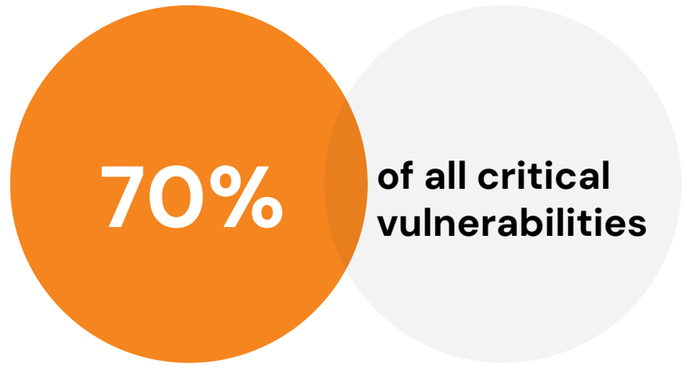
Auditable control over interrupt state: enabling safety-critical and real-time guarantees

Lexically-scoped object delegation: secure sharing of objects between compartments

CHERIoT RTOS: a clean-slate real-time operating system designed to exploit these features

Cost of Memory Safety Risks

Evidence base on memory safety is extensive, consistent, and alarming



Over the past two decades, memory-safety vulnerabilities—specifically spatial and temporal memory flaws—have consistently accounted for roughly 70% of all critical security defects across major open-source and proprietary software trusted computing bases spanning desktop operating systems like Windows and Linux, mobile systems like Android and iOS, web runtimes like Chromium and OpenJDK, and embedded platforms like VxWorks and FreeRTOS. Beyond being widespread, these vulnerabilities serve as the underlying engine for many zero-day exploits actively deployed in real-world attacks, and because they reside inside privileged components, they frequently persist in unpatched or unpatchable systems for years after initial disclosure.

The threat landscape has grown at a dramatic rate; the National Institute of Standards and Technology's (NIST) National Vulnerability Database (NVD) shows a five-fold increase in firmware attacks between 2017 and 2021 (Security Signals: Firmware Attacks on the Rise. Microsoft). The surge coincided with the large-scale deployment of connected IoT devices such as smart meters. The scale of the risk suggests that without structural shifts hardware security attack volumes will continue to trend upwards. Hardware-enforced memory safety offers a decisive defence response to the growing risks.

MITRE's 2025 CWE Top 25 Most Dangerous Software Weaknesses list includes several critical vulnerabilities that are directly and deterministically mitigated by CHERIoT, including:

- Out-of-bounds write (#5)
- Use-after-free (#7)
- Out-of-bounds read (#8)
- Classic buffer overflow (#11)
- Null pointer dereference (#13)

The estimated financial impact of security failures underscores the urgency of addressing root-cause vulnerabilities like memory safety. IBM's Cost of a Data Breach Report 2026 states that the global average breach cost was $4.99M million in 2026, an increase of 12% over the previous year; it highlights that "Frontier AI models have radically

shifted the cybersecurity threat landscape". Generative AI has lowered the time, cost and expertise needed to launch attacks, pushing organisations towards continuous business disruption. Nationally the UK average cost of a significant cyber-attack on a business is estimated at £195,000 which scales to a potential annual UK-wide cost of £14.7 billion. These figures paint a consistent picture: cyber-attack risk is pervasive, economically material, and growing rapidly with the advent of AI (AI driven attacks increased by 56% over the last year alone).

Why the energy sector is particularly exposed

The GB's smart metering programme has currently deployed over 38 million SMETS devices. Rollout continues with the goal of comprehensive national coverage from the current 66% of homes. Devices are connected to the Data Communications Company (DCC) network via Wide Area Network (WAN) links, and to Home Area Networks (HAN) serving in-home displays, electric vehicle chargers, and other consumer devices. Smart meters are just one component of a far broader embedded firmware estate that underpins the UK's energy infrastructure.

Across the energy sector critical functions are controlled by embedded devices running firmware written predominantly in C or C++:

- Power distribution management systems issue commands to circuit breakers and grid equipment
- Building Management Systems (BMS) control HVAC, access, and power across commercial and industrial facilities
- Safety Instrumented Systems (SIS) provide last-resort protection at generation and processing sites
- SCADA Human-Machine Interfaces (HMIs) provide operator control of grid and industrial scale assets
- District heating and substation controllers manage thermal and electrical distribution networks.

Each of these functions have been successfully exploited in real-world attacks through memory safety vulnerabilities in embedded firmware.

This exposure is structural, not incidental. Energy sector devices share characteristics that make them particularly difficult to protect through conventional means:

1. Long operational lifetimes: meters are expected to operate for 10–15 years. The threat landscape in 2036 will be materially different from that of 2026. A device deployed today must be secure across its whole life, not merely at installation.
2. Critical infrastructure: smart metering is classified as Critical National Infrastructure (CNI). Compromise at scale could enable billing fraud, energy theft, demand manipulation, or, in extreme scenarios, targeted disruption of grid stability through coordinated device behaviour.
3. Legacy C codebases: embedded metering firmware is predominantly written in C, for efficiency and hardware compatibility. C provides no memory safety guarantees. Even high-quality C code, rigorously tested and statically analysed, can contain exploitable memory safety bugs.
4. Scale and heterogeneity: the sector operates millions of devices from hundreds of manufacturers, spanning decades of firmware generations, communicating over diverse protocols including Modbus, DLMS/COSEM, IEC 61968, and proprietary WAN stacks. A single exploitable vulnerability in a widely-deployed component can represent a systemic risk across the entire infrastructure.

