National Cyber Security Centre
a part of GCHQ

10 Years of seL4 at The NCSC

Adam W1
Verification Research Lead, NCSC

National Cyber Security Centre
a part of GCHQ

Who is The NCSC?

Making the UK the safest place to live and work online.

Remit:

1. Understand cyber security, and distil this knowledge into practical guidance that we make available to all
2. Respond to cyber security incidents to reduce the harm they cause to organisations and the wider UK
3. Use industry and academic expertise to nurture the UK's cyber security capability
4. Reduce risk to the UK by securing public and private sector networks

National Cyber Security Centre
a part of GCHQ

Why Are We Speaking Today?

- NCSC has been involved with seL4 for over a decade
- Want to pull back curtain on
  - Origins of our involvement
  - What we use seL4 for
  - What we've contributed to the ecosystem
  - What some thoughts for the future

National Cyber Security Centre
a part of GCHQ

What Do We Do?

- We provide advice and guidance on cyber security for the UK
- Provide consultancy on how build and assure systems of importance to national security
- We have specific requirements for different security critical design components

National Cyber Security Centre
a part of GCHQ

Building Bespoke Components

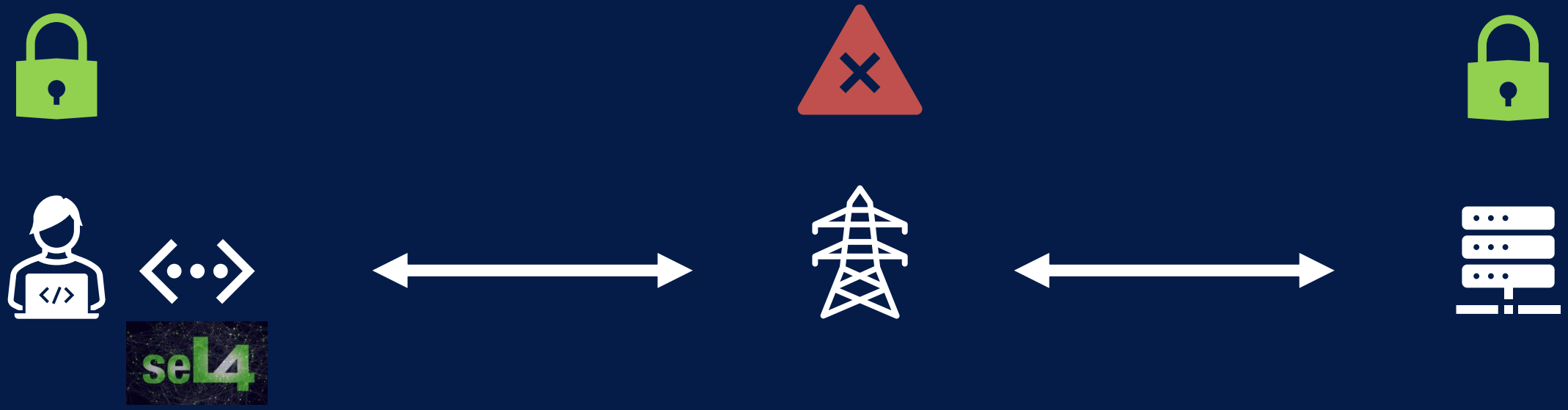
- We commission new hardware where existing devices don't provide the functionality and security we require
- We have a set of vendors we trust to build these devices
- We encourage a diversity of vendors to foster innovation
- In 2016, a vendor approached us with an interesting idea…

National Cyber Security Centre
a part of GCHQ

Secure Data Separation in Software

- Can we build a device to allow secure remote communication with classified government systems over untrusted bearers?
- It will be portable with a small form factor, and software based
- Data separation will be enforced with a formally verified micro-kernel

National Cyber Security Centre
a part of GCHQ



National Cyber Security Centre
a part of GCHQ

Why This Was Innovative

- We mandate a robust security plan to ensure that
  - a fault in one component does not compromise the security of another
  - classified data must remain separate from unclassified
- Security case very challenging in software alone
- Does that change when you have a formal proof of isolation?

National Cyber Security Centre
a part of GCHQ

What Do the Guarantees Buy Us?

- Data separation vital in security devices
- If red data ends up in black locations, critical failure
- Extremely hard to strongly guarantee in software alone

- seL4 proofs provide separation guarantees at a system level
- When conditions met, and system configured correctly, failure in one partition cannot affect the behaviour or learn the contents of another.

