Applus+ IDIADA

Beam Connectivity

CATAPULT
Compound Semiconductor Applications

University of Exeter

Swansea University
Prifysgol Abertawe

The Next Steps in Security for Connected Vehicles

Rob Potter
Chief Technology Officer
Beam Connectivity

Cyber security headwinds

Secure hardware foundations: CHERI

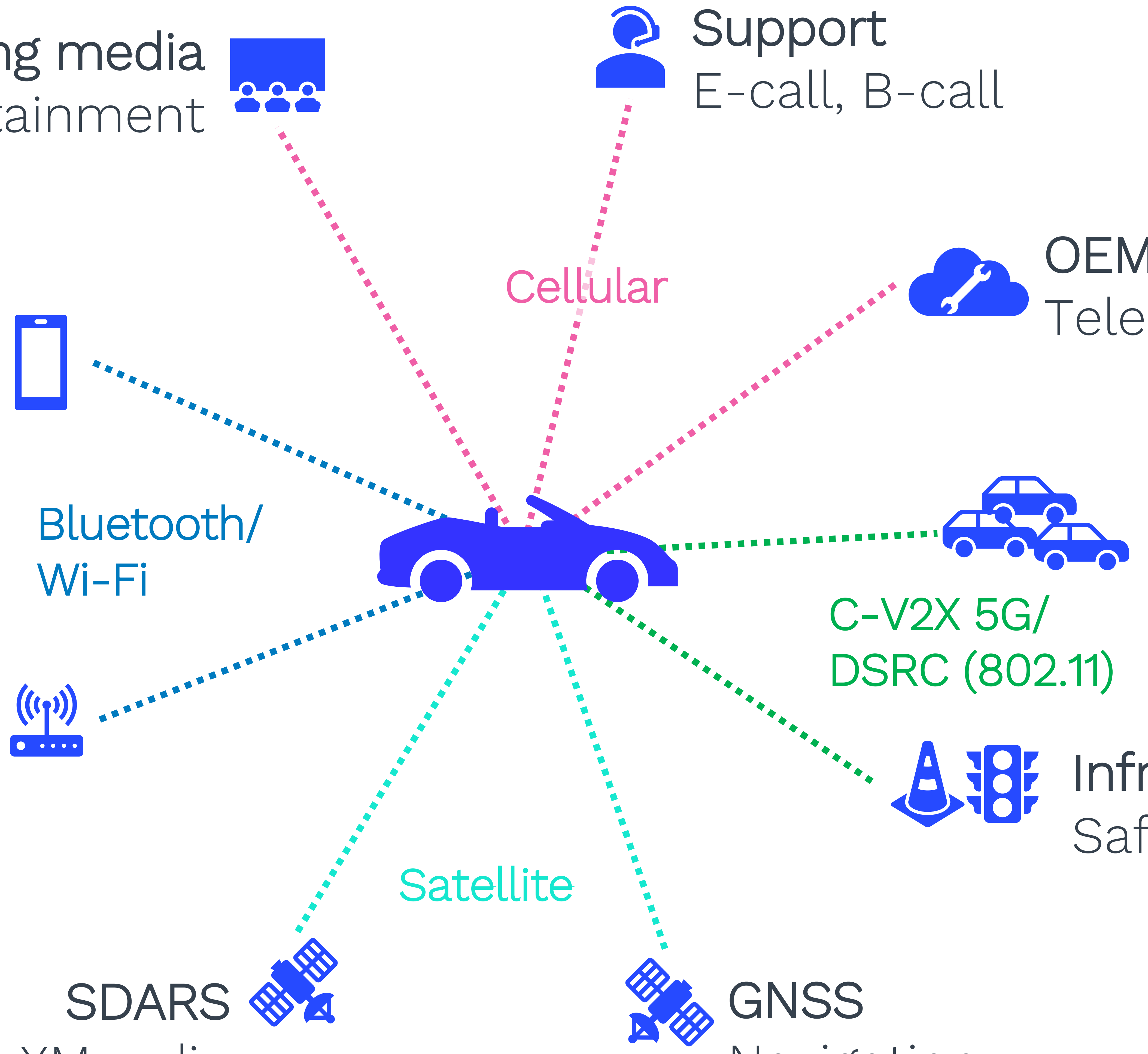
Project AutoCHERI

Cyber security headwinds

Secure hardware foundations: CHERI

Project AutoCHERI

Variety of wireless attack vectors



Internet streaming media
Infotainment

Support
E-call, B-call

Cellular

OEM cloud
Telematics, health, mobile app

Occupant's mobile
Media, Android Auto, Apple CarPlay, Baidu CarLife

Bluetooth/
Wi-Fi

Vehicles (V2V)
Safety, efficiency

C-V2X 5G/
DSRC (802.11)

