cyberagentur

Formally verified IT – Germany’s next cybersecurity paradigm

Dr. Christoph Hof

Prague, 5th September 2025

General introduction

01

Vision

Our WHAT

Cyber security for
the digital sovereignty
of Germany

Mission

Our HOW

We identify, fund and evaluate disruptive research for the day after tomorrow

The Research Strategy of Cyberagentur

Founded in 2020 as an in-house company under the federal government represented jointly by the Federal Ministry of Defence (BMVg) and the Federal Ministry of the Interior and Community (BMI)

The Cyberagentur uniquely combines the ability to …

- work on all research topics that pertain to the wider field of **cybersecurity**
- Directly engage with **national security and defence players** in order to address their future needs and requirements
- Allow pursuance of **high risk / high rewards** research projects
- Identify **disruptive technologies and innovation** early on in order to develop relevant funding opportunities at an early stage

Focus Cybersecurity: our research strategy is aligned with Germany's **National Cyber Security Strategy 2021** (and relevant supporting documents):

- Increase cybersecurity overall for the **state, society and the economy**
- Directly enable governmental agencies with **defensive and offensive** cybersecurity capabilities

Principles of Research Strategy

Principles of Strategic Orientation

Technology maturity	▪ Research projects in application-oriented basic research ▪ TR level 1-4 according to EU definition
Inter-disciplinarity	▪ Identification and commissioning of solutions from different scientific domains
Role	▪ Cyberagentur as project sponsor ▪ Using public procurement law as an instrument ▪ Own assessment and evaluation capability
Claim	▪ Platform for knowledge and experience in the field of cyber security
Demand management	▪ Demand = requirements on the base of the needs-based coordination (priority) ▪ Supply = requirements based on trend analysis
Scope	▪ Commissioning of various players e.g. research institutions, universities, companies, start-ups
Geograph. Frame	▪ Commissioning at national level or in EU or NATO countries
Trans-parency	▪ Providing the results of the projects to the federal government ▪ Publications subject to confidentiality

Agentur für Innovation in der Cybersicherheit GmbH

“Innovation for Cybersecurity”

- Federal R&D agency, launched in 2020
- Goal: DE+EU technological sovereignty
- Basic research: TRL ≤ 4, high risk & gain
- Relevant to interior / exterior security communities!
- Research budget ≈ 88 M€ in 2025 (until 2024 ≈ 60 M€)
- Funding via procurement: 100 % funding + overhead + profit margin / IP license
- Participants from EU, EEA, NATO+JP, KR, AU, NZ, CH
- Results public, unless security risks

cyberagentur

Federal Ministry of the Interior

Federal Ministry of Defence

THE LINUX FOUNDATION

seL4 FOUNDATION

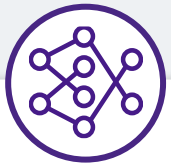
Thematic framework of the Cyberagentur

Key technologies

- Communication of the future
- Cryptology
- Cybersecurity through quantum technologies
- Cybersecurity through AI & for AI
- Autonomous intelligent systems

Secure systems

- Cybersecurity of the Federal Administration
- Critical infrastructure protection
- Cybersecurity in difficult environments
- Secure hardware and supply chains
- Interoperability: digitized files & data fusion



Secure society

- Digital identities
- Cyber-resilient society
- Human-machine interaction
- Cyber-enabled state
- Digital consumer protection

Thematic framework of the Cyberagentur

Key te

- Communic
- Cryptology
- Cybersecu technologi
- Cybersecu
- Autonomo

ction

ction

Project office of the Cyberagentur in Dresden

Planned focus (tbc) on

Trustworthy Technical Value Chains

- Trustworthy IT architectures and supply chains
- Trustworthy communication
- Identities and Consumer Protection in Cyberspace

cyberagentur

More on the Cyberagentur and its unique selling points

02

Program Overview

Key Message: Wide range of research projects covering a broad scientific spectrum

RESEARCH PHASE

- **Au**thentication Using New **Bi**ometric Methods (AuBi)
- Secure Neural **B**rain-**C**omputer-**I**nterfaces (BCI)
- **E**ncrypted **C**omputing (EC)
- Cybersecurity of Critical Infrastructures (HSK)
- **M**obile **Q**uantum **C**omputer (MQC)
- Trustworthy **IT** Ecosystem (EvIT)
- **R**obust & **S**ecure **M**achine **L**earning (RSML)
- **S**ide-**C**hannel **A**ttacks with **Q**uantum **S**ensors (SCA-QS)

CONCEPT PHASE

- Harm Caused by Cybercrime (SCK)

OFFER EVALUATION

- **Au**dio **Fo**rensics for obtaining Location Information (AuFo)
- **F**orensic of **I**ntelligent **S**ystem (FIS*)*
- Cyberagentur Ideas Competition **HAL2025**
- **Mo**bile **In**frastructure: **Lo**cation orientation for **M**obile **A**utonomous **S**ystems (MoIn-LaMAS)
- **S**ide-**c**h**a**nnel resistant **P**ost-**Q**uantum **C**ryptology (SCA4PQC)
- Future Forms of Cybercrime (zCK)
- **H**olistic **e**valuation of **ge**nerative foundation **mo**dels in the security context
- **F**orensic **D**igitalization (FD)