The attack surface therefore extends well beyond the meter itself, it includes:

- Meter Asset Managers that maintain large device fleets
- Energy suppliers handle billing systems
- BMS operators manage building infrastructure
- The DCC operates the communications backbone

All are exposed to cascading risk if an exploitable memory vulnerability exists anywhere in the firmware supply chain.

Consumer landscape

As of late 2025, Great Britain has rolled out smart meters to approximately 70% of all homes or approximately 38 million smart electricity and gas meters. This enables over 20 million homes for Time of Use (ToU) tariffs, export and flexibility revenue for their electricity.

The smart metering infrastructure is defined in GB Smart Metering Equipment Technical Standards (SMETS) with an architecture that includes a Zigbee Smart Energy Profile (SEP) home area network (HAN). The HAN connects all of the SMETS defined assets via wireless technology so that they can communicate with each other locally and through back through a wide area network (WAN) to energy suppliers and other parties.

The communications hub is supplied by the Data Communications Company (DCC) with rental and bandwidth charges paid by the energy supplier. Meters are procured by an installing supplier and are owned by meter asset providers (MAPs) who finance meter assets and in turn lease back to energy suppliers.

Communications hubs and meters are accessed through the private network and security keys run by the DCC. When a supplier gains a new customer, their access key is installed on the meter while the losing supplier's key is removed. This means that meters can stay on the wall when consumers switch suppliers.

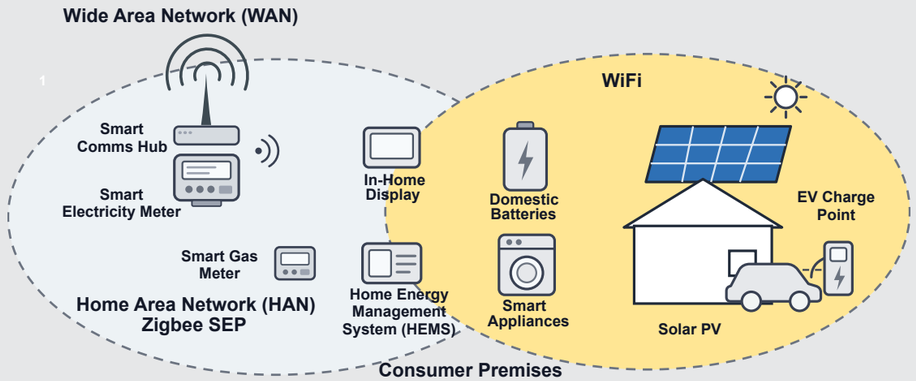


Figure 1. Smart metering and home energy management system architecture in Great Britain.

There are a few consumer installable technologies on the HAN, an In Home Display and a class of devices called the consumer access device (CAD). These devices can read data from the metering in real-time and CAD functionality is built in to Hildebrand's home energy management system (HEMS). Notably these devices also sit on Wifi.

Low carbon technology adoption has been growing in households across Britain due to environmental and financial incentives. Most smart technologies are Wifi connected and typically managed by a mobile app provided by the vendor of the low carbon technology. For instance an electric vehicle may have an app with the ability to set charging times and user preferences or a smart charge point that can be programmed to take advantage of low cost electricity.

As homes adopt more technology there is a growing need for home energy management systems that will orchestrate the energy producing, consuming and storing technologies. Dynamic prices and In home as well as grid constraints need to be considered when optimising.

Software insufficient

Software industry has responded to memory safety risk with a suite of software and compiler-level mitigations, such as:

Address Space Layout Randomisation (ASLR)

Makes exploiting memory bugs probabilistically harder by randomising memory layouts but does not prevent exploitation. Furthermore, constrained embedded environments often cannot implement it fully.

Stack Canaries

Detect some stack overflow attacks, but not heap corruption or use-after-free

Static analysis and fuzzing

Find some bugs before deployment but cannot enumerate the full attack surface; generate high false-positive rates leading to alert fatigue; cannot provide completeness guarantees.

Memory-safe language rewrites

Rust and similar languages prevent memory safety errors in newly written code, but cannot address existing C/C++ codebases; require full developer upskilling and toolchain changes; and, for embedded devices, often incur unacceptable code size and runtime overhead.

Both software-only methods and hardware assisted methods of vulnerability mitigation involve a reduction in performance and/or an increase in resource usage. The programs need to include additional instructions to guard against improper memory access, which slows down the execution, and shadow stacks, shadow memory and similar objects occupy memory space. Some techniques create such a large performance penalty that they are only usable as debugging tools, not to be included in release versions of software2.

More importantly, these mitigations reduce risk. They do not eliminate it. The attacker's advantage remains: developers must find and fix every vulnerability; an attacker needs only one. CHERI rebalances this asymmetry by removing entire classes of vulnerability at source, rather than attempting to detect or contain their exploitation.

