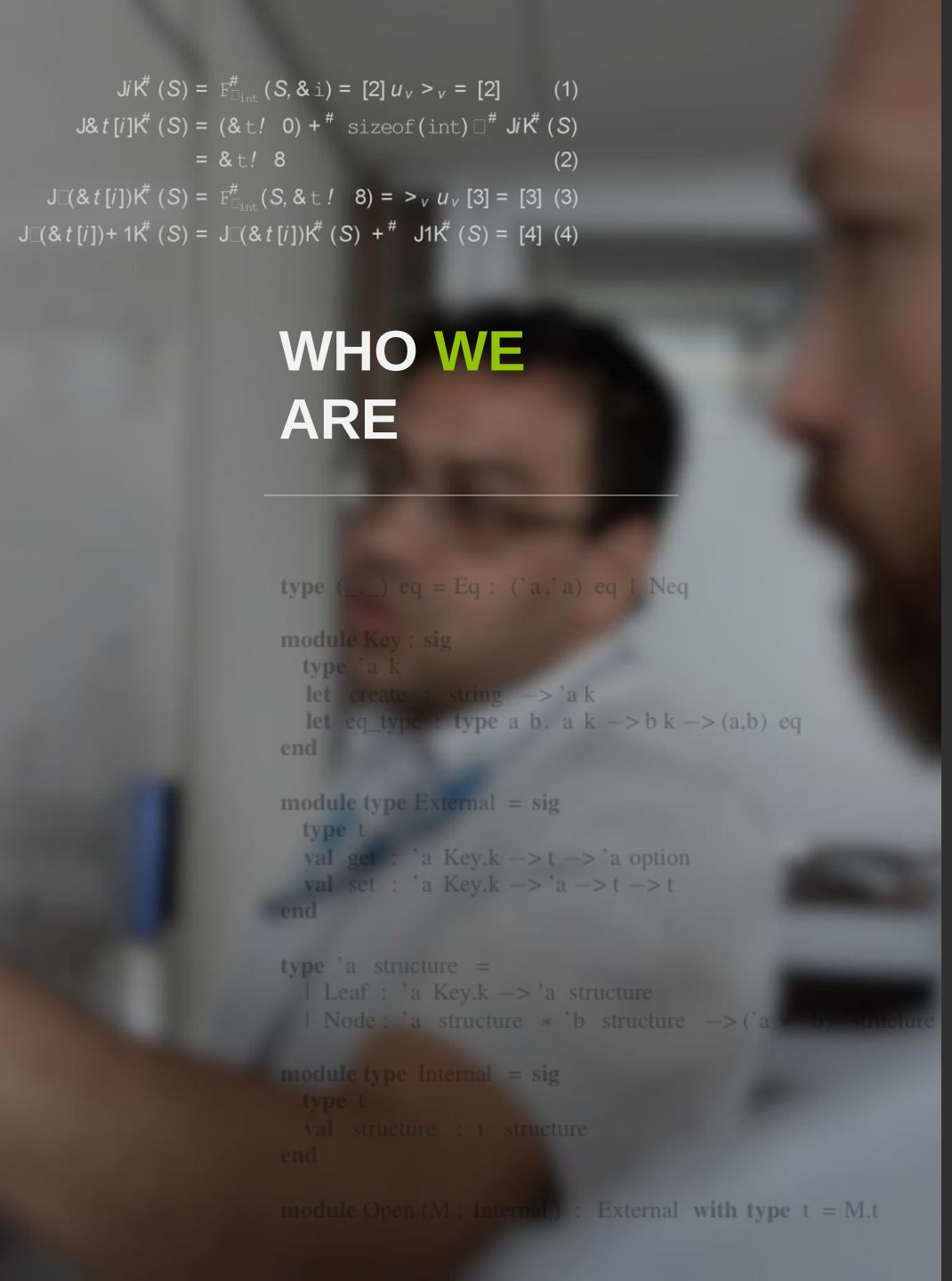
RETOUR D'EXPÉRIENCE D'UN PROJET SÉLECTIONNÉ – VESSEDIA

Florent Kirchner



WHO WE ARE

RESEARCH FOCUSED

We take active roles in the implementation of international research & innovation roadmaps

INDUSTRY STRONG

Our teams develop and support platforms used worldwide by scientists and engineers alike