National Cyber Security Centre
a part of GCHQ

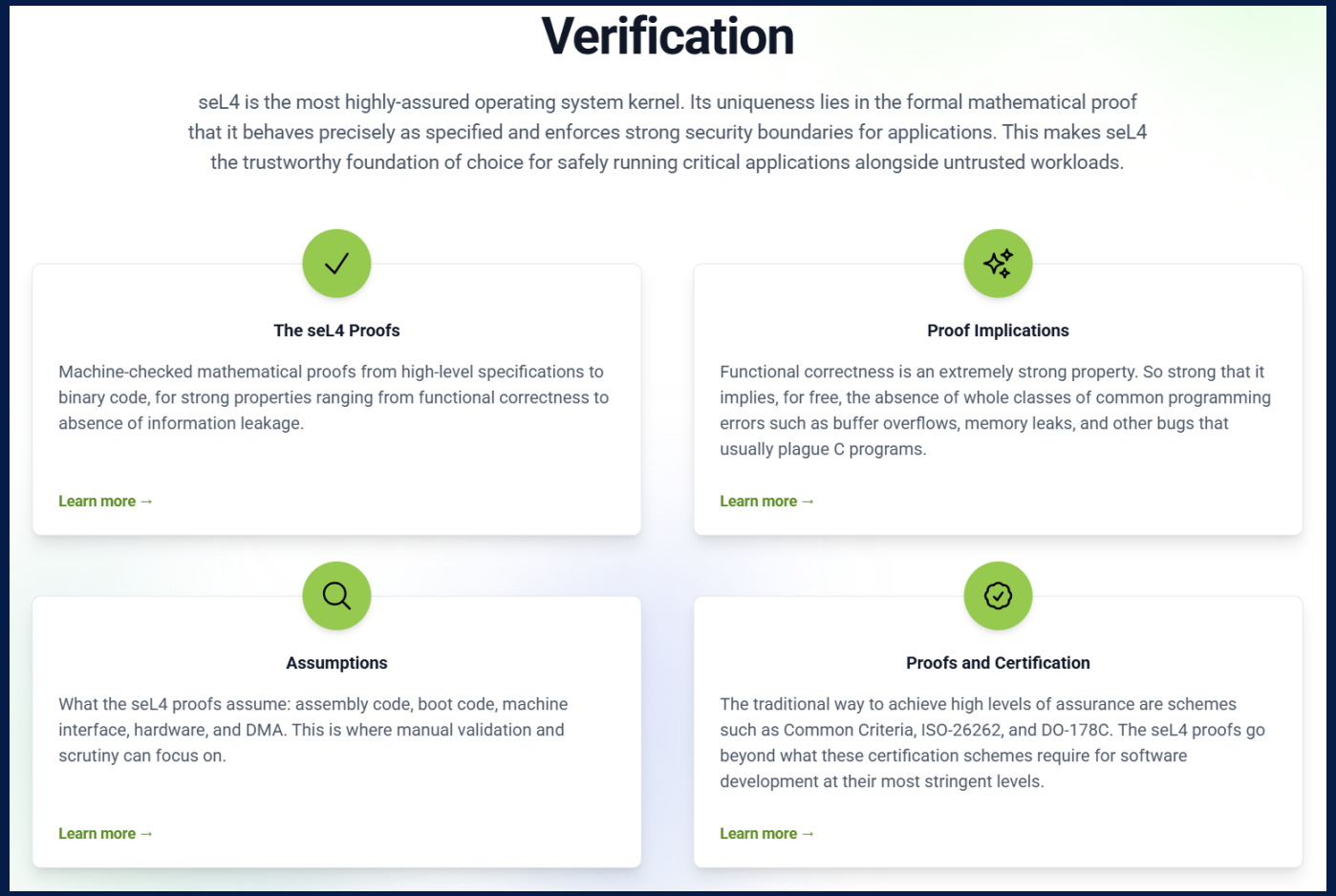
Formal Guarantees and Assurance

- Use of seL4 allows system level development and reasoning
- Promotes holistic approach to system design and analysis

- Similar to other formal analysis techniques
- Allows you to shift assurance burden around your system
- Can better target your assurance to focus on assumptions and less provably correct components

National Cyber Security Centre
a part of GCHQ

Clear Assumptions Vital



Verification

seL4 is the most highly-assured operating system kernel. Its uniqueness lies in the formal mathematical proof that it behaves precisely as specified and enforces strong security boundaries for applications. This makes seL4 the trustworthy foundation of choice for safely running critical applications alongside untrusted workloads.