CHERI's architectural response

Tackling the root cause

CHERI addresses the root cause rather than the symptom. Its hardware enforcement operates at every memory access, regardless of software quality, compiler configuration, or attacker capability. The properties it provides cannot be bypassed by software alone.

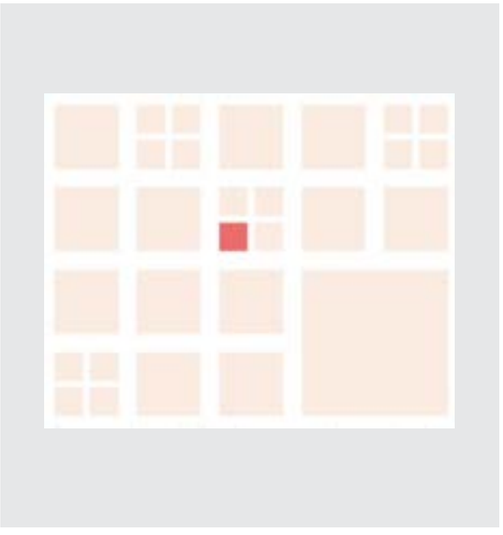
At the hardware level, CHERI extends the processor's instruction-set architecture so that conventional memory pointers can be represented as capabilities. A capability contains not only the address of an object in memory, but also metadata defining the memory region that may be accessed and the permissions associated with that access. The processor maintains an additional validity tag that distinguishes legitimate capabilities from ordinary data, preventing software from simply constructing or forging a privileged pointer. Whenever a capability is used to load, store or execute memory, the processor checks its validity, bounds and permissions as part of the memory operation. An attempted access outside the permitted region, or an operation for which the capability does not have permission, therefore fails at the point of use rather than relying on application code to detect the violation.

Real security

For the energy sector specifically, CHERI's value proposition translates to:

- Elimination of buffer overflows and out-of-bounds access: the most common firmware attack vectors as a category, not as individual bugs to be patched
- Deterministic use-after-free protection: removes an entire class of attacks that has driven high-profile exploits across operating systems, browsers, and embedded platforms
- Hardware-enforced compartmentalisation: limits the blast radius of any residual vulnerability to the affected component, preventing lateral movement across a device

The financial and operational implications of this architecture shift are explored in the following sections.



CHERI's compartmentalisation prevents contagion

Compliance: a market driver

Security-by-design is legally mandatory

Three overlapping regulatory frameworks are creating a compliance imperative for connected device manufacturers in the GB and EU energy sector. The combined effect is that security-by-design is becoming legally mandatory, with significant penalties for non-compliance and product liability exposure for manufacturers who ship devices with known exploitable classes of vulnerability. Each of the frameworks is described below.

EU Cyber Resilience Act (CRA): Regulation (EU) 2024/2847

The Cyber Resilience Act came into force on 10 December 2024; it represents the most comprehensive mandatory cybersecurity framework for connected devices ever enacted. The CRA applies to all "products with digital elements" placed on the EU market including connected hardware and any software integral to their operation. It applies to manufacturers, importers, and distributors regardless of organisation size or country of origin.

Non-compliant products cannot be sold in the EU from December 2027. Market surveillance authorities may impose fines; for the most serious violations, penalties can reach €15 million or 2.5% of global annual turnover, whichever is greater.

Key obligations:

- Products must be designed and developed to be secure by default and secure by design
- Manufacturers must implement security throughout the product lifecycle, including during planning, design, development, and maintenance phases
- Vulnerability handling and disclosure processes must be established and maintained for the expected product life
- Security updates must be provided and made available for a defined support period
- Products must bear the CE marking to confirm compliance
- Incident reporting obligations apply from 11 September 2026
- Full compliance required from 11 December 2027

UK Product Security and Telecommunications Infrastructure (PSTI) Act 2022

The PSTI Act came into full effect in April 2024, placing mandatory security obligations on manufacturers of consumer connectable products sold in the UK. Compliance with PSTI is enforced by the OPSS (Office for Product Safety and Standards). Non-compliant products may be removed from the UK market and financial penalties may be imposed.

Key obligations:

- No default passwords: all devices must have unique device-level credentials or require the user to set a password at initialisation
- Vulnerability disclosure policy: manufacturers must publish and maintain a clear process for receiving and responding to reported vulnerabilities
- Transparency on security update periods: consumers and buyers must be informed of the minimum period for which security updates will be provided
- Minimum security period: manufacturers must commit to providing security updates for a defined periodNIS2 Directive and energy sector obligations

NIS2 Directive and energy sector obligations

The revised Network and Information Systems Directive (NIS2) is transposed into UK law through the Network and Information Systems (Amendment) Regulations and is under active update through the UK Government's Cyber Security and Resilience Bill. NIS2 establishes heightened security requirements for operators in essential sectors like energy.

Key obligations:

- Risk management measures: organisations must implement appropriate technical and organisational measures to manage cybersecurity risks, such as policies on information systems security, supply chain security, encryption, and access control
- Supply chain security: entities must assess and manage the cybersecurity risks arising from their suppliers and service providers, including as security properties of hardware and software components they procure
- Incident reporting: significant incidents must be reported to the relevant national authority within strict timeframes: an early warning within 24 hours, a full incident notification within 72 hours, and a comprehensive final report within one month. Failure to report carries substantial penalties.