Home/office/charge point Wi-Fi
SOTA updates, smart home

Infrastructure (V2I)
Safety, efficiency

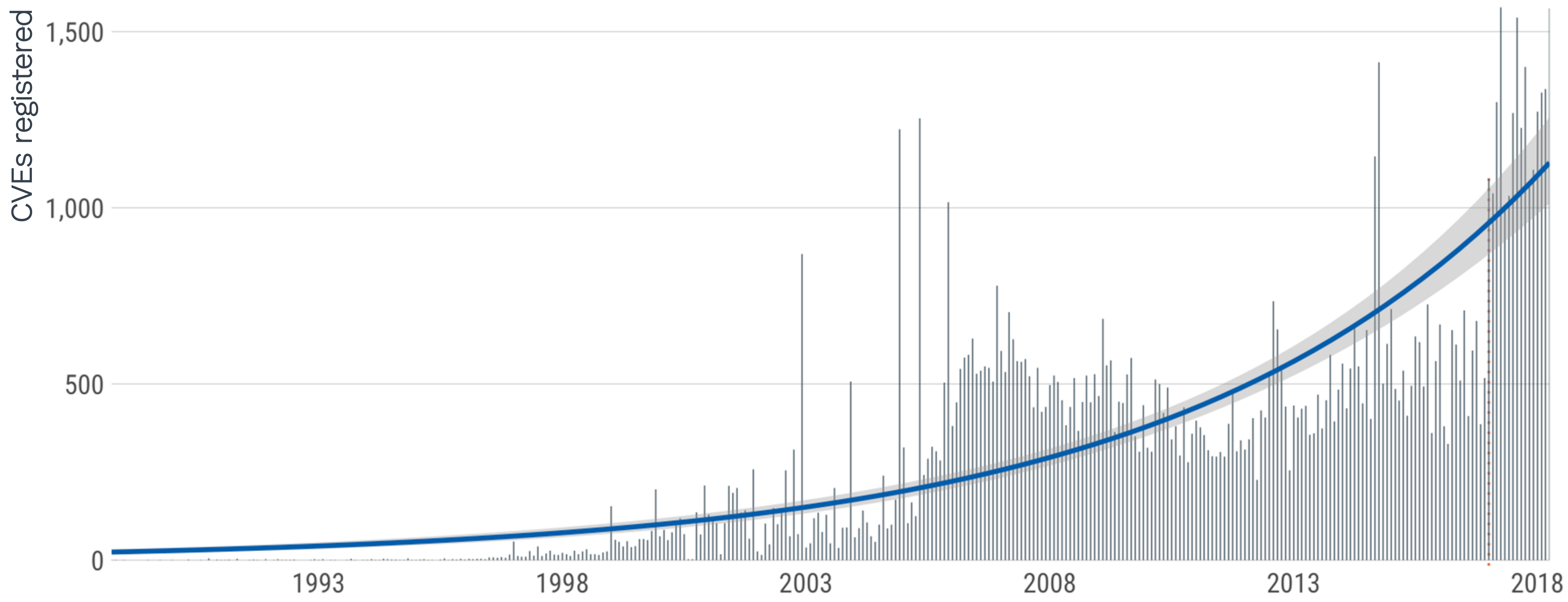
Satellite

SDARS
SiriusXM radio

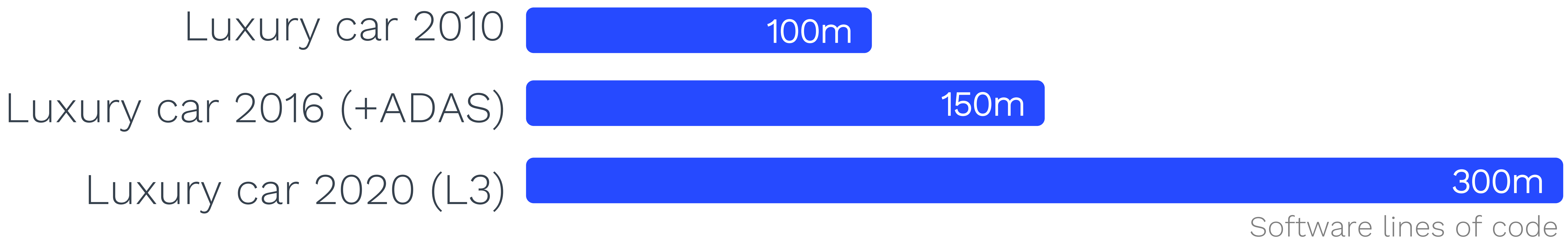
GNSS
Navigation

Increasingly challenging security landscape

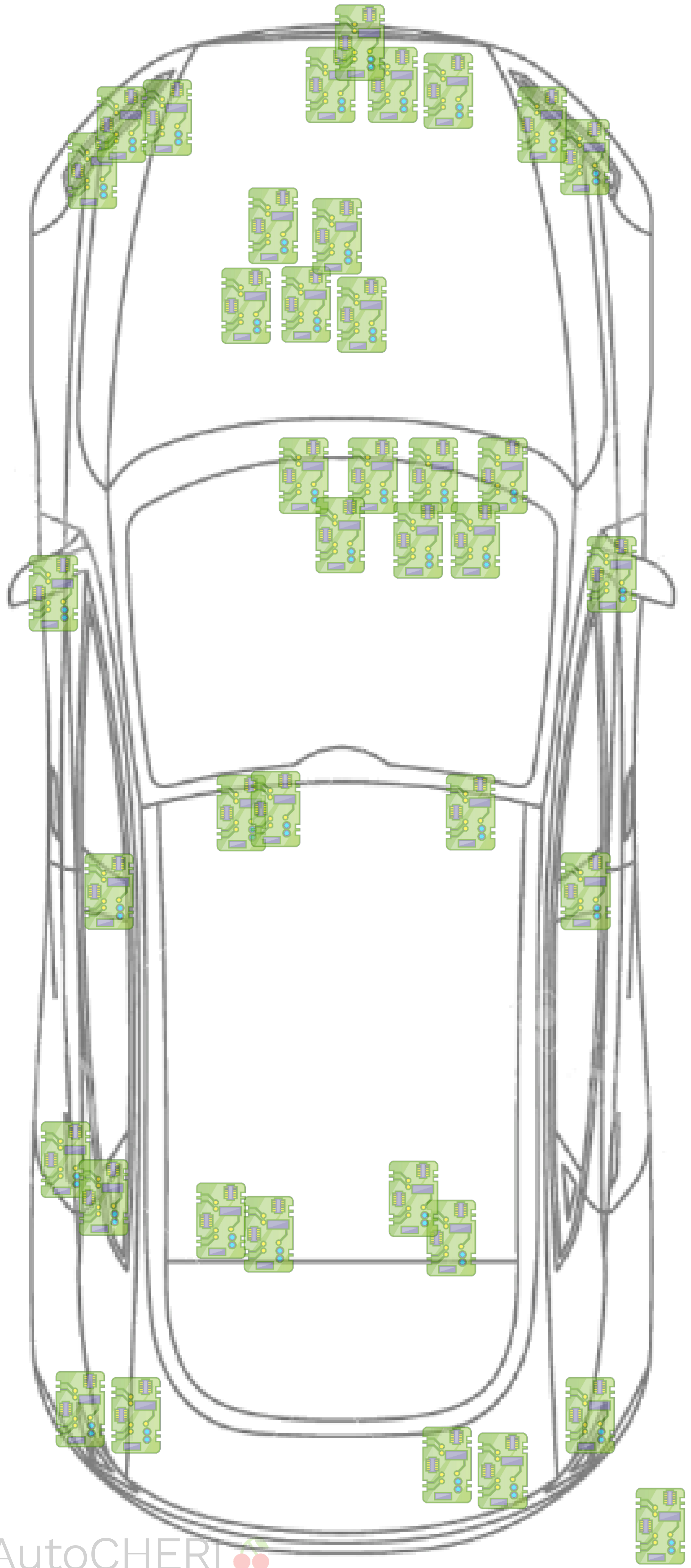
- System complexity
- Software complexity
- Supply chain disruption
- Vulnerabilities found
- Geo-political tensions