The seL4 Proofs

Machine-checked mathematical proofs from high-level specifications to binary code, for strong properties ranging from functional correctness to absence of information leakage.

Learn more →

Proof Implications

Functional correctness is an extremely strong property. So strong that it implies, for free, the absence of whole classes of common programming errors such as buffer overflows, memory leaks, and other bugs that usually plague C programs.

Learn more →

Assumptions

What the seL4 proofs assume: assembly code, boot code, machine interface, hardware, and DMA. This is where manual validation and scrutiny can focus on.

Learn more →

Proofs and Certification

The traditional way to achieve high levels of assurance are schemes such as Common Criteria, ISO-26262, and DO-178C. The seL4 proofs go beyond what these certification schemes require for software development at their most stringent levels.

Learn more →

National Cyber Security Centre
a part of GCHQ

Assessing Guarantees

- Investigated guarantees and assumptions they rely on
- Are the gaps mitigable?
- Which conditions/risks are worrying in the real world

- Concluded the conditions are manageable
- Understand where systems relying on seL4 can be deployed

National Cyber Security Centre
a part of GCHQ

Proposal Accepted

- Worked with vendor to build device
- Long assurance process, discussed at seL4 Summit in 2023
- Thousands now deployed across multiple UK government departments
- Remains the only device assured to deal with UK data this sensitive exclusively in software.

National Cyber Security Centre
a part of GCHQ

In For The Long Haul

National Cyber Security Centre
a part of GCHQ

Technology Resilience

- High assurance devices tend to have long lives
- Ensuring technology they're based on persists is important
- A healthy ecosystem around a technology is hugely beneficial
  - More investment
  - More innovation
  - More options

National Cyber Security Centre
a part of GCHQ

Ecosystem Investment

- NCSC has invested in seL4 ecosystem over last few years
- Idea is to help seL4 community be self sustaining
- Open source funding model

- Good for NCSC, seL4 and wider community

National Cyber Security Centre
a part of GCHQ

NCSC Ecosystem Funding

- AARCH64 proofs
- seL4 Dev Kit
- Development of MicroKit
- seL4 x CHERI
- Website and documentation updates

National Cyber Security Centre
a part of GCHQ

What Are We Working On?

National Cyber Security Centre
a part of GCHQ

What Else Are We Using seL4 For?

- Very happy with our first project
- Understanding and awareness of seL4 raised
- Identified other use cases where seL4 offers specific benefit

National Cyber Security Centre
a part of GCHQ

Removable Media is a Problem

- Data transfer across classification boundaries needs to be tightly controlled
- Data import/export is necessary, but comes with obvious risks
- These systems must be carefully designed with strong guarantees of information flow