AN EXPERTISE IN FRENCH-RENOWNED SPECIALTIES

- Deductive verification
- Symbolic execution
- SAT/SMT solving
- Constraint solving
- Abstract interpretation
- Runtime verification
- Simulation
- Tool engineering

SCIENTISTS & ENGINEERS 26

PH.D STUDENTS 13

POSTDOCS 5

MONTAGE DE PROJETS

- **Les projets Européens sont :**
  - Difficiles a monter: concurrence très rude, niveau de qualité exigé est très élevé
  - Une source importante de financements donc très demandés
  - Appels d'offres complexes et nombreux (2 calls par an dans ICT et SEC)

- **Le montage se professionnalise:**
  - Manière d'écrire une proposition particulière
  - Edition de texte et d'arguments non techniques
  - Connaissance des règles du jeu impérative

Call - Digital Security Focus Area

H2020-DS-2016-2017

ICT-driven transformations bring opportunities across many important sectors but also vulnerabilities to critical infrastructures and digital services, which can have significant consequences on the functioning of society, economic growth and the technological innovation potential of Europe. These challenges are being addressed through innovative approaches that cross the boundaries of individual H2020 pillars, calls and challenges. Therefore the main research & Innovation activities in Digital Security are grouped in a dedicated focus area cutting across LEIT–ICT and Societal Challenges parts of the work programme, including evidently the Societal Challenge 7 on "Secure Societies", but also the Societal Challenge 1 on "Health, demographic change and wellbeing".

Proposals are invited against the following topic(s):

DS-01-2016: Assurance and Certification for Trustworthy and Secure ICT systems, services and components

Specific Challenge: The constant discovery of vulnerabilities in ICT components, applications, services and systems is placing our entire digital society at risk. Insecure ICT is also imposing a significant cost on users (individuals and organisations) who have to mitigate the resulting risk by implementing additional technical and procedural measures which are resource consuming.

Smart systems, highly connected cyber-physical systems (CPS) are introducing a high dynamism in the system to develop and validate. Hence, CPS are evolving in a complex and dynamic environment, making safety-critical decisions based on information from other systems not known during development.

Another key challenge is posed by domains, such as medical devices, critical infrastructure facilities, and cloud data centres, where security is deeply intertwined and a prerequisite for other trustworthiness aspects such as safety and privacy.

The challenges are further intensified by the increasing trend of using third party components for critical infrastructures, by the ubiquity of embedded systems and the growing uptake of IoT as well as the deployment of decentralized and virtualized architectures.

In order to tackle these challenges, there is a need of appropriate assurances that our ICT systems are secure and trustworthy by design as well as a need of certified levels of assurance where security is regarded as the primary concern. Likewise, target architectures and methods improving the efficiency of assurance cases are needed in order to lower their costs.

Scope: a. Research and Innovation Actions - Assurance

Providing assurance is a complex task, requiring the development of a chain of evidence and specific techniques during all the phases of the ICT Systems Development Lifecycle (SDLC for short: e.g. design verification, testing, and runtime verification and enforcement) including the validation of individual devices and components. These techniques are complementary yet all necessary, each of them independently contributing towards improving security assurance. It includes methods for reliability and quality development and validation of highly dynamic systems.

Proposals may address security, reliability and safety assurance at individual phases of the SDLC and are expected to cover at least one of the areas identified below, depending on their relevance to the proposal overall objectives:

- Security requirements specification and formalization;
- Security properties formal verification and proofs at design and runtime
- Secure software coding;
- Assurance-aware modular or distributed architecting and algorithmic;
- Software code review, static and dynamic security testing;
- Automated tools for system validation and testing;
- Attack and threat modelling;
- Vulnerability analysis;
- Vendor (third-party) application security testing;
- Penetration testing;
- Collection and management of evidence for assessing security and trustworthiness;
- Operational assurance, verification and security policy enforcement;
- Adaptive security by design and during operation.

Proposal should strive to quantify their progress beyond the state of the art in terms of efficiency and effectiveness. Particular importance within this context should be placed on determining the appropriate metrics.

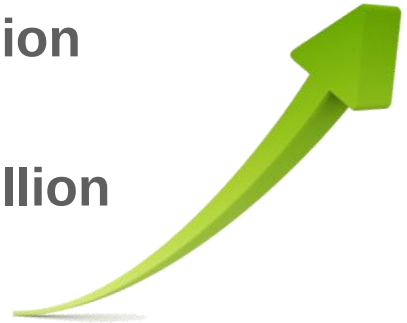
Proposals should take into account the changing threat landscape, where targeted attacks and advanced persistent threats assume an increasingly more important role and address the challenge of security assurance in state-of-the-art development methods and deployment models including but not limited to solutions focussing on reducing the cost and complexity of assurance in large-scale systems.