Data compiled from MITRE, NVD and Rapid7
https://www.rapid7.com/blog/post/2018/04/30/cve-100k-by-the-numbers



Vehicle architecture evolution



🟩 Electronic Control Unit (ECU)

Today: 100+ legacy compute nodes

- One ECU per function, e.g. windows, locks, heated seats
- Connected via simple networking: CAN, LIN, FlexRay

Tomorrow: High performance compute nodes

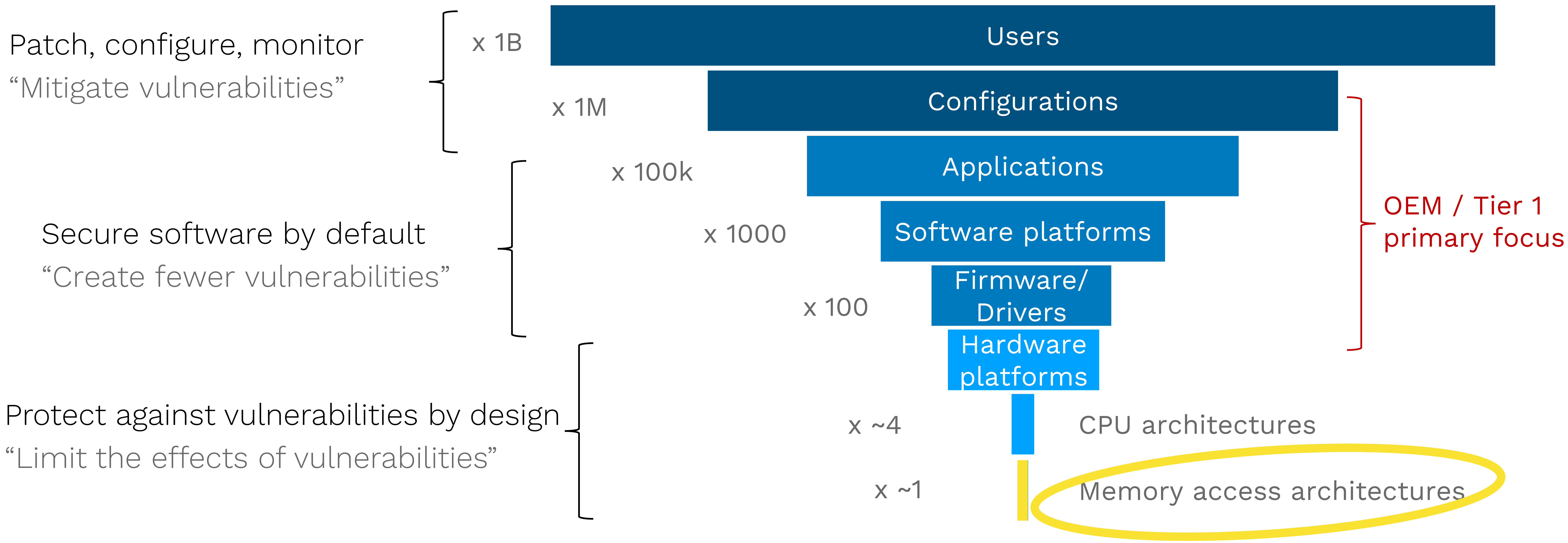
- Consolidate into fewer, centralised nodes
- More powerful, shared compute nodes
- Variety of cyber critical & performance sensitive workloads
- Need isolation via hypervisor technologies

Cyber security headwinds

Secure hardware foundations: CHERI

Project AutoCHERI

The Cyber Pyramid – Fixing the foundations



Patch, configure, monitor
“Mitigate vulnerabilities”

Secure software by default
“Create fewer vulnerabilities”

Protect against vulnerabilities by design
“Limit the effects of vulnerabilities”