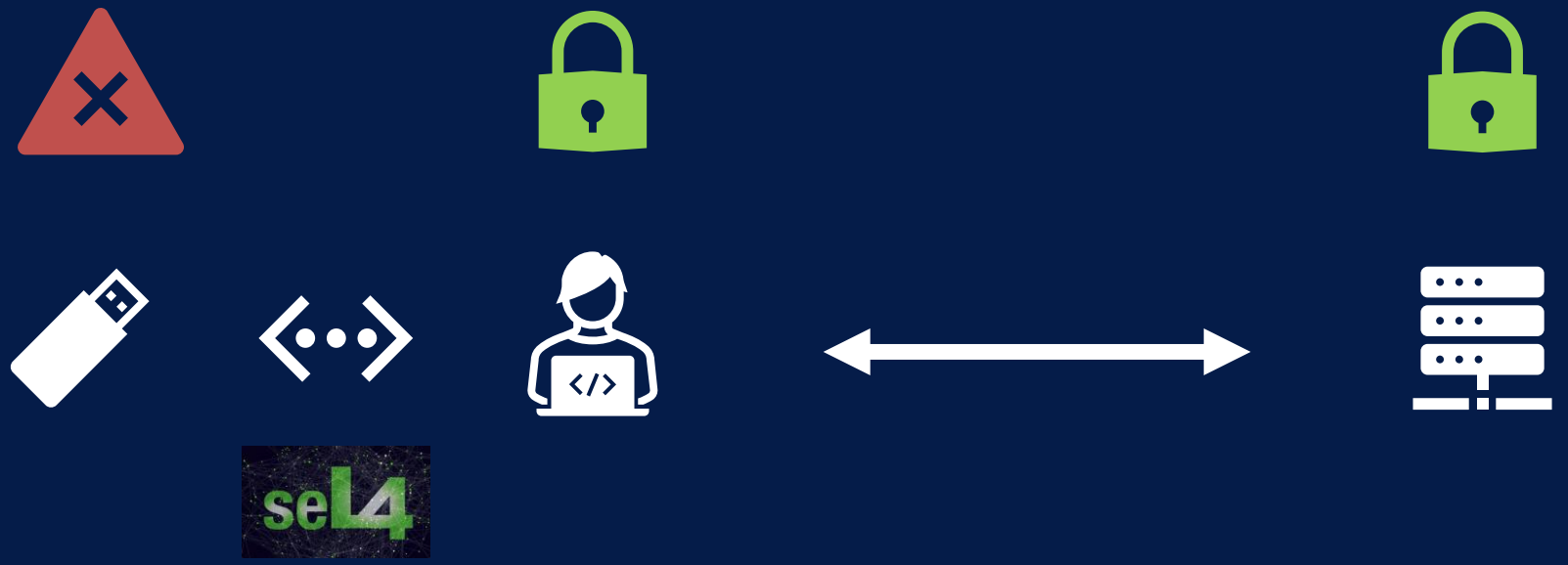
National Cyber Security Centre
a part of GCHQ

Classified Data Import/Export Device

- NCSC has supported UK industry to build a data import/export device that:
  - Is highly portable
  - Enables safe over the network transfer of data
  - Allows user to plug removable media into existing trusted IT infrastructure
  - Will form part of wider cross domain architecture

National Cyber Security Centre
a part of GCHQ

Classified Data Import/Export Device



National Cyber Security Centre
a part of GCHQ

Why, and Why seL4?

- Previous solutions required standalone, expensive form factor
- seL4 allows safe isolation of untrusted media in portable form factor
- Provides confidence to connect untrusted media to existing trusted IT infrastructure
- No fear of local device, or wider network compromise

National Cyber Security Centre
a part of GCHQ

Is seL4 Just for High Assurance?

- We've been involved with seL4 since 2016
- In 2026, we see a much healthier, accessible technology and ecosystem
- More interest and awareness
- More concrete projects using seL4 publicly
- More usability

National Cyber Security Centre
a part of GCHQ

Wider use cases for seL4

- More usability/accessibility opens door for more real-world deployments of seL4
- seL4 OS makes cost/benefit equation much more favourable

