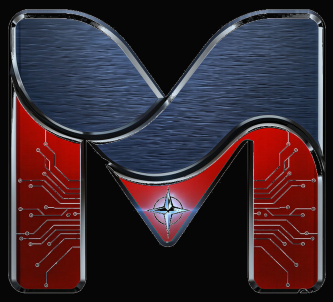

MICKAI EBOOK SERIES · PLAYBOOK No. 1

Sovereign AI for the UK Regulated Workstation.

An engineering playbook for defence-nuclear, civil-nuclear, defence primes, finance, pharma, and critical national infrastructure. Four parts on the constraint, the substrate, the desk, and the playbook.

AUTHOR

Micky Irons

Founder and named inventor, Mickai LTD.

Crunchbase · LinkedIn · GitHub · mickai.co.uk

EBOOK · No. 1 IN A SERIES OF EIGHT

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk

UK IPO patent family GB2607309.8 to GB2610422.4 · Trade mark UK00004373277

DATE · 13 May 2026 · v1

EBOOK · No. 1 IN A SERIES OF EIGHT

Mickai LTD · Companies House 17166618 · press@mickai.co.uk · mickai.co.uk

TABLE OF CONTENTS

Contents

FOREWORD

A note from the author

This ebook is the engineering counterpart to the regulated UK workstation's egress posture. It is written for the design engineer, the engineering CTO, the procurement officer, and the regulator inside the buyer organisation, and for the platform partners and integrators who want to reach that buyer with a credible joint architecture.

I worked on the Sellafield site before founding Mickai LTD. The constraint described in Part I is not theoretical; it is the working day of every engineer on every regulated UK site, observed from inside it. The architecture you will read about in Part II is what happens when an engineer who lived inside the constraint sits down to design the AI substrate that would have made the constraint productive rather than blocking. Part III is what the substrate actually does at the desk. Part IV is the playbook for an engineering CTO who wants to pilot it inside their own estate this quarter.

The substrate primitives in this ebook are filed at the UK Intellectual Property Office across the GB2607309.8 to GB2610422.4 patent family. The trade mark Mickai is registered at UK00004373277. The schema, the conformance vectors, and the reference verifier are scheduled for joint open-source release upon UK IPO acknowledgement of the OAR family.

Micky Irons

Founder and named inventor, Mickai LTD · 13 May 2026

PART I · THE CONSTRAINT

Why every UK regulated workstation runs the same egress posture, and why the cloud AI security platform stack cannot satisfy it

1. The structural constraint at the UK regulated workstation

A design engineer at a UK regulated workstation, in any of the verticals named below, sits at a desk running CAD against design geometries, P&ID; diagrams, structural analyses, simulation models, control-software listings, and ten or more other regulated engineering applications. Production data on the screen is, by data classification, content the site does not allow off-perimeter. The engineer cannot open Claude, ChatGPT, Codex, Copilot, Cursor, Gemini, or any other cloud AI tool, because every one of those tools requires the prompt and the surrounding context to leave the operator's network and reach a vendor-controlled endpoint.

The rule is not a recommendation; it is the operating posture of every defence-nuclear yard, every Nuclear Decommissioning Authority site, every defence prime, every PRA-regulated bank, every pharma prime, and every critical national infrastructure operator in the United Kingdom. The engineer therefore sits at a workstation in 2026 with no AI assistance at all, while an engineer in an unregulated environment is using AI to extend their throughput by an order of magnitude. The productivity gap is structural, not behavioural. The operator is not anti-AI; the operator is anti-egress.

> **Sovereign AI at the workstation closes that gap at the cryptographic primitive layer, without moving a single packet off the operator's perimeter.**

2. Where the constraint binds, vertical by vertical

Defence-nuclear

BAE Systems' submarine programme at Barrow-in-Furness designs and builds the Astute-class and Dreadnought-class platforms; every workstation on that yard holds design data the site does not let out of its perimeter. Rolls-Royce Submarines at Raynesway in Derby designs and manufactures the pressurised water reactors that propel them; the same egress posture binds the propulsion engineering line. Babcock International's nuclear engineering and submarine refit operations at Devonport, Faslane, and Bristol run under the same data class. AWE at Aldermaston and Burghfield,

the design authority for the UK's nuclear warhead, runs the strictest of all. None of these sites can use cloud AI, period.