Innovation: CHERI

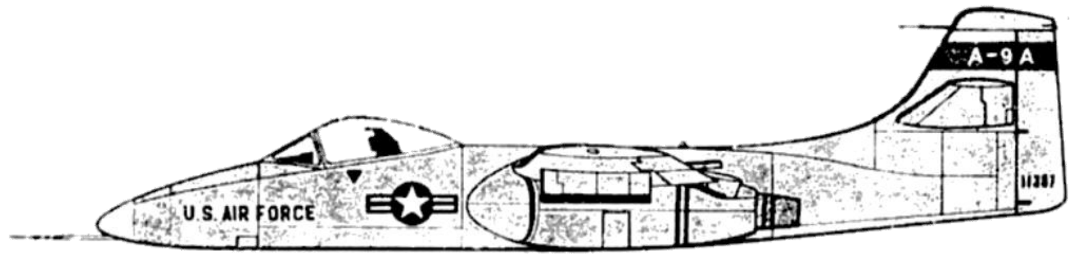
AutoCHERI

Credit: Agata Samojlowicz, DSbD Deputy Challenge Director, Innovate UK

Memory safety

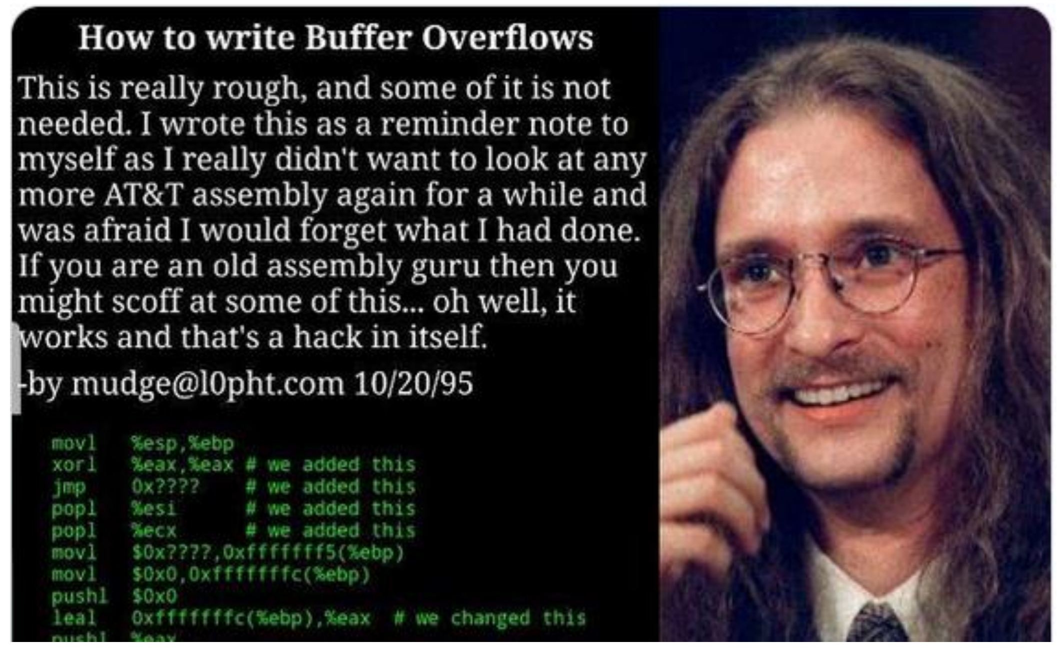
1972

October 1972: USAF study first described a memory safety vulnerability



1996

Aleph One’s seminal article is published: ‘Smashing the Stack for Fun and Profit’



How to write Buffer Overflows

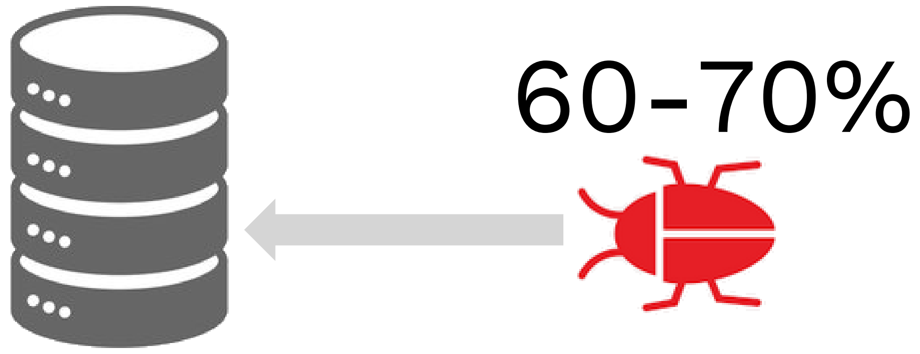
This is really rough, and some of it is not needed. I wrote this as a reminder note to myself as I really didn't want to look at any more AT&T assembly again for a while and was afraid I would forget what I had done. If you are an old assembly guru then you might scoff at some of this... oh well, it works and that's a hack in itself.

-by mudge@l0pht.com 10/20/95

```
movl   %esp,%ebp
xorl   %eax,%eax # we added this
jmp    0x????    # we added this
popl   %esi      # we added this
popl   %ecx      # we added this
movl   $0x????,0xfffffff5(%ebp)
movl   $0x0,0xfffffffc(%ebp)
pushl  $0x0
leal   0xfffffffc(%ebp),%eax  # we changed this
pushl  %eax
```

2022

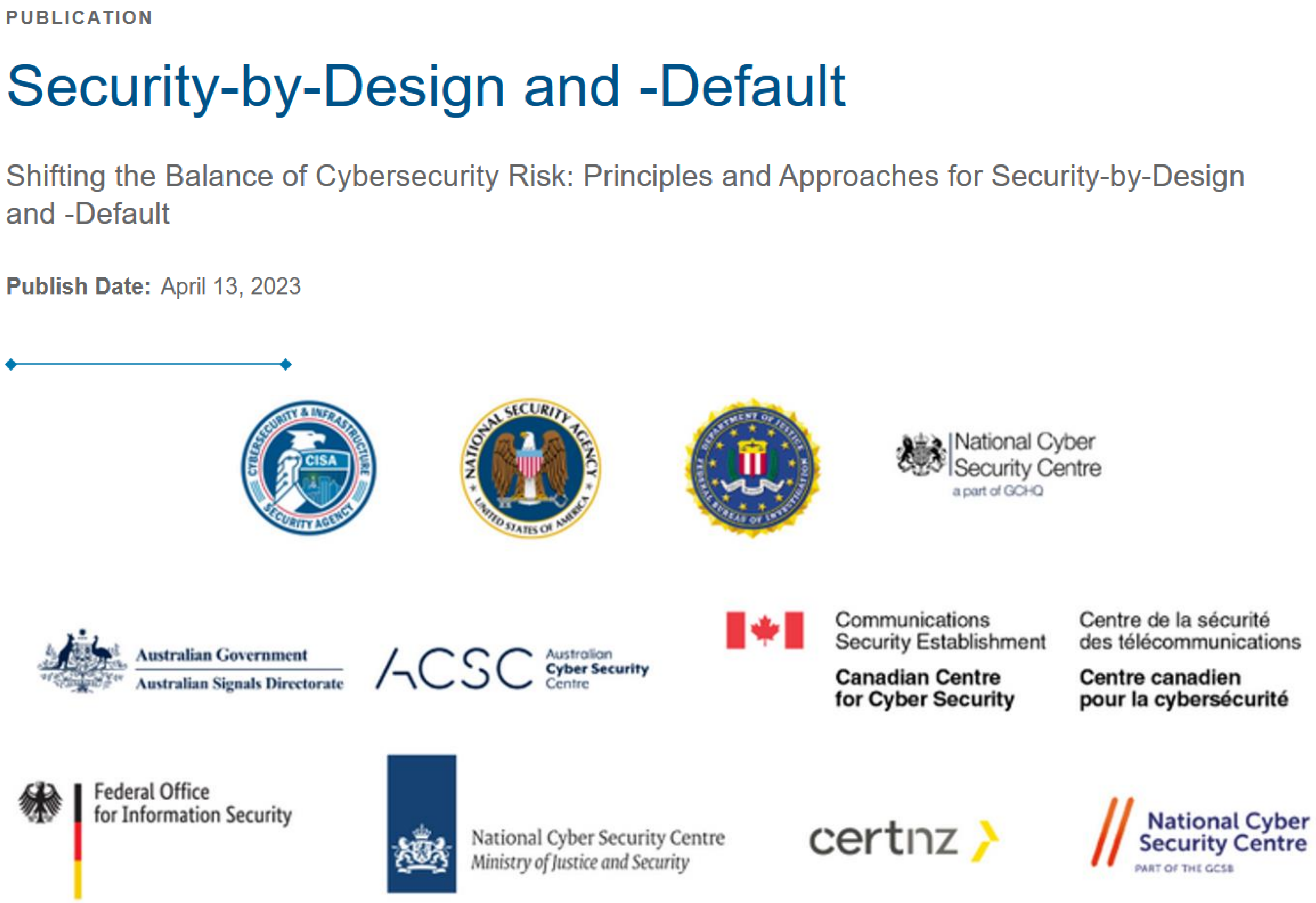
In Q1 over 400 memory safety vulnerabilities reported to the National Vulnerability Database