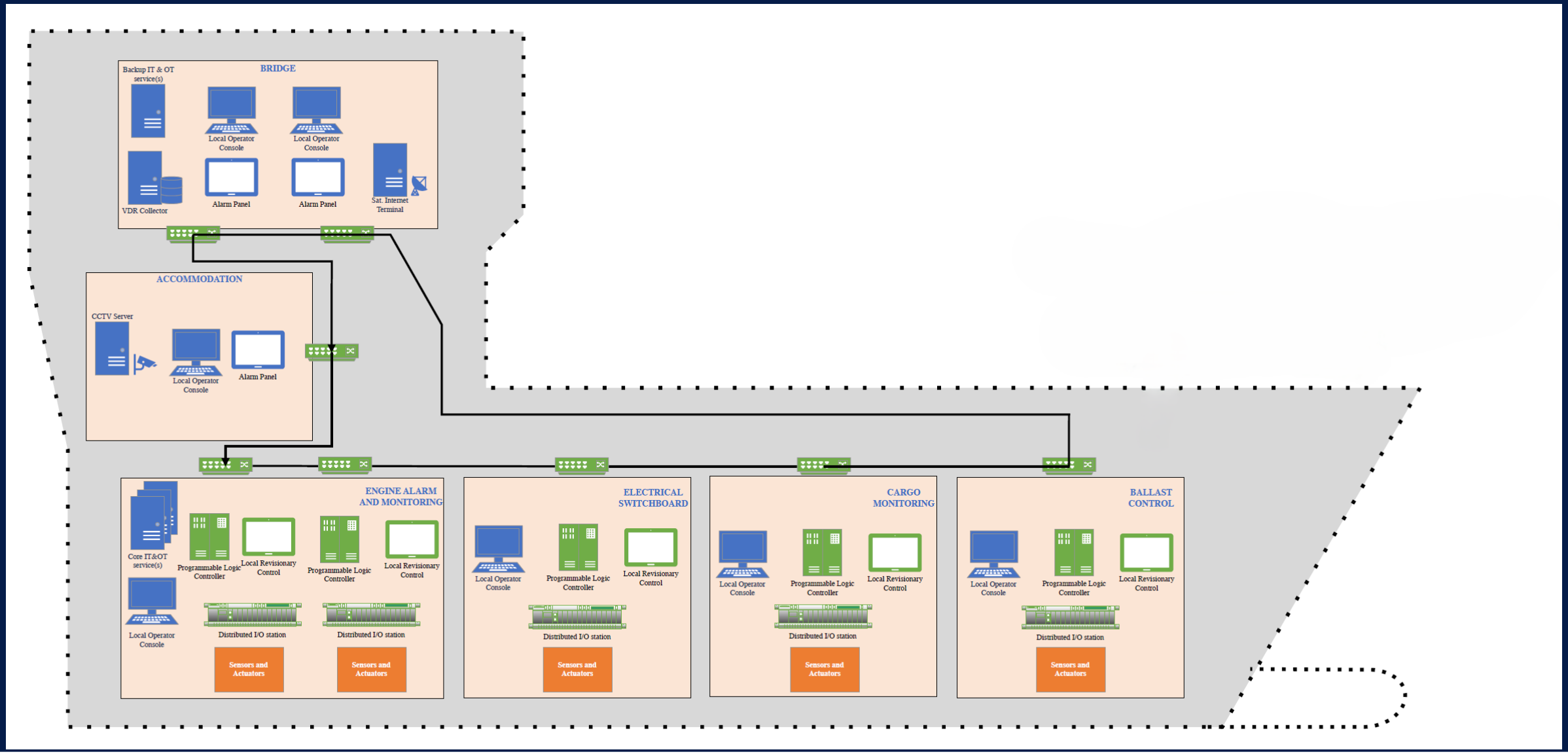
- We see aging infrastructure asking for wider connectivity
- Providing information flow guarantees can help mitigate some of these risks

National Cyber Security Centre
a part of GCHQ

Exploring seL4 for Infrastructure

- seL4 raises floor for security
- What benefits does an seL4 based maritime ICS system offer?
- Wanted to explore development on top of seL4 based OS
- Partnered with Kry10 to build KMIDS (**K**ry10 **M**aritime **I**CS **D**emonstration **S**cenario)