NCSC Secure by Design

The NCSC's Secure by Design principles, and DCMS's associated guidance, call explicitly for security to be built into products architecturally, rather than added retrospectively. CHERI is referenced by CISA (the US equivalent of NCSC) as a "promising memory safety mitigation in hardware" and an "important part of an overall strategy to eliminate memory safety vulnerabilities." While not a legal requirement, the Secure by Design approach is mandatory across all UK government departments to protect 'crown data and services'.

How CHERI secured products deliver compliance

Hardware-enforced security properties are increasingly significant in cybersecurity certification and conformity assessment, they provide architectural evidence that is verifiable, persistent, and not contingent on the absence of unknown bugs

or the maintenance of software mitigations. CHERI directly embodies this advantage. Its capability-based memory safety does not degrade over time and does not depend on patch cadence, making it materially easier to discharge the obligations imposed by the CRA, PSTI Act, NIS2 and the NCSC guidance. For example, the CRA requires demonstrable security controls across the entire product lifecycle, a bar that software mitigations alone struggle to meet; devices with hardware-enforced memory safety and compartmentalisation are substantially better placed for conformity assessment, particularly for products classified as "important" or "critical" where third-party assessment by a Notified Body is required.

The CHERIoT platform delivers conformity assessment through CHERIoT-Audit which enables manufacturers to generate auditable records of firmware compartmentalisation properties thus directly addressing CRA documentation obligations. Under the PSTI Act the same architectural properties simplify ongoing compliance; fewer emergency patches are needed, easing update transparency obligations, and the compartmentalisation model limits the blast radius of any remaining vulnerabilities therefore reducing the likelihood that an issue reaches the threshold requiring mandatory disclosure.

"Regulations such as EU product liability directives are easier to comply with when most of the reused code can be removed from the end product's attack surface."

SCI Semiconductor

CHERI compliance advantage

The compliance advantages translate into commercial advantages. Software-only compliance is not free; it imposes ongoing costs that CHERI-enabled devices substantially reduce:`

Compliance activity	Software-only approach	CHERI-enabled approach
Vulnerability management	Continuous patching across full codebase	Entire classes eliminated architecturally; residual surface smaller
Conformity assessment	Extensive documentation of controls for each component	Hardware-enforced properties are verifiable and persistent
Penetration testing	Must test full attack surface including memory-safety vectors	Memory-safety attack surface eliminated from scope
Incident response	Full forensic investigation required for each memory safety exploit	Class of exploit cannot succeed; incident risk reduced
Update lifecycle management	Frequent patch cycles required; see Section 4	Fewer patches; longer maintenance intervals feasible

These advantages extend specifically to CPA (Commercial Product Assurance), the NCSC's assurance scheme for security products procured into UK government and critical national infrastructure. CPA evaluation requires security laboratories to characterise and test the full exploitable attack surface of a device; in conventional embedded systems, memory-safety vulnerability classes account for a substantial portion of that surface and demand extensive adversarial test coverage that must be revisited following each significant firmware update. By architecturally eliminating these classes, CHERI reduces both the initial evaluation scope and the cost of re-certification across the product lifecycle — translating directly into lower assurance overhead for manufacturers and a more sustainable path to maintaining certification over extended device lifetimes. Hildebrand will demonstrate this in practice: the CHERI-secured SAPC will be submitted for CPA certification, providing an independently verified, evidence-based benchmark of evaluation time and cost against a conventional equivalent and establishing a concrete reference point for the assurance economics of CHERI adoption in smart metering infrastructure (See Section 6).

Economic benefits of CHERI in energy

Fewer updates, lower operational cost

The energy sector operates some of the largest and most demanding connected device deployments in existence: millions of devices distributed across generation, transmission, distribution, and consumer premises, operating over decade-long lifecycles in environments where availability and integrity are safety-critical. The operational cost exposure of energy-related IoT and smart metering infrastructure concentrates around three interrelated areas:

1. the recurring burden of security-driven firmware updates,
2. the compounding of risk and cost across extended device lifetimes, and
3. the liability arising from field recalls when remote remediation proves insufficient

1. Fewer firmware updates

Each firmware update to fleets of this scale carries significant cost. The direct costs alone are substantial:

- network bandwidth charges
- processor cycles and flash wear consumed during download and installation
- infrastructure required to host, sign, and monitor update packages at scale
- engineering time to identify, patch, test, and release a fix for each vulnerability
- regression testing, security assessment, and staged rollout before fleet-wide deployment

Beyond the direct costs, the indirect and risk costs compound the picture: some devices in a large fleet will fail to apply an update successfully, requiring field engineer intervention; devices in an update state may be temporarily unavailable for operational functions; repeated security updates signal product weakness to customers and regulators; and a vulnerability not patched within an acceptable window may trigger PSTI, NIS2, or sector-specific enforcement action. GB smart metering illustrates the scale: the meter rollout alone represents millions of devices communicating over managed national infrastructure, where a single mandatory security update can cost tens to hundreds of thousands of pounds in engineering, testing, network, and field support.