CVE-2022-42431 – Tesla Model 3

- *Flaw exists within the bcmdhd driver (Broadcom Bluetooth).*
- *Lack of proper validation of the length of user-supplied data prior to copying it to a buffer.*
- *CWE-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)*

CHERI: Recommended in US, UK & others



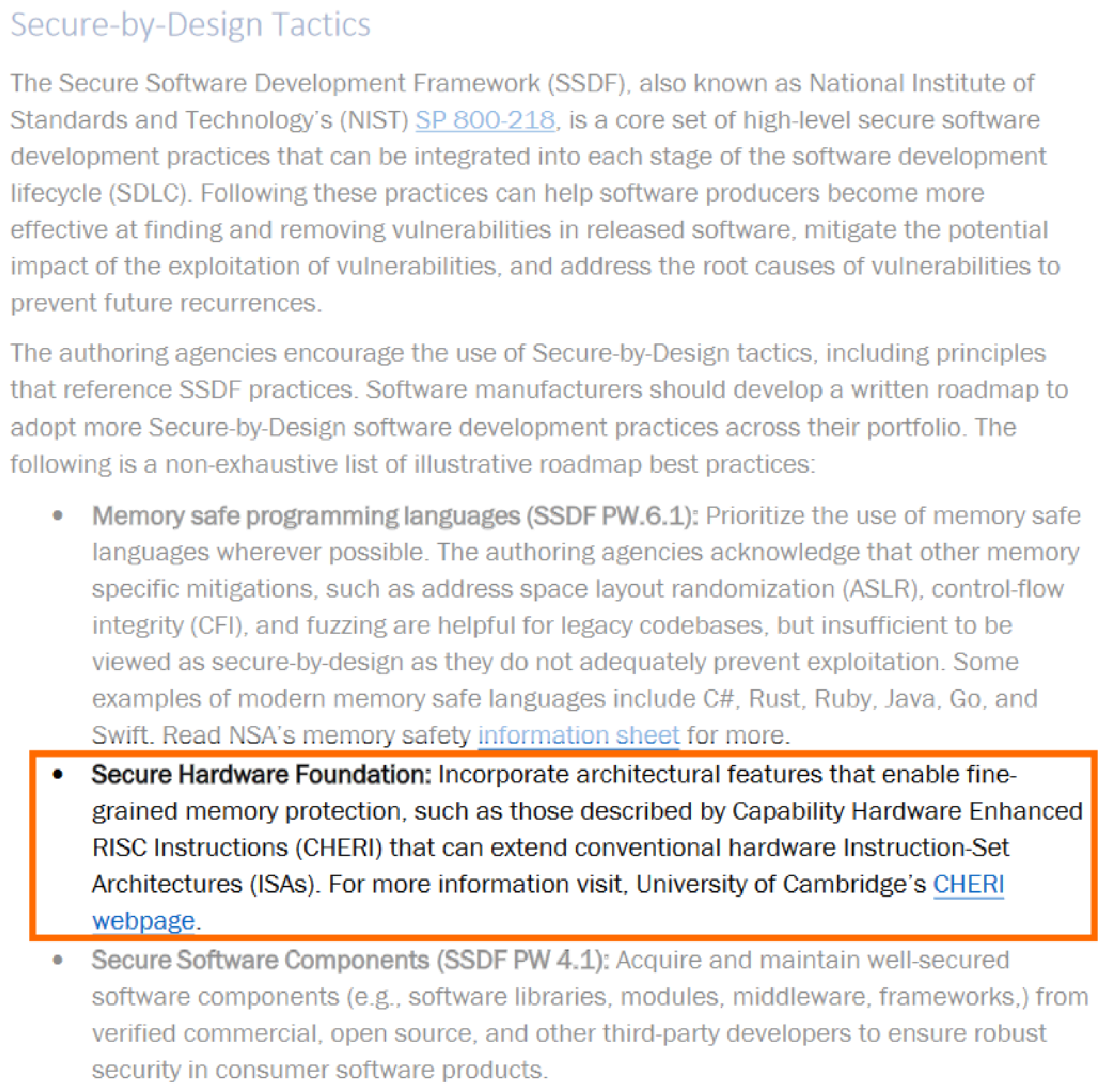
PUBLICATION

Security-by-Design and -Default

Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-by-Design and -Default

Publish Date: April 13, 2023

National Cyber Security Centre
a part of GCHQ
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre
Communications Security Establishment
Canadian Centre for Cyber Security
Centre de la sécurité des télécommunications
Centre canadien pour la cybersécurité
Federal Office for Information Security
National Cyber Security Centre
Ministry of Justice and Security
certnz
National Cyber Security Centre
PART OF THE GCSB