Civil and decommissioning nuclear

EDF Energy UK runs the operating fleet of UK civil reactors; Hinkley Point C and Sizewell C are in construction; the Nuclear AMRC at Sheffield runs the manufacturing engineering research base. The Nuclear Decommissioning Authority portfolio (Sellafield Ltd, Magnox Ltd, Dounreay Site Restoration Ltd, and the wider site licensee community) is the largest, most expensive, most schedule-sensitive industrial decommissioning programme on the UK balance sheet. Every workstation across that portfolio runs the same egress constraint. The throughput gap on the engineering side of the NDA portfolio alone is a national-scale cost-out variable.

Defence primes (non-nuclear)

Leonardo UK, Thales UK, MBDA UK, QinetiQ, Lockheed Martin UK, Raytheon UK, Northrop Grumman UK, and the wider defence supply chain (Cobham, Ultra Electronics, Chemring, Meggitt, Marshall, GKN Aerospace) all run hard data-class boundaries that forbid prompt egress.

Aerospace and civil aviation

Rolls-Royce's civil aerospace engineering at Derby, Airbus UK at Filton and Broughton, BAE Systems' Air sector, GKN Aerospace, and the regional supply chain run engineering data classes where the operator does not voluntarily release prompts to vendor flows.

Finance

The UK's PRA-regulated banks (HSBC UK, Barclays, Lloyds Banking Group, NatWest Group, Santander UK, Standard Chartered) run transaction monitoring, credit decisioning, market surveillance, and compliance review queues on workstations under SS1/23 model risk management expectations. The PRA names third-party AI dependency as concentration risk that must be priced into operational resilience. The workstation does not get cloud AI; it stays at no AI.

Pharma and life sciences

GSK and AstraZeneca run pre-clinical compound libraries, trial datasets, and pre-publication research evidence that hold structural IP positions. The same holds for the UK's wider pharma cluster (Pfizer UK, Novartis UK, Roche UK, MSD UK, Janssen UK, Eli Lilly UK) and the academic-prime joint ventures at Crick, Babraham, Diamond, and the Wellcome Sanger Institute.

Critical national infrastructure

National Grid, SSE, Drax, Centrica, ENW, UK Power Networks, BT, Openreach, Virgin Media O2, Thames Water, Severn Trent, United Utilities, and the wider water and energy sector all run operational data classes where the egress question is itself the assurance question.

Government primes and outsourcers

Capita, Serco, Atos UK, Fujitsu UK, KPMG UK, PwC UK, EY UK, and Deloitte UK run government workloads where the data class often forbids vendor-key AI.

3. Why cloud AI security platforms cannot satisfy the constraint

The conventional cloud AI security platform (Lakera, Check Point AI Security, Palo Alto AI Access Security, Wiz AI-SPM, and the wider category) ships a runtime detection layer across workforce, application, and agent surfaces, fuelled by a vendor-cloud threat intelligence feed and delivered as a cloud-and-agent platform. The architecture is excellent for the use cases those platforms already serve.

Underneath every AI security platform sits a cryptographic primitive that decides who holds the keys, what format the audit chain is in, and whether the chain can be verified by a regulator without the platform vendor in the loop. That primitive is where the UK regulated buyer draws the line. Vendor-key audit, vendor-format logs, and vendor-cloud inference are, today, structurally unacceptable to the buyer described in section 2.

> **The substrate question is upstream of the platform question. The platform category is welcome to ride above the substrate; the substrate cannot be supplied by the platform.**

PART II · THE SUBSTRATE ANSWER

The cryptographic primitive underneath every AI agent

4. The Mickai sovereign hardware AI workstation, in plain terms

A Mickai sovereign hardware AI workstation is a desktop or rack workstation, certified by Mickai LTD, that runs the Mickai Sovereign Intelligence Operating System (SIOS) on the operator's iron, with the model weights resident on the workstation's encrypted storage, the inference compute resident on the workstation's GPU or NPU, the audit ledger signed under the operator's TPM-bound key, and the verifier running locally in any browser tab. No prompt, no context, no token, and no output leaves the operator's network. The substrate is the same SIOS substrate documented under the brain taxonomy at mickai.co.uk/brains: six subsystems, twenty-five brains, an Arbiter Brain at the head and a hash-linked, post-quantum signed audit ledger at the foot.