2. Long asset life

Smart meters are expected to operate for 15–20 years, and over that period the accumulation of software vulnerabilities in a conventional embedded device is substantial. Vulnerability density in shipping C/C++ firmware is typically in the range of 1–5 defects per 1,000 lines of code, with a meaningful fraction being memory-safety relevant; a device with 100,000 lines of firmware might accumulate 10–50 exploitable memory-safety vulnerabilities over its lifetime, each requiring patching at the costs described above. In the final years of device life — particularly as OEMs wind down active development support — the ability to issue timely patches diminishes, creating end-of-lifecycle vulnerability windows during which known defects cannot be reliably remediated. Where a vulnerability is sufficiently severe and OTA remediation is not available or cannot be trusted, physical intervention becomes necessary. Meter Asset Managers are acutely aware of this cost: a field engineer visit to a domestic premise runs to £80–£150 depending on location and complexity, before materials, and a recall affecting even 1% of a million-device fleet represents £800,000 to £1.5 million in field intervention alone.

3. Security liability

CHERI does not eliminate all classes of vulnerability — no technology can. Logic errors, authentication weaknesses, protocol design flaws, and application-layer vulnerabilities remain possible and require ongoing software discipline to manage. What CHERI does is eliminate entire vulnerability

categories that currently drive a substantial proportion of security patch cycles: specifically, the memory-safety classes that account for roughly 70% of exploitable CVEs in typical embedded codebases. Buffer overflow and out-of-bounds attacks cannot succeed against CHERI-protected code; use-after-free vulnerabilities are deterministically mitigated at the hardware level; and pointer injection (i.e., the ability for an attacker to forge or manipulate memory pointers to redirect execution) is architecturally prevented.

The implication is not that CHERI-enabled devices will never require firmware updates, but that the frequency of security-driven updates will be substantially lower, and the risk of a critical unpatched window — where a known vulnerability cannot be remediated before exploitation — is also materially reduced. This directly changes the economics of long-lifecycle deployment: by reducing the number of security patches required across the device lifetime and making end-of-lifecycle risk substantially lower, a CHERI-enabled device can credibly commit to a longer, lower-cost support period, directly addressing the PSTI Act's requirement for manufacturers to specify minimum security update durations. The same logic applies to the tail risk of physical intervention: by eliminating the memory-safety vulnerability classes that most commonly drive critical severity ratings, CHERI substantially reduces the probability of a recall ever becoming necessary — delivering a meaningful actuarial reduction in field cost liability for meter operators and energy suppliers across the full device lifecycle.

University of Warwick CHERI Cost / Benefit Analysis

On the benefit side, the study identifies reductions in security personnel costs, fewer security-driven development iterations, lower operational patching overhead, improved compliance posture under emerging regulation, and materially reduced exposure to insurance claims and regulatory fines — with the study concluding that CHERI adoption is likely to be substantially net-positive, particularly where litigation avoidance is material.

These benefits do not come without investment. The study identifies three principal cost categories:

1. silicon and hardware development
2. codebase migration and
3. training

Codebase migration costs, modelled on the CheriBSD and WebKit JavaScriptCore ports, are estimated at approximately £470,000 for those reference projects, with typical modifications affecting fewer than 1.4% of lines of code. Training and ongoing maintenance for an organisation of twenty engineers is estimated at approximately £140,000 in the first year, declining as CHERI expertise matures in the market. Hardware costs are volume-dependent and become substantially more favourable at production scale.

On balance, the Warwick analysis finds that benefits outweigh costs, estimating over £1.9 million net benefits for large organisations.

£1.9m benefit

Compartmentalisation

New business models enabled by CHERI

CHERI's memory safety properties address existing costs and risks. Its compartmentalisation capabilities enable something qualitatively new: the ability to run isolated, mutually distrusting software components on a single embedded device, with hardware-enforced boundaries that prevent any component compromising another.

This is architecturally distinct from anything achievable in conventional embedded platforms. Today, smart meters are monolithic, all firmware components (metering logic, communications stack, cryptographic functions, and any value-added services) run within a single trust domain. A vulnerability in any component can, in principle, be exploited to access all other components' data and functions.

CHERIoT's compartment model changes this. Each software compartment is granted precisely the capabilities it needs — no more. A compromised communications stack cannot read metering data. A third-party application cannot access the cryptographic key store. The metering function cannot be disrupted by a fault in the HAN interface. These boundaries are enforced in hardware and verified at compile time by CHERIoT-Audit.



Multi-Vendor firmware architecture

Today smart meter firmware is typically developed and maintained by a single OEM or a tightly controlled software supplier. This model limits competitive dynamics, concentrates supply chain risk and makes it difficult to introduce new features or services without a full firmware release cycle.

CHERI compartmentalisation enables a different model: multiple independent software vendors supplying components that run in isolated compartments on a single device without the need for mutual trust between vendors.