Secure-by-Design Tactics

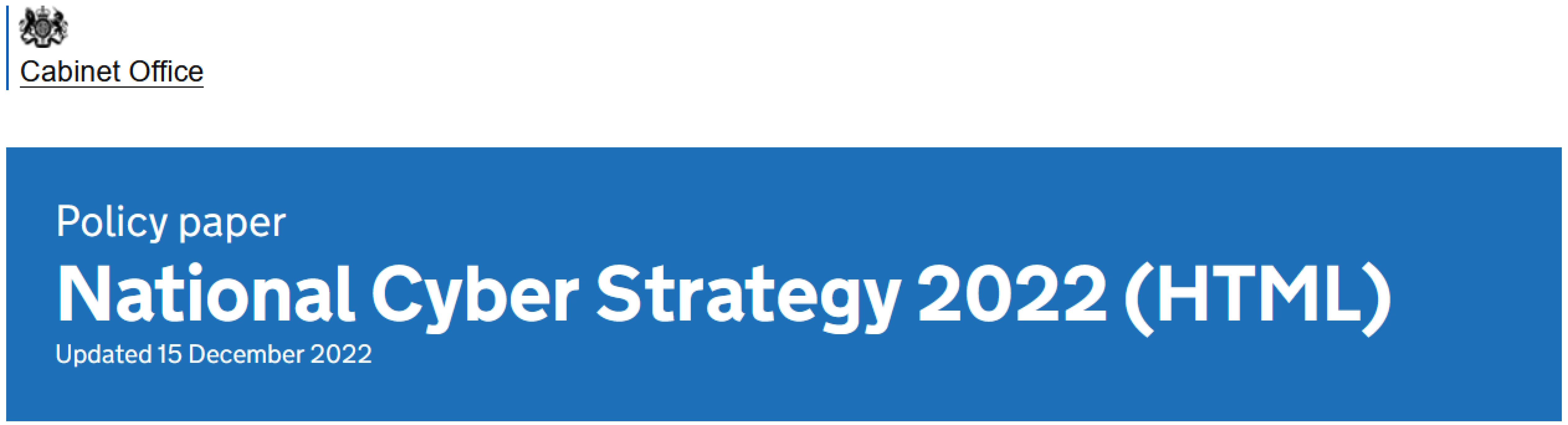
The Secure Software Development Framework (SSDF), also known as National Institute of Standards and Technology's (NIST) SP 800-218, is a core set of high-level secure software development practices that can be integrated into each stage of the software development lifecycle (SDLC). Following these practices can help software producers become more effective at finding and removing vulnerabilities in released software, mitigate the potential impact of the exploitation of vulnerabilities, and address the root causes of vulnerabilities to prevent future recurrences.

The authoring agencies encourage the use of Secure-by-Design tactics, including principles that reference SSDF practices. Software manufacturers should develop a written roadmap to adopt more Secure-by-Design software development practices across their portfolio. The following is a non-exhaustive list of illustrative roadmap best practices:

- **Memory safe programming languages (SSDF PW.6.1):** Prioritize the use of memory safe languages wherever possible. The authoring agencies acknowledge that other memory specific mitigations, such as address space layout randomization (ASLR), control-flow integrity (CFI), and fuzzing are helpful for legacy codebases, but insufficient to be viewed as secure-by-design as they do not adequately prevent exploitation. Some examples of modern memory safe languages include C#, Rust, Ruby, Java, Go, and Swift. Read NSA's memory safety information sheet for more.
- **Secure Hardware Foundation:** Incorporate architectural features that enable fine-grained memory protection, such as those described by Capability Hardware Enhanced RISC Instructions (CHERI) that can extend conventional hardware Instruction-Set Architectures (ISAs). For more information visit, University of Cambridge's CHERI webpage.
- **Secure Software Components (SSDF PW 4.1):** Acquire and maintain well-secured software components (e.g., software libraries, modules, middleware, frameworks,) from verified commercial, open source, and other third-party developers to ensure robust security in consumer software products.