Further approved programs: **5** (ARA, DDK, FoUnD-VR, ZANDER-F, 3S)

Programme: Robust Secure Machine Learning

(Cyber-)Security implications of large, generalizable, and multimodal AI models

Research and development of novel approaches, models, and tools for robust and secure ML processes:

- New mechanisms and architectures for a high degree of robustness and reliability of data, training, and (system) execution
- Modular and end-to-end verification for provable security properties

Abbreviation: RSML

Department : Key Technologies

Division : Cybersecurity through AI & Cybersecurity for AI

Procedure : PCP

Status : Negotiation of phase 3

Automated assurance of data quality

Hybrid models (data-driven/symbolic)

Formal model verification

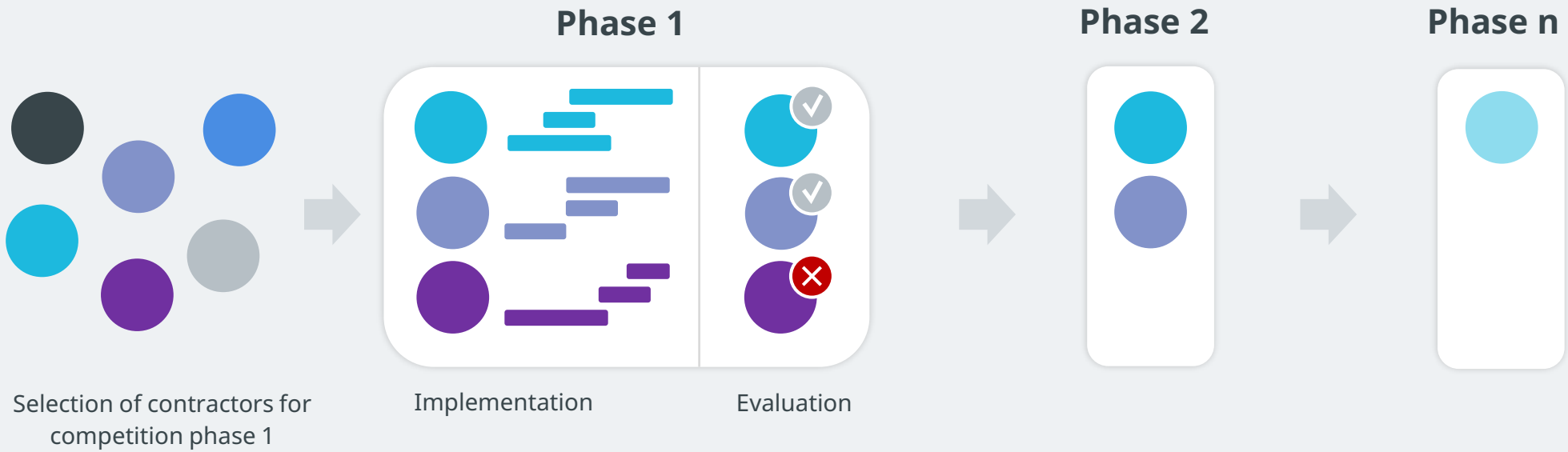
Secure system embedding

Verification via the life cycle

Pre-Commercial Procurement (PCP)

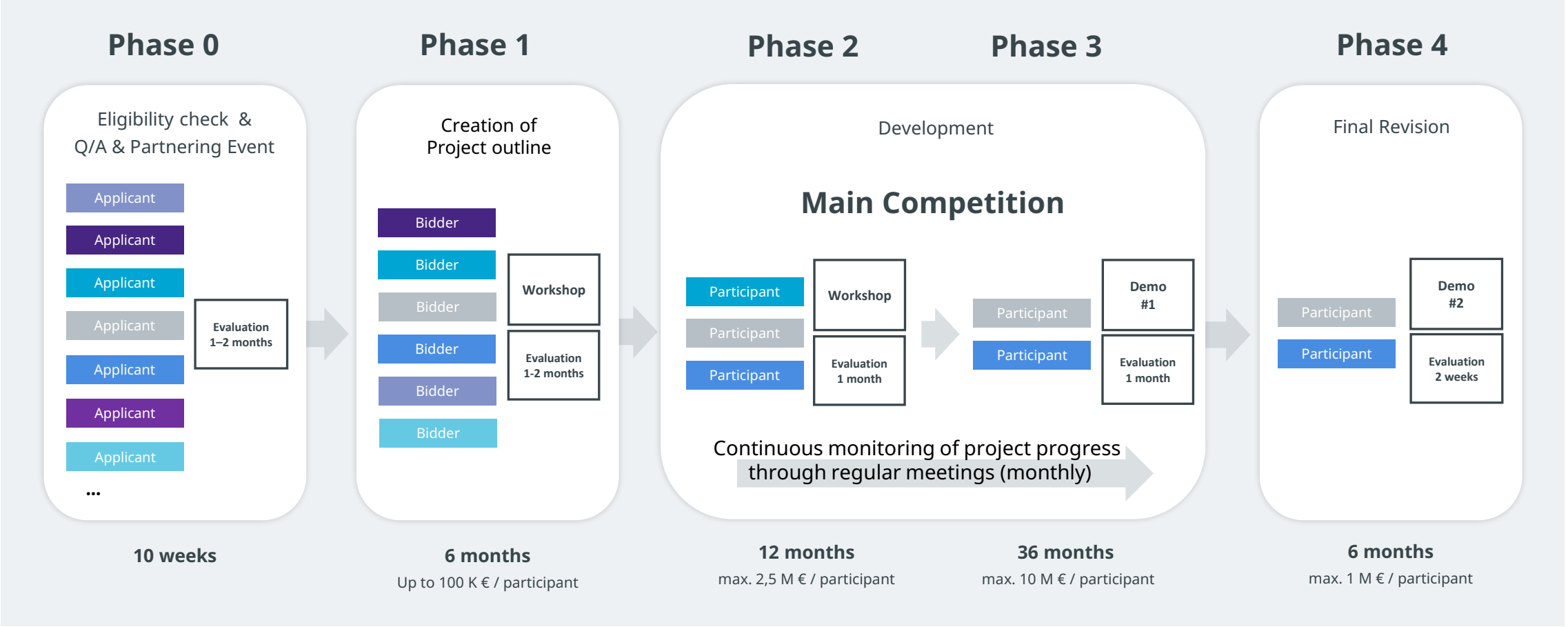
Phase-based pre-commercial (R&I) procurement by public authorities