Consider a smart meter where:

- The metering core (measurement, calibration, tariff calculation) is provided and certified by the meter OEM
- The communications stack (DCC WAN, HAN, ZigBee, LTE-M) is provided by a specialist communications supplier
- A billing services module is provided by the energy supplier
- An in-home display interface module is provided by a third-party HAN device manufacturer

In a conventional architecture this approach would require extensive inter-vendor trust agreements, security assessment of each party's code and complex integration testing because any component can access any other's data. With CHERIoT compartmentalisation each component is isolated by hardware. The metering core's certification is not affected by the security of the communications module. Energy suppliers can update their billing logic without a full device firmware cycle. Third-party developers can contribute services with a limited, auditable capability set.

This is a structural enabler of open metering ecosystems and offers a significant shift from the closed, vertically integrated model that dominates today.

Secure third-party application models

The compartmentalisation model extends to value-added services and applications. An energy supplier or meter manufacturer could, for example, offer a certified application runtime on CHERI-enabled meters thus allowing approved third parties to deploy services (e.g. demand response, flexibility market participation, EV charging coordination) without compromising the integrity of the metering function.

This is analogous to the trusted execution environments (TEEs) used in smartphones to isolate payment and identity functions but implemented at a lower hardware level without the complexity and overhead of a full TEE implementation and with auditable, formally verified boundaries.

The commercial implications are significant:

- New revenue streams for energy suppliers and MAMs from value-added services on existing hardware
- Faster innovation cycles as new services can be deployed and updated independently of metering firmware
- Reduced certification burden because each compartment's security properties can be assessed independently rather than requiring full re-certification of the device on each firmware update
- Market differentiation as CHERI-enabled metering platforms become programmable infrastructure, not static measurement hardware

Reduced hardware bill of materials

Today security isolation between functions on an embedded device typically requires separate microcontrollers or dedicated security elements (secure enclaves, TPMs, hardware security modules). These add cost, board space and integration complexity.

CHERIoT's hardware compartmentalisation provides equivalent isolation within a single device, on a single die, without the overhead of additional silicon. For a smart meter:

- A single ICENI chip can host the metering function, the communications processor, the cryptographic key store and optional third-party services, in hardware-isolated compartments
- The need for a separate secure enclave chip for key management is reduced or eliminated
- Board-level design complexity and component count are reduced
- At the volume of the UK smart meter rollout, a bill of materials saving of even £2–5 per device translates to £2–5 million per million devices deployed. This is a direct cost reduction available to OEMs who adopt CHERI-enabled silicon.

"New utility models are possible where the meter is a platform for a GB smart energy app store"

Hildebrand Technology Limited

hildebrand

Enables longterm service relationships

The compartmentalisation model also enables a new commercial relationship between device manufacturers, energy suppliers and end users: the meter as a managed services platform rather than a one-time hardware sale.

If a device can securely host independently updated, third-party certified software compartments, energy suppliers can:

- Deploy new tariff and flexibility services to existing devices without device replacement
- Update service logic independently of hardware firmware cycles
- Offer differentiated service tiers to consumers on the same physical hardware

For MAMs, who bear operational cost across a 10–15 year device lifecycle, this changes the economics of metering from a capital-intensive hardware rollout to an ongoing services model with hardware replacement driven by functional obsolescence rather than security necessity.

hildebrand

Demonstrating CHERI in the energy sector

Hildebrand is a technology innovation company that's operated in the UK energy sector for over twenty years.

Hildebrand are recognised for delivering robust hardware, software and data solutions as part of their mission to support the drive to Net Zero.

For the CHERI Adoption programme, Hildebrand will integrate the SCI ICENI chip into three products to demonstrate CHERI's capabilities in production-relevant hardware:

01

cSAPC

A CHERI-secured Standalone Auxiliary Proportional Controller (SAPC) compatible with GB SMETS2 meters. CHERI offers hardware-enforced separation between metering logic, DCC communications, and HAN interface functions.

02

cCOP11

A CHERI-secured asset meter certified to participate in GB's flexibility market. Demonstrates CHERI's applicability across meter types.

03

CHERI Pi

A microcontroller board enabling third-party application and software development on CHERIoT. Provides a developer platform enabling energy suppliers, service vendors, and system integrators to develop and test CHERIoT-compartmentalised applications ahead of full product deployment.

hildebrand

Market Opportunity

The case for CHERI-enabled devices in the UK energy sector is not driven by a single consideration, there are four forces at work:

1. The threat landscape is worsening. Memory safety vulnerabilities remain the dominant class of exploitable defect. The expansion of the connected device estate, the growth of AI-assisted attack tooling and the geopolitical dimension of critical infrastructure targeting all increase the probability that any specific vulnerability will be found and exploited during a device's operational lifetime.
2. The regulatory environment is tightening. The EU CRA (compliance mandatory from December 2027), the UK PSTI Act and NIS2 collectively create legal obligations for security-by-design across the connected device lifecycle. Non-compliance is not a risk to be managed; it is a product market exclusion.
3. The operational cost of the status quo is rising. Security patch cycles are expensive. Field interventions are expensive. Breach remediation is expensive. As device fleets scale so do the operational liabilities of maintaining conventional firmware. CHERI does not eliminate these costs entirely but it substantially reduces the largest cost component: memory-safety-driven patch and remediation cycles.
4. CHERI's compartmentalisation does not merely reduce risk, it enables a qualitatively different product architecture that supports multi-vendor firmware ecosystems, secure third-party application platforms, reduced hardware BOM, and a transition from one-time hardware sale to ongoing managed services.