https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default

CHERI: Recommended in US, UK & others

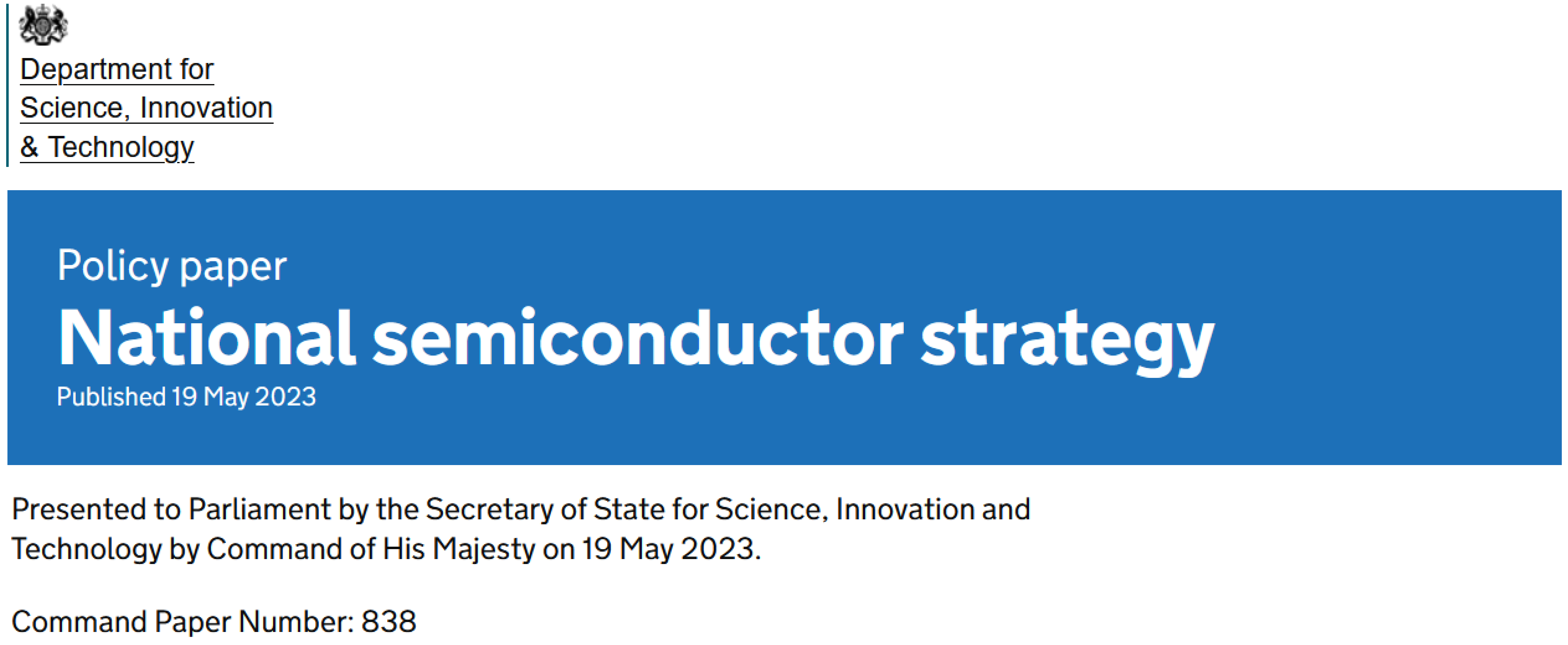


Cabinet Office

Policy paper

National Cyber Strategy 2022 (HTML)

Updated 15 December 2022



Department for Science, Innovation & Technology

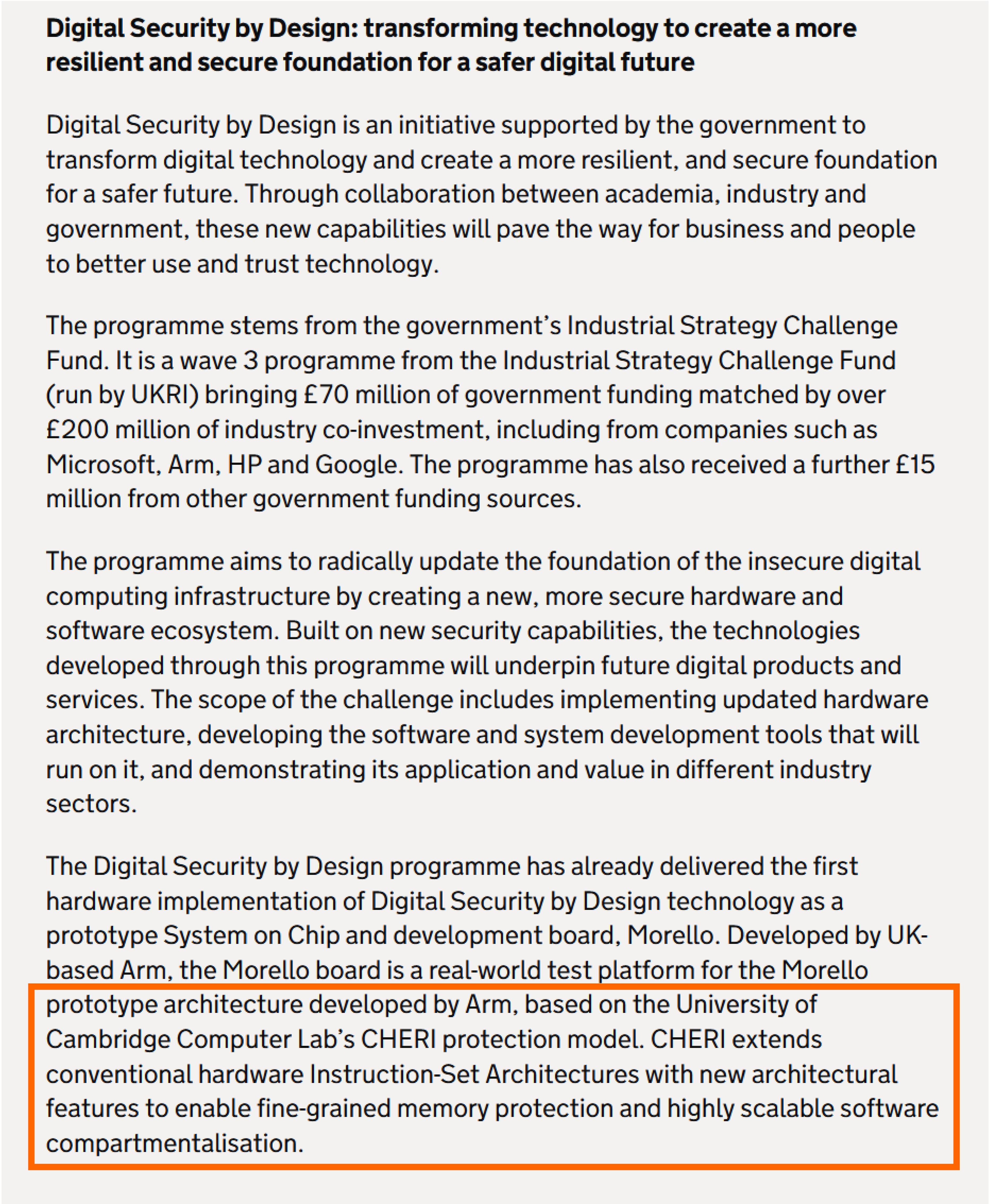
Policy paper

National semiconductor strategy

Published 19 May 2023

Presented to Parliament by the Secretary of State for Science, Innovation and Technology by Command of His Majesty on 19 May 2023.

Command Paper Number: 838



Digital Security by Design: transforming technology to create a more resilient and secure foundation for a safer digital future

Digital Security by Design is an initiative supported by the government to transform digital technology and create a more resilient, and secure foundation for a safer future. Through collaboration between academia, industry and government, these new capabilities will pave the way for business and people to better use and trust technology.

The programme stems from the government's Industrial Strategy Challenge Fund. It is a wave 3 programme from the Industrial Strategy Challenge Fund (run by UKRI) bringing £70 million of government funding matched by over £200 million of industry co-investment, including from companies such as Microsoft, Arm, HP and Google. The programme has also received a further £15 million from other government funding sources.

The programme aims to radically update the foundation of the insecure digital computing infrastructure by creating a new, more secure hardware and software ecosystem. Built on new security capabilities, the technologies developed through this programme will underpin future digital products and services. The scope of the challenge includes implementing updated hardware architecture, developing the software and system development tools that will run on it, and demonstrating its application and value in different industry sectors.