- Introduced by the European Commission (PCP 2007/1 Issued on June 11, 2007)
- Objective: Strengthening competition in research and development projects
- Procedure:



Competition: Pre Commercial Procurement

Key Message: Increased use of competitive thinking in basic research



cyberagentur

Unique Selling Points

Combination of different scientific fields and thinking out of the box

Funding for research programs that are not considered by venture capitalists

Interdisciplinary / cross-departmental

Driven by future needs of public sector demand

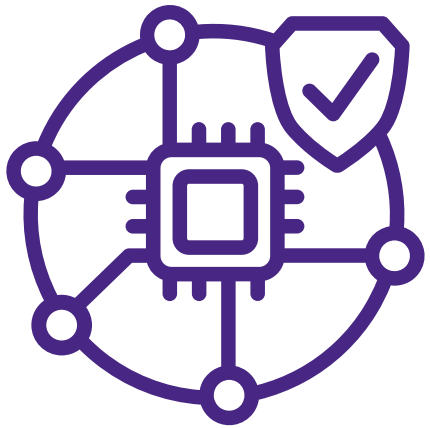
Permission to fail in a high number of cases

Financing of research topics with very high risk

A new paradigm: provable cybersecurity

03

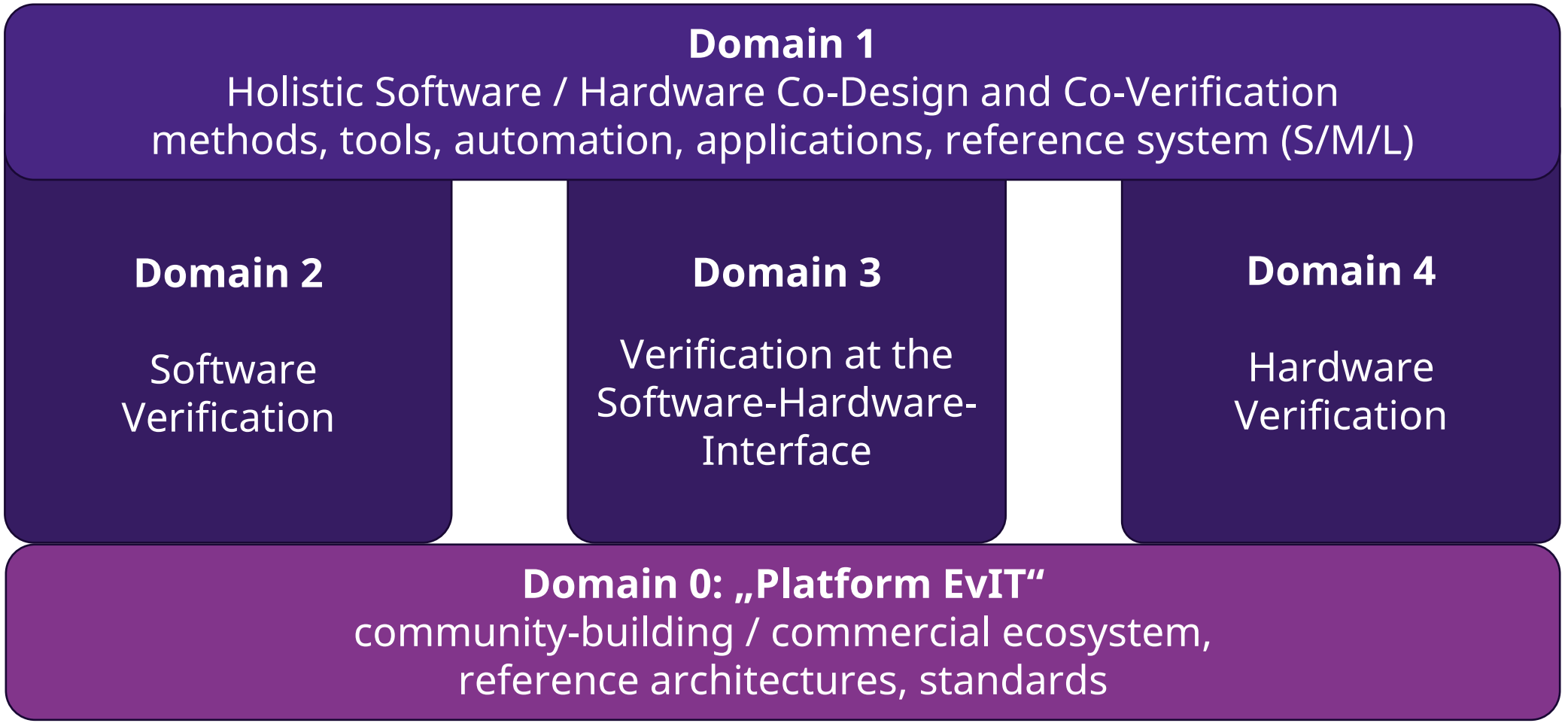
Ecosystem formally verifiable IT (EvIT)