Chips available now

After 15 years of development, CHERI-enabled silicon is available today. SCI Semiconductor's ICENI chip is in production. The CHERIoT RTOS and toolchain are mature, open-source and backed by Microsoft, Google and the CHERI Research Centre at Cambridge. The Hildebrand cSAPC and cCOP11 products are programme deliverables under active development.

The window for first-mover advantage is now open but will not be indefinitely. As the CRA deadline of December 2027 approaches device manufacturers who have not begun the transition to hardware-enforced security will face a costly late scramble to demonstrate compliance. Those who adopt CHERI now will be able to deliver:

- Proven technology, certified products and operational experience ahead of regulatory deadlines
- A supply chain and engineering capability that competitors must replicate from scratch
- Reference deployments that demonstrate compliance to regulators and buyers

Who benefits?

Smart meter manufacturers: The ICENI chip from SCI Semiconductor, and the CHERIoT ecosystem around it, provides a production-ready path to hardware-enforced memory safety and compartmentalisation. Contact Hildebrand for access to reference designs, tooling, and regulatory engagement support.

Energy suppliers and Meter Asset Managers: The lifecycle cost of managing a CHERI-enabled device fleet is materially lower than that of a conventional fleet. The risk of a critical security event requiring emergency response with the attendant regulatory, operational and reputational consequences is substantially reduced. The commercial opportunity of a programmable, compartmentalised metering platform enables new service models that are not available on conventional hardware.

hildebrand

Hildebrand Technolgoy Limited
63 Dean Street
London
W1D 4QG

info@hildebrand.co.uk
hildebrand.co.uk

2026
Position Paper

Further reading

Academic and Technical Papers

Watson, R.N.M. et al. (2020). CHERI: A Hybrid Capability-System Architecture for Scalable Software Compartmentalization. University of Cambridge Technical Report UCAM-CL-TR-941. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-941.pdf

Watson, R.N.M. et al. CHERI ISAv9. University of Cambridge Technical Report UCAM-CL-TR-987. Available: https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-987.pdf

Chisnall, D. et al. CHERI C/C++ Programming Guide. Available: https://ctsrd-cheri.github.io/cheri-c-programming/

CHERIoT Platform. (2024–2026). CHERIoT Platform Specification and Formal Model. Available: https://cheriot.org

Industry Statistics — Memory Safety

Microsoft Security Response Centre. (2019). A Proactive Approach to More Secure Code. Available: https://msrc-blog.microsoft.com/2019/07/16/a-proactive-approach-to-more-secure-code/

Google Project Zero. (2022). The More You Know, The More You Know You Don't Know. Available: https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html

MITRE. (2025). CWE Top 25 Most Dangerous Software Weaknesses 2025. Available: https://cwe.mitre.org/top25/archive/2025/2025cwetop25.html

CISA. (2023). The Urgent Need for Memory Safety in Software Products. Available: https://www.cisa.gov/news-events/news/urgent-need-memory-safety-software-products

CISA / NSA / NCSC et al. (2023). The Case for Memory Safe Roadmaps. Available: https://www.cisa.gov/case-memory-safe-roadmaps

Cost of Breach

IBM / Ponemon Institute. (2025). Cost of a Data Breach Report 2025. Available: https://www.ibm.com/reports/data-breach

CHERI Alliance. (2026). CHERI Adoption Global Ecosystem Assessment Q1 2026. Available: https://cheri-alliance.org/adoption/

Regulatory Framework

European Parliament and Council. (2024). Regulation (EU) 2024/2847 — Cyber Resilience Act. OJ L 2024/2847. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

European Parliament and Council. (2022). Directive (EU) 2022/2555 — NIS2 Directive. Available: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

UK Government. (2022). Product Security and Telecommunications Infrastructure Act 2022. Available: https://www.legislation.gov.uk/ukpga/2022/46/contents/enacted

NCSC / DCMS. Secure by Design. Available: https://www.ncsc.gov.uk/topic/secure-by-design

CHERI Ecosystem and Silicon

SCI Semiconductor. (2024). Press Release: ICENI Family — Global-First CHERI-Enabled Devices. Available: https://www.scisemi.com/company/press-release-iceni-family/

CHERI Research Centre, University of Cambridge. Available: https://cheri.cst.cam.ac.uk/

lowRISC / SCI Semiconductor. Sunburst Chip Repository Release. Available: https://lowrisc.org/news/lowrisc-and-sci-semiconductor-release-sunburst-chip-repository-for-secure-microcontroller-development/

Microsoft CHERIoT-Ibex. Available: https://github.com/microsoft/cheriot-ibex

'2016 Ukraine Electric Power Attack, Campaign C0025 | MITRE ATT&CK®'. Accessed 3 August 2026. https://attack.mitre.org/campaigns/C0025/.

Bauwens, Jan, Peter Ruckebusch, Spilios Giannoulis, Ingrid Moerman, and Eli De Poorter. 'Over-the-Air Software Updates in the Internet of Things: An Overview of Key Principles'. IEEE Communications Magazine 58 (February 2020): 35–41. https://doi.org/10.1109/MCOM.001.1900125.