The Digital Security by Design programme has already delivered the first hardware implementation of Digital Security by Design technology as a prototype System on Chip and development board, Morello. Developed by UK-based Arm, the Morello board is a real-world test platform for the Morello prototype architecture developed by Arm, based on the University of Cambridge Computer Lab's CHERI protection model. CHERI extends conventional hardware Instruction-Set Architectures with new architectural features to enable fine-grained memory protection and highly scalable software compartmentalisation.

Cyber security headwinds

Secure hardware foundations: CHERI

Project AutoCHERI

Applus⊕ IDIADA

Beam Connectivity

CATAPULT
Compound Semiconductor Applications

University of Exeter

Swansea University
Prifysgol Abertawe

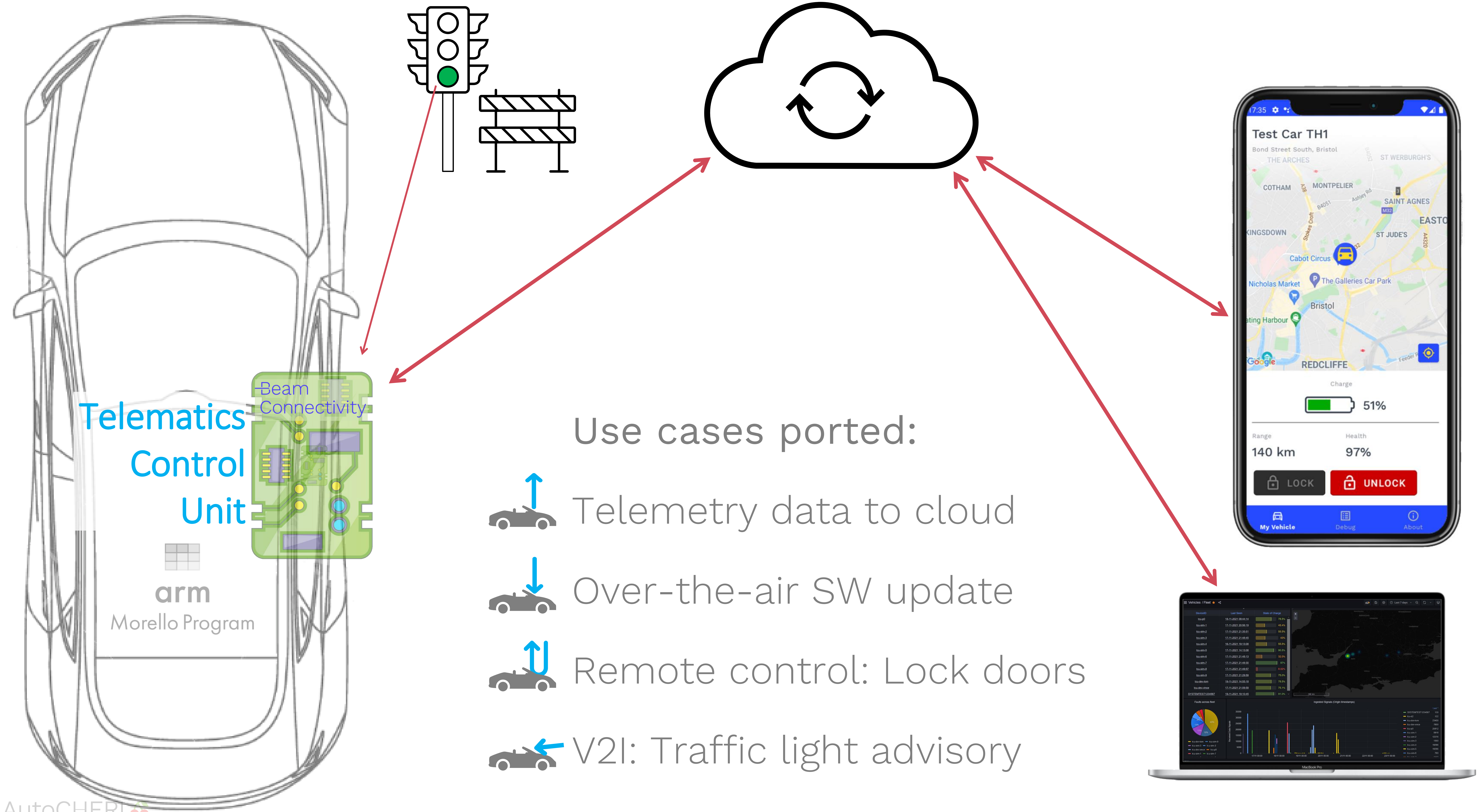
AutoCHERI

https://autocheri.tech

"Understand performance/security trade-off of CHERI[*] for cyber and safety critical automotive applications"

[*] Capability Hardware Enhanced RISC Instructions

arm
Morello Program



Use cases ported:

- Telemetry data to cloud
- Over-the-air SW update
- Remote control: Lock doors
- V2I: Traffic light advisory

AutoCHERI

Project workstreams

✓ Complete
⟳ In-progress
• Up next

Research

- ✓ Functional requirements (V-Model)
- ✓ Threat Assessment & Remediation Analysis (TARA)
- ⟳ CHERI efficacy against automotive threats

Applus+ IDIADA
Beam Connectivity
Swansea University Prifysgol Abertawe

Implementation

- ✓ Port TCU codebase to Morello
- ✓ Implement new features
- ✓ Benchmark and compare
- ⟳ Security testing!

Beam Connectivity
University of Exeter

Market

- ✓ Understand route to market
- ⟳ Understand benefits/ barriers for adoption
- • Align CHERI to automotive regulations

Applus+ IDIADA
CATAPULT Compound Semiconductor Applications

Business case for CHERI in Automotive

- 🔐 More secure software, without a performance impact
- 🗑 Doesn’t require ground-up rewrite of code
- 🐞 Fewer in-field patches, recalls or SW updates
- 📈 Increased productivity of software teams
- ⚖️ Aligned to regulations: UN ECE 155 (cyber) and 156 (SW update)

AutoCHERI

https://autocheri.tech

Learn more: Hall 2, C2-110

Applus IDIADA

Beam Connectivity

CATAPULT
Compound Semiconductor Applications

University of Exeter

Swansea University
Prifysgol Abertawe

arm
Morello Program