"Provable cybersecurity"

- **Holistic formal verification** of security properties for SW+HW through **co-design and co-verification**
- More **automation** & better scaling of formal methods and tools
- **Verified OS** for multicore (embedded) system; long-term: desktop/server
- Grow **ecosystem** of researchers, commercial providers and users; attract talent into formal verification; spread + create trust via **open source**
- Official project kickoff: 20 January 2025
- 5 projects, 42 million € (gross), 3 or 4 years duration

Program (EvIT) : Research domains



The projects and partners – I: building on seL4

- **Converse - Kry10** (Wellington, NZ) + Proofcraft (Sydney)
  - Multikernel OS with dynamic updates
  - *Matt Brecknell's talk scheduled on Wednesday*

- **PISTIs-V** – PlanV GmbH (Munich) + UNSW Sydney, U Gothenburg
  - Prevention of timing attacks (Spectre/Meltdown) with a special instruction
  - Automation of Driver verification
  - *Gernot Heiser's group's talks scheduled on Wednesday*

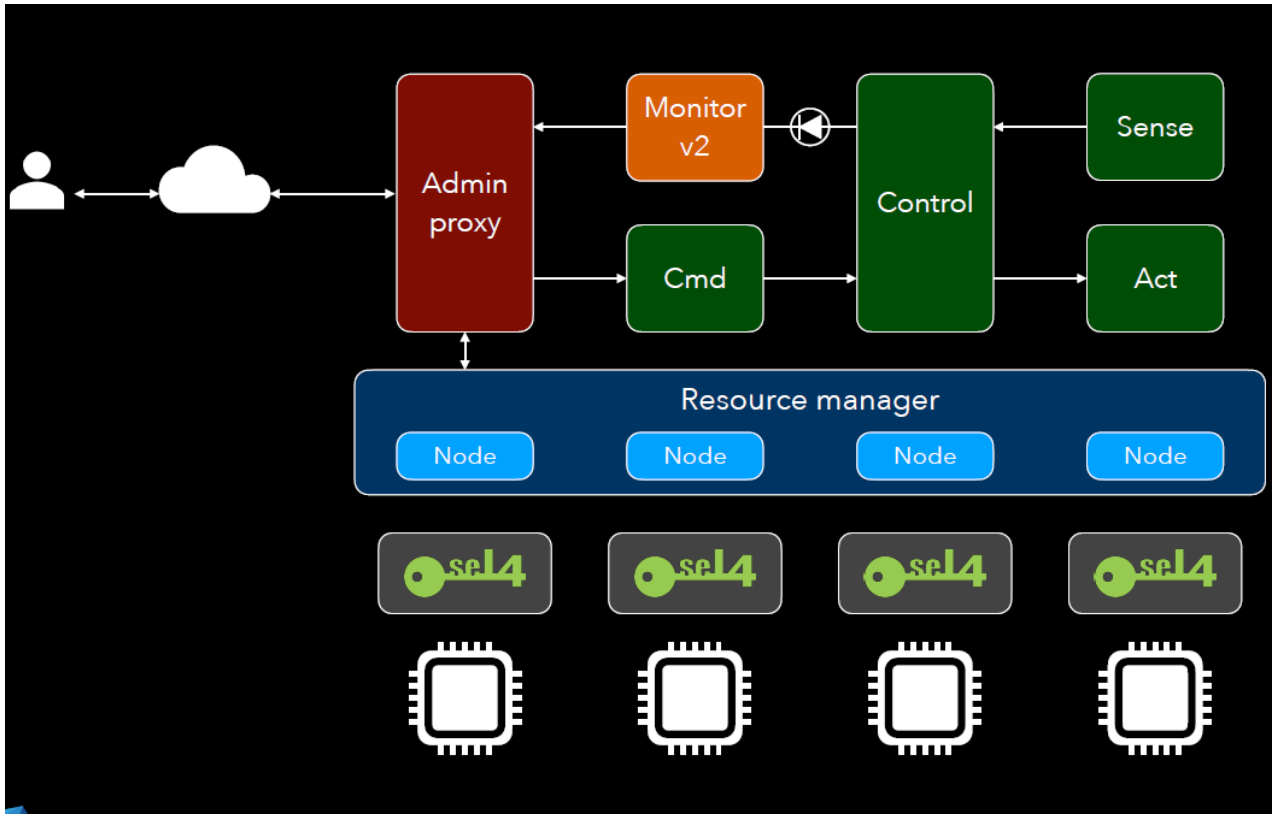
The projects and partners – II

- **Formula-V** – Barkhausen Institut (Dresden) + TU Dresden, TU Berlin, Kernkonzept GmbH, Ferrous Systems GmbH, Fraunhofer AISEC
  - Verification of SW+HW in a holistic approach with Rust => Rocq, Unikernel-OS on RISC V, CHERI