5. The audit substrate: FIPS 204 ML-DSA-65, hash-linked CBOR

Every committed action across a deployed AI workload is serialised in CBOR (Concise Binary Object Representation), hashed under SHA-3-512, signed under the operator's TPM-bound FIPS 204 ML-DSA-65 key, and appended to a hash-linked chain. The chain is the canonical record of what the AI did, who it did it to, and under whose authority. The schema is open. The conformance vectors are open. The verifier is open.

Why FIPS 204

FIPS 204 ML-DSA-65 is the NIST-standardised post-quantum digital signature scheme, published in 2024. It is the algorithm the NCSC post-quantum migration roadmap names for the 2031 high-priority infrastructure deadline and the 2035 universal cryptographically-relevant deadline. Signing the audit chain under ML-DSA-65 in 2026 means the chain still verifies in 2035 against a cryptographically-relevant quantum attacker that did not exist when the chain was signed.

Why SHA-3-512

SHA-3-512 (Keccak family, NIST FIPS 202) is the hash function that links each record in the chain to its predecessor. Tampering with any record anywhere in the chain breaks the linkage at every subsequent record. The chain is therefore append-only by construction; the operator does not have to enforce append-only at the application layer.

Why CBOR

CBOR (RFC 8949) is a deterministic binary serialisation format. The same logical record always serialises to the same byte string, which is the property the signing operation requires. JSON, by

contrast, is not canonical (whitespace, key order, number representation all vary). A signed JSON audit log is therefore not portable across implementations; a signed CBOR audit log is.

6. Trust-domain externalisation as the operating pattern

The architectural pattern that makes the same chain replayable by four parties at once is trust-domain externalisation. The operator holds the signing key. The schema is open. The verifier is open. The conformance vectors are open. The vendor of the underlying AI is not the trust root; the vendor is a participant. When the vendor changes, when the vendor is acquired, when the vendor fails, the chain continues to verify under the operator's key.

The worker who was surveilled at Time T can, at Time T plus eighteen months, walk the chain on a phone in a browser tab and produce a deterministic verdict per action that affected them. That is the structural property that policy alone does not produce. It is the property the substrate produces by construction.

7. The browser-resident offline verifier

Any party (the operator's CISO, the operator's auditor, the relevant sector regulator, the union representative, a forensics investigator, a shareholder, a journalist with a court order) can replay the chain on a sandboxed laptop, offline, in any browser tab, weeks or months after the event. The verifier emits one of four deterministic verdicts per record. VERIFIED. INVALID. STALE. REVOKED. There is no fifth verdict. There is no probabilistic answer. The chain either holds or it does not.

The verifier ships as a WebAssembly module. It runs with a no-network invariant. The operator can supply the chain on a USB drive or via an intranet endpoint; the verifier does not need to phone anyone. This is the property the regulator actually requires for evidence at a tribunal.

PART III · AT THE DESK

What the engineer at the desk actually gets

8. Concrete workflows across the verticals

Examples, at the workstation, with no network egress, across multiple primes and operators.

CAD copilot at a BAE Systems Barrow submarine workstation

"Extract a parts list from this Astute-class hull-section assembly model and cross-reference against the supplier QA register." The model runs on the workstation. The CAD file never leaves. The audit ledger records the prompt, the files referenced, the reasoning steps, the output, signed under the engineer's TPM-bound key.

PWR engineering assistant at a Rolls-Royce Submarines Raynesway workstation

"Walk through this primary-circuit P&ID and identify isolation points for refit shutdown." Diagram stays on the workstation. Reasoning trace replayable by the QA function months later, without recourse to any vendor.

Decommissioning copilot at a Sellafield, Magnox, or Dounreay workstation

"Given this dose-rate isosurface dataset, propose three shielding configurations that meet ALARP." Dataset stays on the workstation. Output is a signed substrate record, not a vendor JSON.

PLC and SIL code generation across nuclear, energy, water, and rail

"Refactor this PLC ladder logic against IEC 61511." Ladder logic stays on operator iron. Substrate records the diff for the SIL assessment.

Transaction monitoring copilot at a UK PRA-regulated bank

"Cluster these flagged transactions against the bank's historical AML topology." Transaction data stays on bank infrastructure. Substrate satisfies SS1/23 model risk evidence.