'CHERIoT Programmers' Guide'. Accessed 3 August 2026. https://cheriot.org/book/.

'Cost of a Data Breach Report 2026 | IBM'. Accessed 3 August 2026. https://www.ibm.com/reports/data-breach.

'Cyber Resilience Act | Shaping Europe's Digital Future'. Accessed 3 August 2026. https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act.

Department for Science, Innovation and Technology. 'Cyber Security and Resilience Bill'. GOV.UK, 12 November 2025. https://www.gov.uk/government/collections/cyber-security-and-resilience-bill.

Feng, Kai, Huanting Wang, Jeremy Singer, and Zheng Wang. 'Interpreter Memory Safety via Differential Fuzzing with a CHERI on Top'. Proceedings of the 2026 ACM SIGPLAN International Symposium on Memory Management, 11 June 2026, 25–39. https://doi.org/10.1145/3814942.3816133.

Fowler, Daniel S., Lukasz Bartoszcze, Carsten Maple, Gregory Epiphaniou, Anhtuan Le, and Miroslaw Malinowski. Economic Factors in CHERI Adoption (ResAuto Deliverable D3.2). Report. WMG, 2024. https://wrap.warwick.ac.uk/id/eprint/189379/.

'FrostyGoop Incident, Campaign C0041 | MITRE ATT&CK®'. Accessed 3 August 2026. https://attack.mitre.org/campaigns/C0041/.

'Google Project Zero'. Accessed 3 August 2026. https://projectzero.google/.

GOV.UK. 'CHERI Adoption and Diffusion Research'. Accessed 3 August 2026. https://www.gov.uk/government/publications/cheri-adoption-and-diffusion-research/cheri-adoption-and-diffusion-research.

GOV.UK. 'Smart Meters in Great Britain, Quarterly Update March 2026'. Accessed 3 August 2026. https://www.gov.uk/government/statistics/smart-meters-in-great-britain-quarterly-update-march-2026.

GOV.UK. 'Summary of Research on the Economic Impact of Cyber Attacks'. Accessed 3 August 2026. https://www.gov.uk/government/publications/independent-research-on-the-economic-impact-of-cyber-attacks-on-the-uk/summary-of-research-on-the-economic-impact-of-cyber-attacks.

GOV.UK. 'The UK Product Security and Telecommunications Infrastructure (Product Security) Regime'. 2 May 2024. https://www.gov.uk/government/publications/the-uk-product-security-and-telecommunications-infrastructure-product-security-regime.

Grisenthwaite, Richard, Graeme Barnes, Robert N. M. Watson, Simon W. Moore, Peter Sewell, and Jonathan Woodruff. 'The Arm Morello Evaluation Platform—Validating CHERI-Based Security in a High-Performance System'. IEEE Micro 43, no. 3 (2023): 50–57. https://doi.org/10.1109/MM.2023.3264676.

'INFORMATICS - DIGIT to Assess the Security of the Open Source Software'. Accessed 3 August 2026. https://ec.europa.eu/newsroom/informatics/items/26511.

McConnell, Steve. Code Complete: A Practical Handbook of Software Construction. Microsoft Press, 2004.

Moghadam, Vahid Eftekhari, Gabriele Serra, Federico Aromolo, Giorgio Buttazzo, and Paolo Prinetto. 'Memory Integrity Techniques for Memory-Unsafe Languages: A Survey'. IEEE Access 12 (2024): 43201–21. https://doi.org/10.1109/ACCESS.2024.3380478.

'NIS2 Directive: Securing Network and Information Systems | Shaping Europe's Digital Future'. Accessed 3 August 2026. https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

Press Release - ICENI Family. n.d. Accessed 3 August 2026. https://www.scisemi.com/company/press-release-iceni-family/.

Reiher, Cathleen. 'Pointer Arithmetic'. Topic. Oracle Help Center, August2023. Accessed 3 August 2026. https://docs.oracle.com/en/operating-systems/solaris/oracle-solaris/11.4/dtrace-guide/pointer-arithmetic.html.

'Secure by Design Principles'. UK Government Security - Beta, n.d. Accessed 3 August 2026. https://www.security.gov.uk/policy-and-guidance/secure-by-design/principles/.

Sen, Ömer, Andreas Ulbig, and Martin Henze. 'Detection of Multi-Stage Cyberattacks on SCADA-Based Control Systems in Power Grids'. RWTH Aachen University, 2025. Online.

'Triton Malware Hits Critical Infrastructure in Saudi Arabia | Infosec'. Accessed 3 August 2026. https://www.infosecinstitute.com/resources/malware-analysis/triton-malware-hits-critical-infrastructure-saudi-arabia/.

Watson, Robert N. M., John Baldwin, Tony Chen, et al. It Is Time to Standardize Principles and Practices for Software Memory Safety (Extended Version). Computer Laboratory, University of Cambridge, n.d. PDF, 29 pages. https://doi.org/10.48456/TR-996.

Watson, Robert N. M., Simon W. Moore, Peter Sewell, and Peter G. Neumann. An Introduction to CHERI. n.d.

hildebrand

September 2026