Proposals should include a clear standardisation plan at submission time.

QUEL EST LE PROBLEME ?

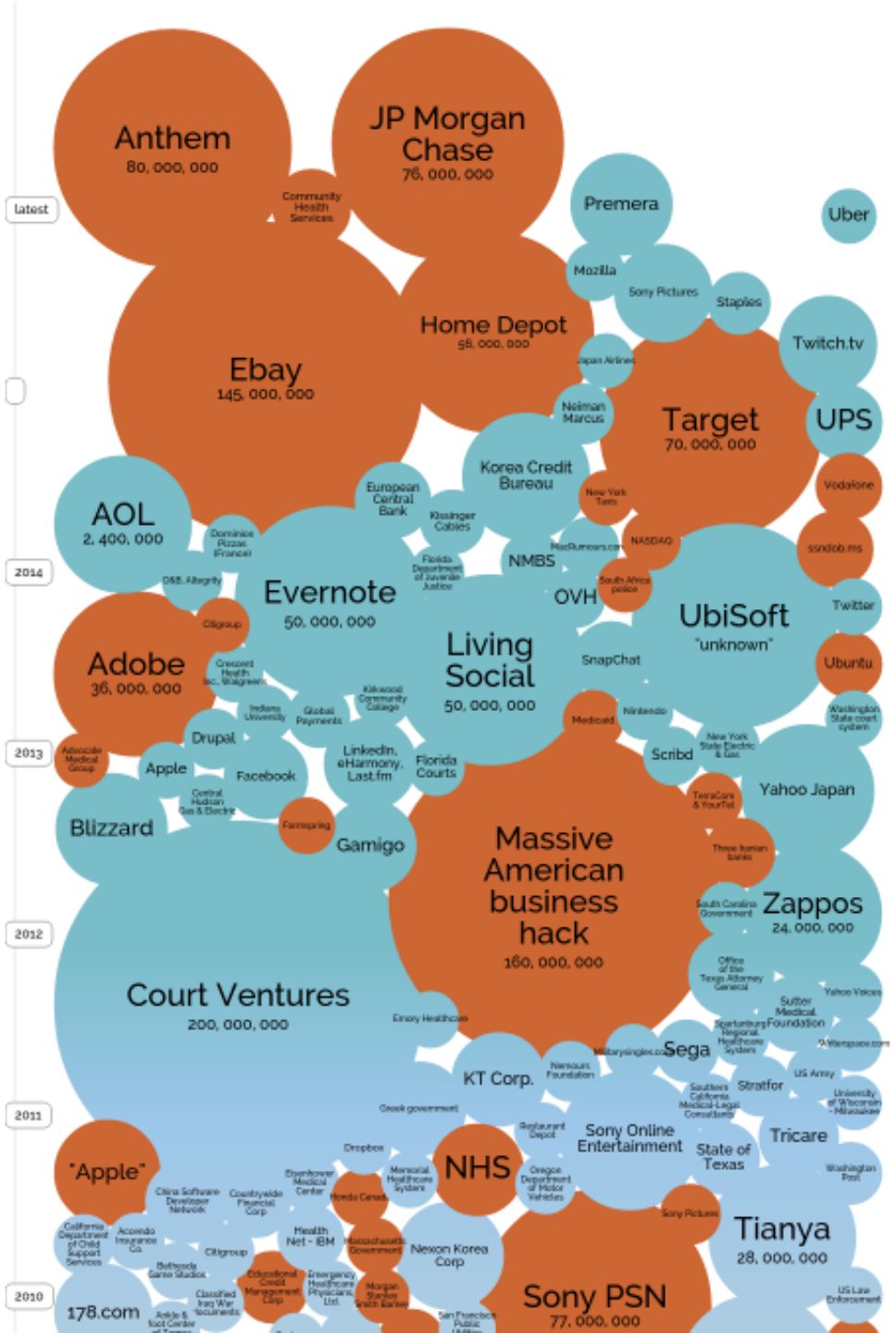
Connected objects

- **2016** 5.5 billion
- **2020** 20.8 billion



“For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need trust and confidence. Unfortunately, […] almost a third of Europeans are not confident in their ability to use the internet for banking or purchases”