- **PROTECT** – DFKI (Bremen) + RWTH Aachen, Cryspen SARL, Lubis EDA, RPTU Kaiserslautern, Universität zu Lübeck, GI German Society for Computer Science
  - "Bottom-up" compositional verification of SW+HW in RISC V, CHERI
  - Co-design with virtual prototypes, prevention of timing attacks
  - Community-building: networking with the community, advertising for formal verification
- **Clash Formal** – QBayLogic (Enschede, NL)
  - Consistent verification of HW + SW in Haskell-based language Clash

The projects and partners – EvIT

CONVERSE (Kry10 + Proofcraft)

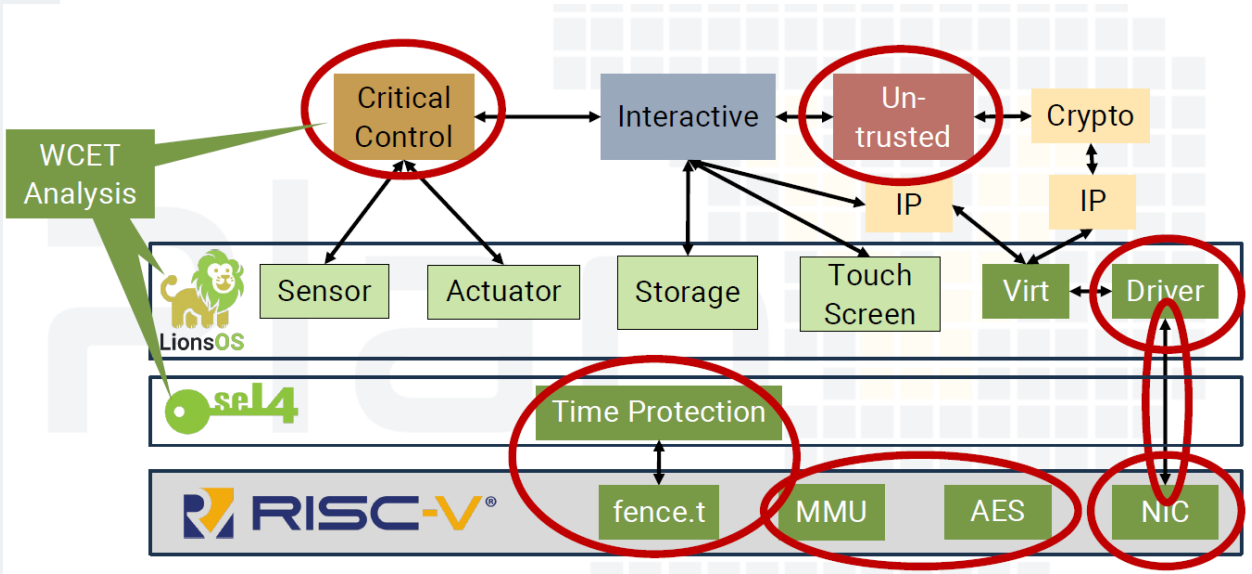
- Multikernel configuration of seL4
- Zero-downtime updates
- Kernel-level and user space verification frameworks, for reasoning about concurrent systems
- Safe configuration of peripheral devices that use legacy Direct Memory Access (DMA)



The projects and partners – EvIT

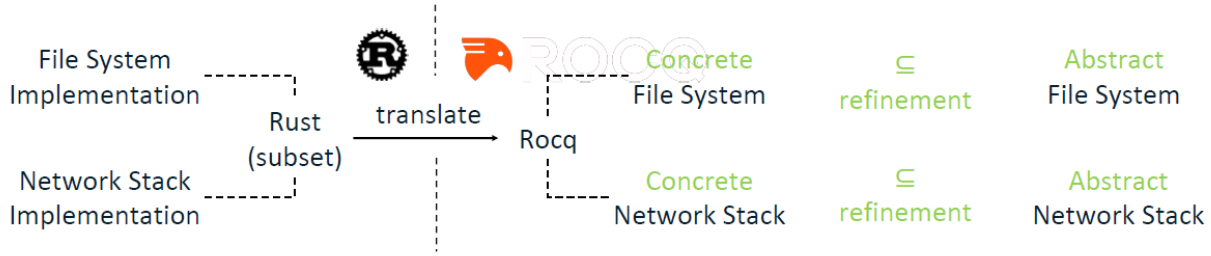
PISTIs-V (Plan V + UNSW, U Gothenburg)

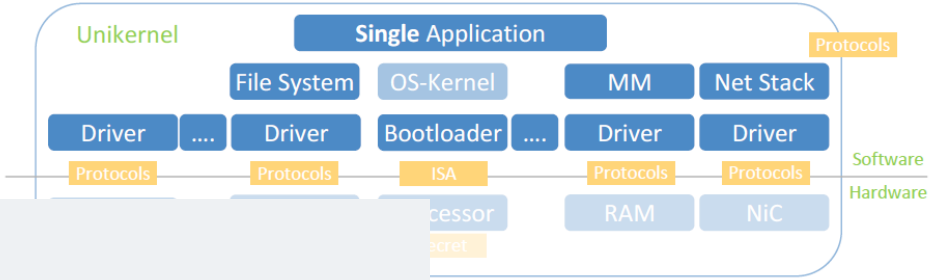
- Verification of LionsOS with security and safety properties
- verification of controllers and drivers for real-world devices, such as Ethernet
- Prove that seL4 prevents micro-architectural covert channels (fence.t instruction)
- end-to-end verification of user-mode components
- worst-case execution time (WCET) analysis of seL4 on a RISC-V processor



The projects and partners – EvIT

Formula-V (Barkhausen Institut et al.)