Pre-clinical informatics at GSK or AstraZeneca

"Predict ADMET properties for this candidate library and rank against the bench results." Compound structures stay on operator workstations; the IP boundary holds.

Network engineering at BT or Openreach

"Analyse this packet capture against the playbook for type-X fault." Capture stays on the operator's network estate. Substrate produces a signed action chain for OFCOM or any subsequent regulator review.

9. Throughput lift, in operator language

Comparable unregulated benchmarks (DORA-style engineering productivity studies on cloud-AI-equipped workstations through 2025 and 2026) put the typical AI-assistance lift at five to ten times on document-heavy engineering work (technical reports, safety cases, change-control packages, regulatory submissions), two to four times on CAD-led design work (drawing markup, assembly review, parts-list extraction), and three to seven times on code-led engineering (PLC, software-on-control, simulation harness authoring). For an operator running a thousand-engineer organisation under a hard egress posture, the gap between zero AI assistance and substrate-grade AI assistance is, conservatively, equivalent to several hundred engineering full-time-equivalents reclaimed from the same headcount, every year, every site.

The throughput estimate is the comparable-benchmark figure, not a promise. The Mickai workstation produces an auditable chain of every AI-assisted action; the operator's own engineering function measures the realised throughput against the chain, in the operator's own language, against the operator's own quality bar.

10. Compliance fit, by regulator

The substrate audit ledger is the artefact the sector regulator can walk for incident review without vendor cooperation. The mapping below is the non-exhaustive list of regulators the substrate is engineered against.

ONR · Office for Nuclear Regulation

Civil and decommissioning side. The Authority's design-data lineage expectation is satisfied at the cryptographic primitive layer; every AI-assisted decision is signed under the operator's TPM-bound key, hash-linked, and replayable offline by the regulator.

Defence Authority · JSP 440 derivatives

Defence-nuclear and defence sides. The workstation slots into existing controlled-IT estates as a certified terminal. The chain is the artefact the Authority reads to verify design lineage, without recourse to the AI vendor in the loop.

PRA · SS1/23 model risk management

Finance side. The cryptographic position the workstation produces is, by construction, the operational resilience evidence the supervisory statement asks for.

ICO · workplace monitoring guidance and UK GDPR

Across all verticals where AI touches data subjects. The chain is the worker's, the union's, the employer's, and the regulator's at once. UK GDPR Article 22 challenges become tractable on cryptographic evidence rather than on procedural representation.

OFCOM, OFWAT, OFGEM · CNI sector regulators

The substrate audit ledger is the artefact the sector regulator can walk for incident review without vendor cooperation.

MHRA · pharma

Pre-clinical and trial data lineage is preserved at the cryptographic primitive layer. The Authority's chain-of-custody expectation is met by the substrate, not by vendor representation.

PART IV · THE ENGINEERING CTO PLAYBOOK

Inventory, pilot, document, transfer

11. The pilot-this-quarter playbook

Three steps that fit inside any existing controlled-IT engagement model, applicable across every vertical in Part I.

Inventory. List the design-engineering, scientific, analytic, and developer workstations across your estate where an AI surface would lift throughput materially but the egress posture forbids it. The list is usually long and well understood inside the IT, OT, and engineering functions.

Pilot. Run one Mickai sovereign hardware AI workstation against one role, at one site, for one engineering quarter. The integration is a certified workstation on the existing controlled estate. The audit substrate satisfies the sector regulator's expectation by construction.

Document and transfer. Document the pilot as a transferable artefact (the audit chain, the verifier verdict log, the throughput delta in operator language, the regulator engagement record). The artefact transfers across your estate and is reusable across the defence-nuclear, civil-nuclear, defence prime, aerospace, finance, pharma, CNI, and government-primer verticals named above.

12. The procurement rubric: twelve dimensions

The procurement officer should score any AI vendor's response against the twelve dimensions below. Pass thresholds depend on the data class; defence-nuclear, defence-prime, and PRA-regulated finance buyers should treat the table as a hard floor.