National Cyber Security Centre
a part of GCHQ

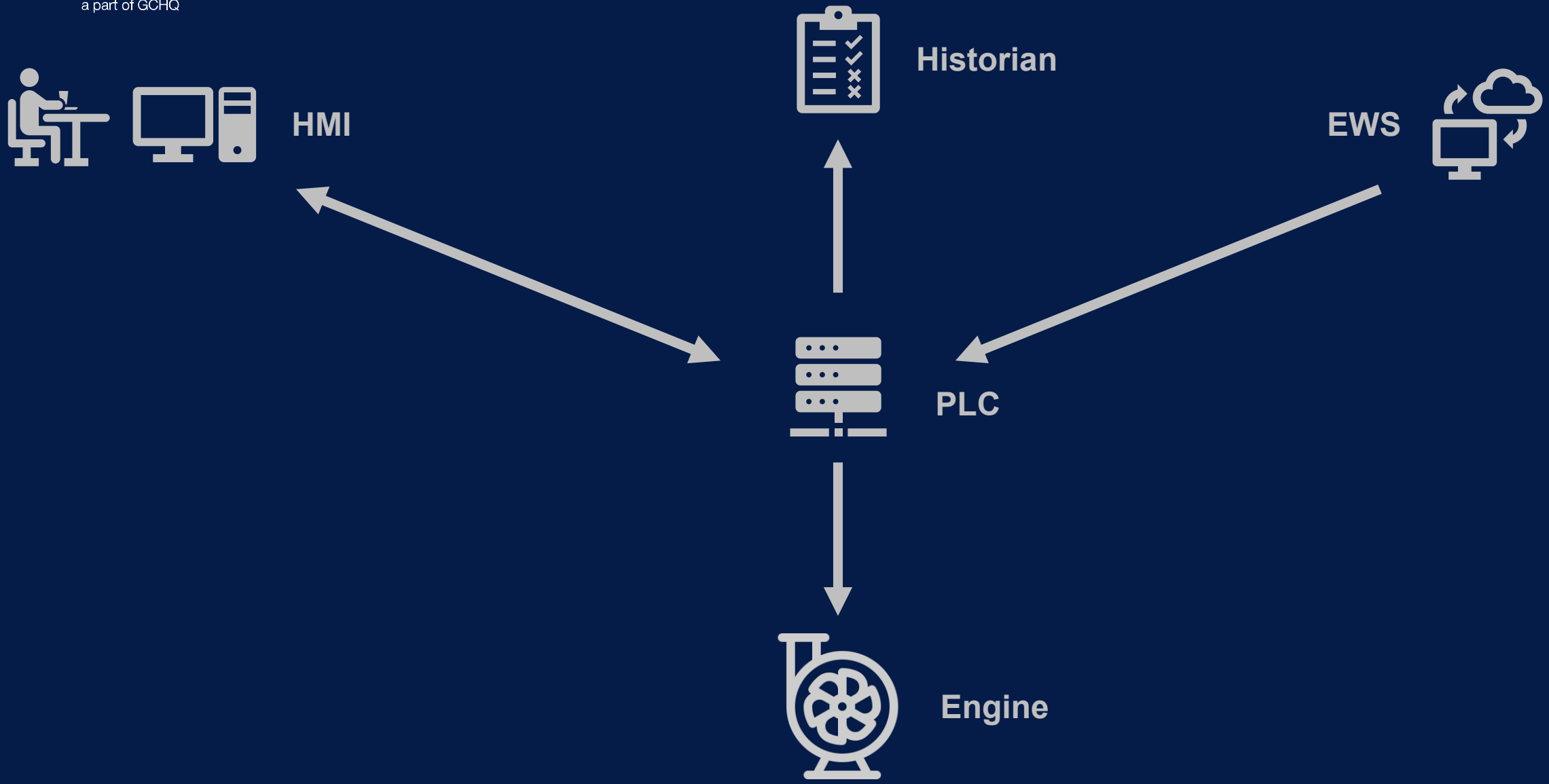


National Cyber Security Centre
a part of GCHQ

KMIDS

- Maritime ICS demo focussed on Engine and Alarm system
- Designed to replicate real world deployment as closely as possible for testing purposes.
- Aimed to be a drop-in replacement for current MOD systems
- Retroactive, system defined, security uplift
- Enables features not previously permitted

National Cyber Security Centre
a part of GCHQ



National Cyber Security Centre
a part of GCHQ

Live Testing

- Deployed in MOD's Simulation testing environment

National Cyber Security Centre
a part of GCHQ

What Does The Future Hold?

National Cyber Security Centre
a part of GCHQ

What Next?

- Brief roundup of some of our work with seL4 over the last decade
- We have several other projects internally
- Proud to be part of the seL4 community
- Excited for the future

National Cyber Security Centre
a part of GCHQ

Greater Adoption

- Greater uptake of seL4 good for community
- The more developer friendly, the better
- Industry partners have a decade of experience
- Valuable feedback to improve developer experience
- Collated experience and views

National Cyber Security Centre
a part of GCHQ

Industry Feedback

- Multi-Core/Multi-Kernel
  - Needs to have communication overhead built in
- Optimistic on emerging OSs
  - More mature development environment desired
- Developer friendly practices
  - Advance warning on new releases
  - Comprehensive release notes
  - Improved debug features

National Cyber Security Centre
a part of GCHQ

seL4 and AI

- AI deeply powerful capability
- Needs strong isolation to limit scope
- Numerous cases of AI escaping sandboxes thought secure

- Use seL4 based systems to enforce this isolation?

National Cyber Security Centre
a part of GCHQ

Conclusion

- The NCSC has been involved with seL4 for 10 years
- Proud to have been part of seL4's history
- Have built and deployed systems based on seL4 to protect UK's National Security
- We think seL4 a unique tool with guarantees that help build secure real-world systems
- Excited for what can be achieved going forward