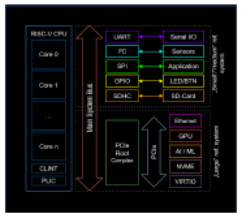
- Verified unikernel platform in Rust and Coq
- Verified file system and network stack, including drivers
- CHERI-Based isolation for unverified code
- RISC-V processor, verified based on SAIL semantics
- Compiler for verified unikernel composition

The projects and partners – EvIT

PROTECT (DFKI et al.)

Which technologies do we use?

- Hardware:
  RISC-V®
- Virtual Prototypes
  - early software development
  - early verification.



- Microarchitecture as a root-of-trust
  - Analyze and mitigate new threat models
  - SW/HW interaction
  - Secure-by-construction design
- Rust
  - Verification tools for Rust (Hax)
- Cryptography
  - Verified Rust crypto-lib
  - Verified IoT onboarding.

- Community-Building

dfki ai

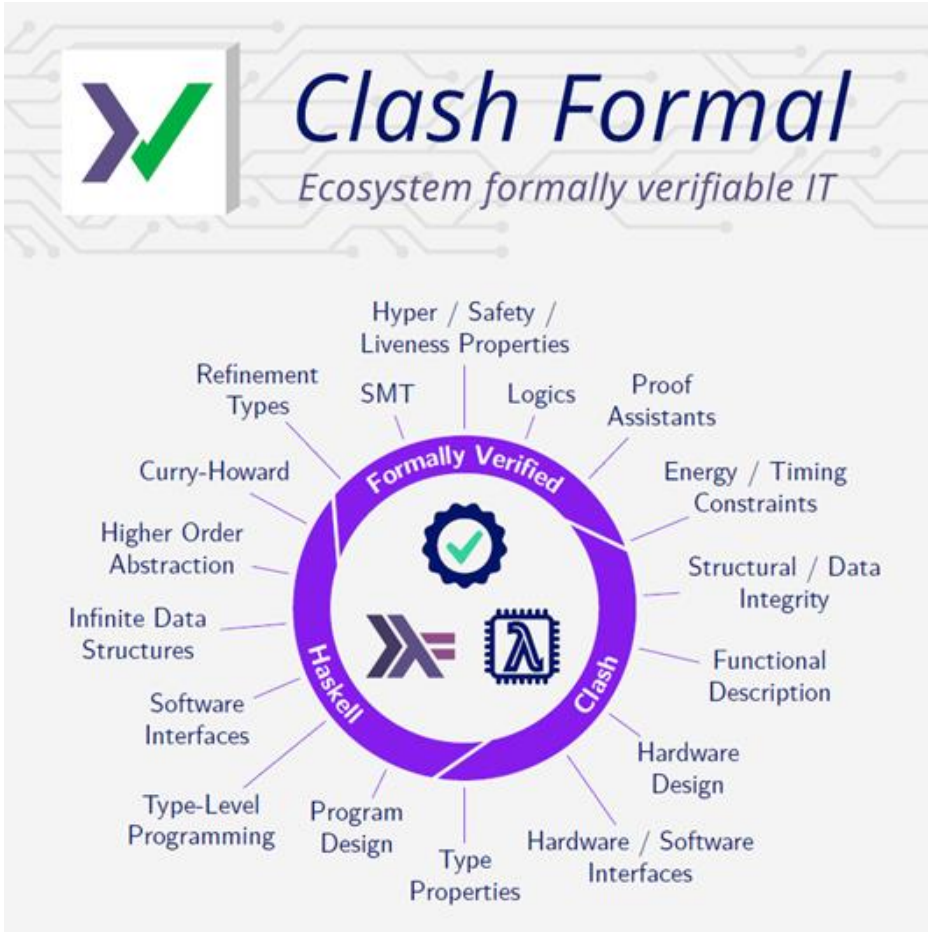
Follow EvIT on LinkedIn

www.linkedin.com/showcase/ecosystem-of-formally-verified-it/

The projects and partners – EvIT

Clash Formal (QBayLogic)

- verification of functional hardware designs with Clash (functional hardware description language)
- Verified crypto core in Clash
- Formally verified RISC-V CPU based on Sail with CHERI support
- Automated reasoning solutions into the functional languages Haskell and Clash
- Create an advanced smart card system



With formal verification, who needs certification?