Dimension	Question
Architecture posture	Platform on cloud, agent on edge, or substrate on operator iron?
Key custody	Operator-controlled key or vendor-controlled key?
Algorithm	Post-quantum from inception or classical-only?
Inference location	On-device, vendor-edge, or vendor cloud?
Audit format	Open schema (CBOR + hash-linked) or vendor JSON?
Verifier model	Browser-resident offline, or vendor connectivity required?
Trust domain	Operator + regulator + worker, or vendor-only?
Air-gap suitability	Designed for no-egress regulated workstation, or cloud-required?

Dimension	Question
UK position	Filed at UK IPO under a UK inventor, or no UK position?
Sector fit	Sells today into defence-nuclear / NDA / PRA banks / pharma, or not?
Latency surface	Workstation-local, or cloud round-trip?
Threat intelligence	Substrate-neutral (any feed welcome above), or feed-bundled vendor lock?

13. Engagement path with the regulator

The most efficient engagement path is to brief the relevant sector regulator on the substrate before the pilot ships. The ICO, ONR, PRA, MHRA, OFCOM, OFWAT, and OFGEM all have engineering and digital-policy desks that can receive a thirty-minute substrate briefing under their existing engagement framework. The regulator does not need to bless the substrate; the regulator needs to understand that the chain they would walk during an incident is a deterministic record under the operator's key, not a vendor JSON.

14. Closing

Engineering leadership at BAE Systems, Rolls-Royce, Rolls-Royce Submarines, Babcock International, AWE, Sellafield Ltd, Magnox Ltd, Dounreay Site Restoration Ltd, EDF Energy UK, Hinkley Point C, Sizewell C, the Nuclear AMRC, Leonardo UK, Thales UK, MBDA UK, QinetiQ, HSBC UK, Barclays, Lloyds Banking Group, NatWest Group, Santander UK, Standard Chartered, GSK, AstraZeneca, National Grid, SSE, BT, Openreach, Capita, Serco, Atos UK, Fujitsu UK, KPMG UK, PwC UK, EY UK, and Deloitte UK are open to a fifteen-minute briefing at any time. press@mickai.co.uk.

The substrate is on the UK IPO public register. The trade mark is registered. The engineering is on the UK record. The next move is institutional.

APPENDIX · ABOUT THE AUTHOR

Micky Irons

Founder of Mickai LTD (Companies House 17166618, England and Wales, registered office 20 Wenlock Road, London, N1 7GU). Named inventor on the Mickai SIOS patent corpus, recorded on the UK Intellectual Property Office public register at numbers GB2607309.8 to GB2610422.4. Trade mark Mickai registered at UK00004373277 (classes 9 and 42, filed 15 April 2026).

Before founding Mickai, Micky was a Sellafield site worker. The egress constraint observed from inside the regulated workstation is the engineering origin of the substrate described in this ebook.

Profiles and links

mickai.co.uk · the canonical Mickai site.

crunchbase.com/person/micky-irons · founder profile, with the Crunchbase founder rank 40,000 to 500 in seven days result documented at mickai.co.uk/articles/amt-crunchbase-40k-to-500-in-seven-days.

linkedin.com/in/mickyirons · personal LinkedIn.

github.com/Micky-CMO · open-source position.

linkedin.com/company/mickai · Mickai LTD company page.

crunchbase.com/organization/mickyirons · Mickai LTD Crunchbase entry.

Email: press@mickai.co.uk

References and further reading

· Nuclear Decommissioning Authority, portfolio and site licensee community: gov.uk/government/organisations/nuclear-decommissioning-authority.

· Office for Nuclear Regulation (ONR), regulatory expectations on engineering substantiation.

· JSP 440, MOD defence manual on security of information, JSP 440 derivatives apply to the defence-nuclear estate.

· PRA Supervisory Statement SS1/23, model risk management principles for banks.

· NCSC, AI Cyber Security Code of Practice (DSIT consultation 2024 to 2025); Timelines for migration to post-quantum cryptography.

· FIPS 204 (ML-DSA), NIST post-quantum digital signature standard.

· Mickai SIOS, six subsystems and twenty-five brains: mickai.co.uk/brains.

· Mickai trade mark UK00004373277, classes 9 and 42, filed 15 April 2026.

Colophon

Set in Inter Tight (Variable) and Inter Black. Cover and body chrome in the Mickai gold-on-void palette. Audit ledger primitives on the cover match the live substrate. Brand voice audited under the Mickai AMT preflight gate; zero violations at publish.