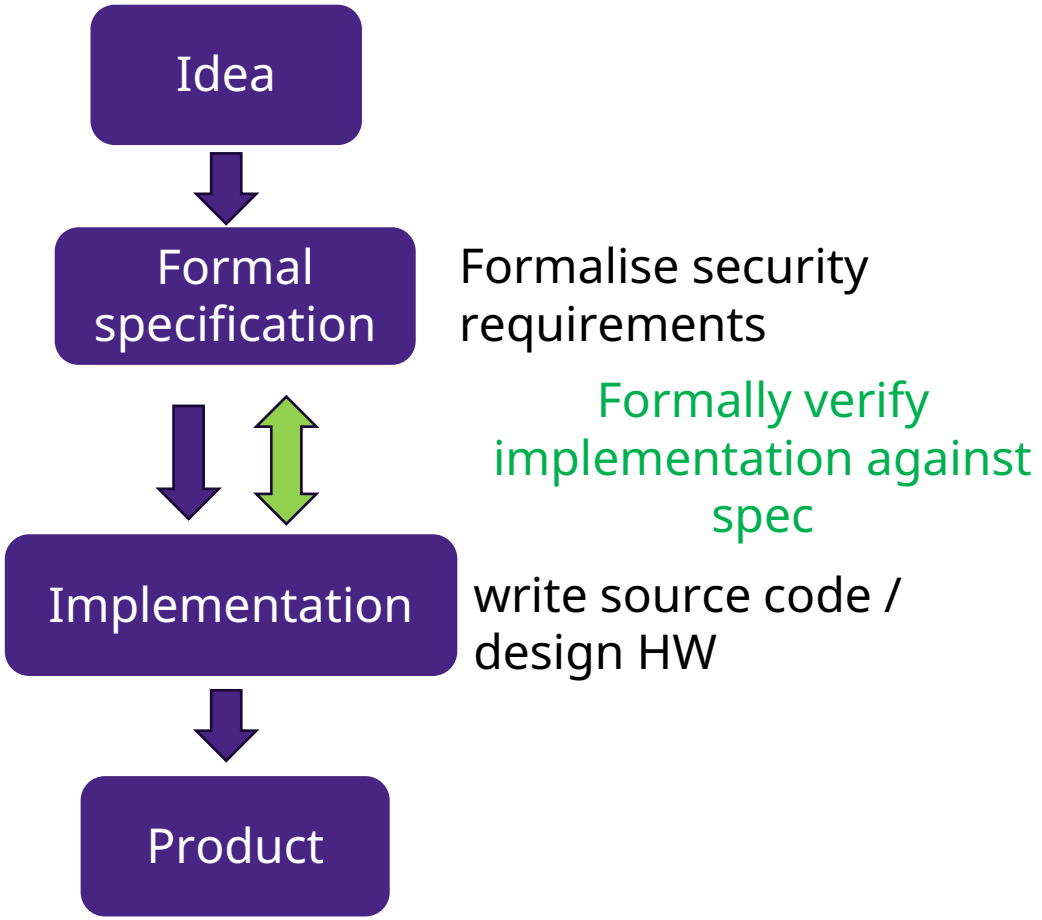
04

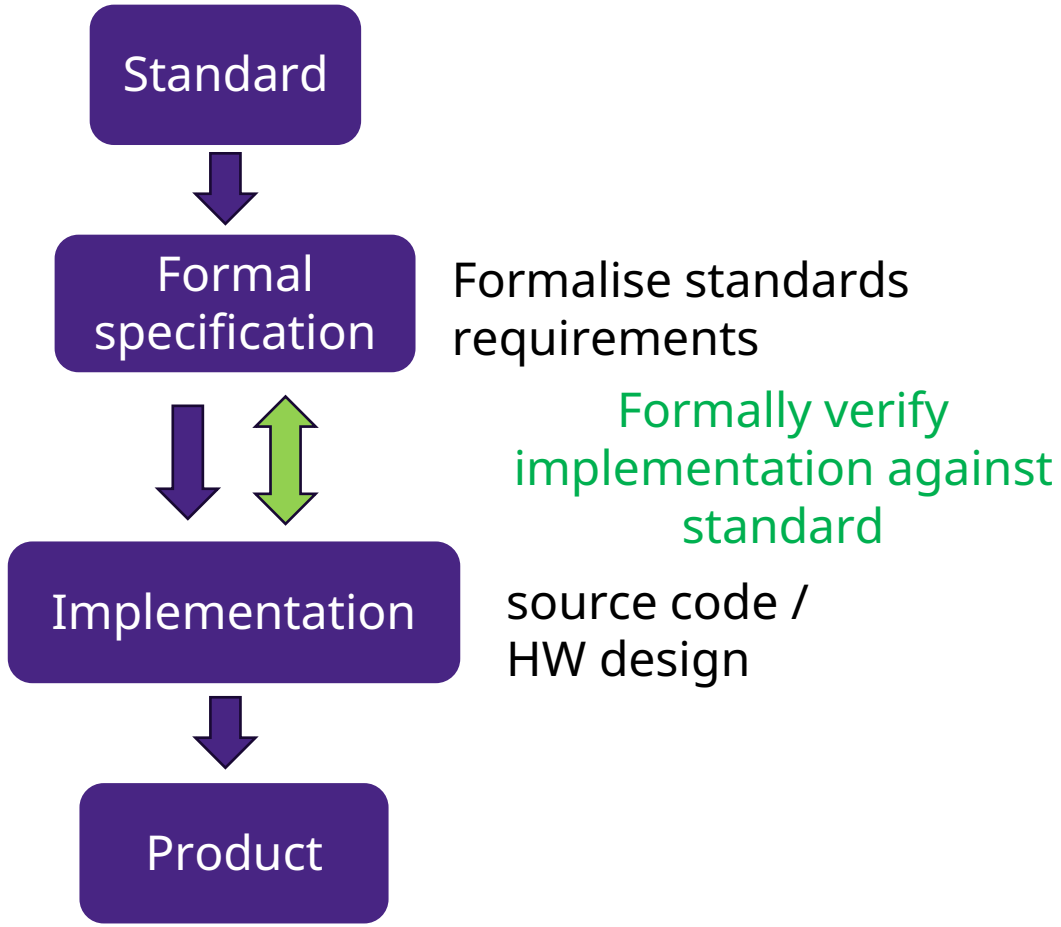
We live in a certified world

- Many regulated markets have certification as an entry requirement
- Some well-known examples:
  - Airplanes (DO-187C, with formal methods supplement DO-333)
  - Cars (ISO 26262, functional safety of electrical / electronic systems)
  - Cybersecurity (Common Criteria), Medical technology, defence equipment, …
- Problems:
  - **High cost**: for the evaluation, for setting up processes, for keeping required documentation. Barrier for small companies!
  - **Slow**: security updates need fast turnaround, but trigger need to re-certify
- **Solution (?):** Specify properties formally, formally verify product conformity.

From formal verification to formal certification

… at least at the *product* level.





Has this been tried before? A brief literature survey

- Alan Wassyng, Tom Maibaum, and Mark Lawford (2010): **On Software Certification: We Need Product-Focused Approaches**, Springer LNCS 6028, pp. 250–274 https://www.researchgate.net/publication/221541340_On_Software_Certification_We_Need_Product-Focused_Approaches (all at McMaster U)
  - *"Certification should be a measurement based activity, in which an objective assessment of a product is made in terms of the values of measurable attributes of the product, using an agreed upon objective function."*
  - Sets out research questions that need to be tackled for software certification
    - Includes the idea of ' "faking" of real processes', i.e. digital twins
  - Highlights the importance of software engineering as an *engineering* discipline
    - Complete with an epistemological framework of software engineering

The inverse opinion: certify the process only!

- Sebastien Dupont et al. (2021), Incremental Common Criteria Certification Processes using DevSecOps Practices, 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), DOI: 10.1109/EuroSPW54576.2021.00009, partially funded by the EU (Horizon 2020) SPARTA project
  - Highlight the EU Cyber Security Act (CSA) and its emphasis of certification.
  - Crucial quotes:
    "To ensure continuity of certification, updates must be analyzed to verify the impact on certified cybersecurity properties. Impacted properties need to be re-certified."
    "However, a "classic" approach to incremental certifications is not yet sufficient to guarantee the necessary flexibility in the modern market. ***It is here that the proposal to certify not the product, but the process of developing a product finds its space.****"*
  - The SPARTA project deliverables consider many interesting related questions.

Back to the product-based approach

- A semi-automatic and trustworthy scheme for continuous cloud service certification, Marco Anisetti et. al. (2020) in *IEEE Transactions on Services Computing*, vol. 13, no. 1, pp. 30-43, doi:10.1109/TSC.2017.2657505.
  - *„The scheme is driven by non-functional requirements defined by the certification authority and by a model of the service under certification.“*
  - Formal treatment; re-certification; but: heuristics to reduce computational complexity
- Automating IoT Security Standard Testing by Common Security Tools, Kaksonen et al. (2025), in *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024), pages 42-53.* doi:10.5220/0012345900003648
  - Automation of tests from the ETSI TS 103 701 test specification for the ETSI EN 303 645 security standard using existing IT security tools – however **no** formal methods
  - *„… full automation is unlikely to be feasible … ”*

Is there a technical *and* a business case for formal certification?

- Technical case: product-based formal certification allows fast re-certification
- Variant: Use formal methods to show that changed part does not affect the rest of the system in unintended ways; re-certify a much smaller part
- Business case:
  - Formal methods are costly, need to code/design for formal certification
  - Certification is costly also (certain processes, documentation, evaluation)

$\Rightarrow$ If you code/design for formal verification anyway, product-based formal certification *saves* money compared to process-based certification!

Further thoughts

What else can follow the programme EvIT .....

- Formal verification of legislative processes (“certifying law”)
  - Verification of a new law against existing set of orders/international law/regulations
  - Possible questions: Does an individual new regulation violate any other regulation/paragraph chain, does it lead to new interpretation of existing laws, which implications does it have to other laws, ...
  - Research Area: Knowledge base - interpretation of the content of a law / semantics of legal language and mapping onto a formalized domain-specific language - specification vs. implementation
- Supply Chains
  - Formally verified systems (SW, HW) are trustworthy even if they come from insecure supply chains
  - Holistic supply chain analysis
  - Physical analysis of hardware? What can be discovered?

Contact

Agentur für Innovation in der Cybersicherheit GmbH - Cyberagentur

Dr. Christoph Hof
Head of the project office of the Cyberagentur in Dresden

hof@cyberagentur.de
+49 151 44150 732

Agentur für Innovation
in der Cybersicherheit GmbH
Große Steinstraße 19
06108 Halle (Saale)
Germany

www.cyberagentur.de

Follow EvIT on LinkedIn

Pic: Cyberagentur