- Cybersecurity Strategy of the EU

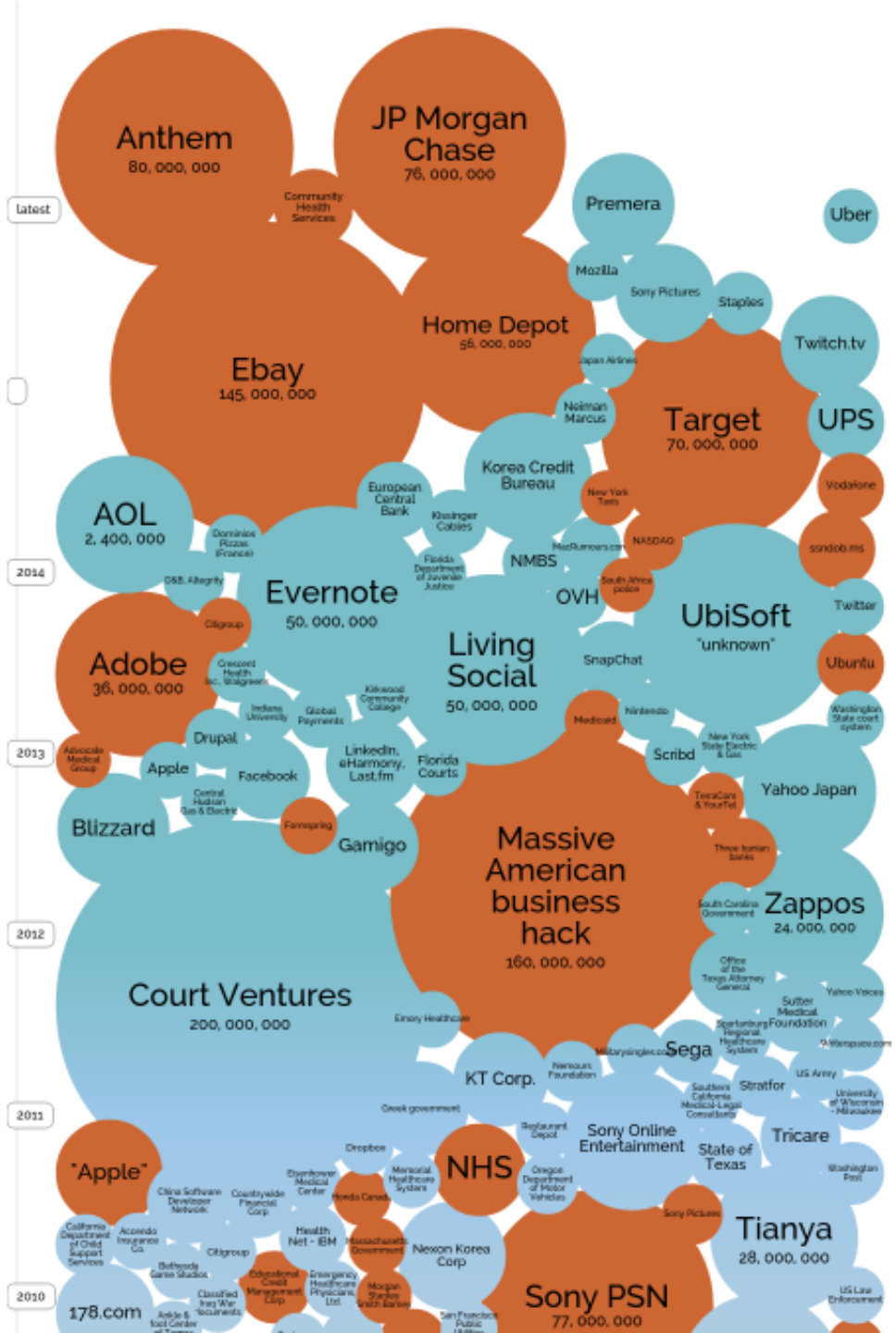


CYBERSECURITY STRATEGY OF THE EU

“For new connected technologies to take off, including e-payments, cloud computing or machine-to-machine communication, citizens will need trust and confidence. Unfortunately, […] almost a third of Europeans are not confident in their ability to use the internet for banking or purchases”

CONNECTED OBJECTS

- **2016 5.5 BILLION**
- **2020 20.8 BILLION**

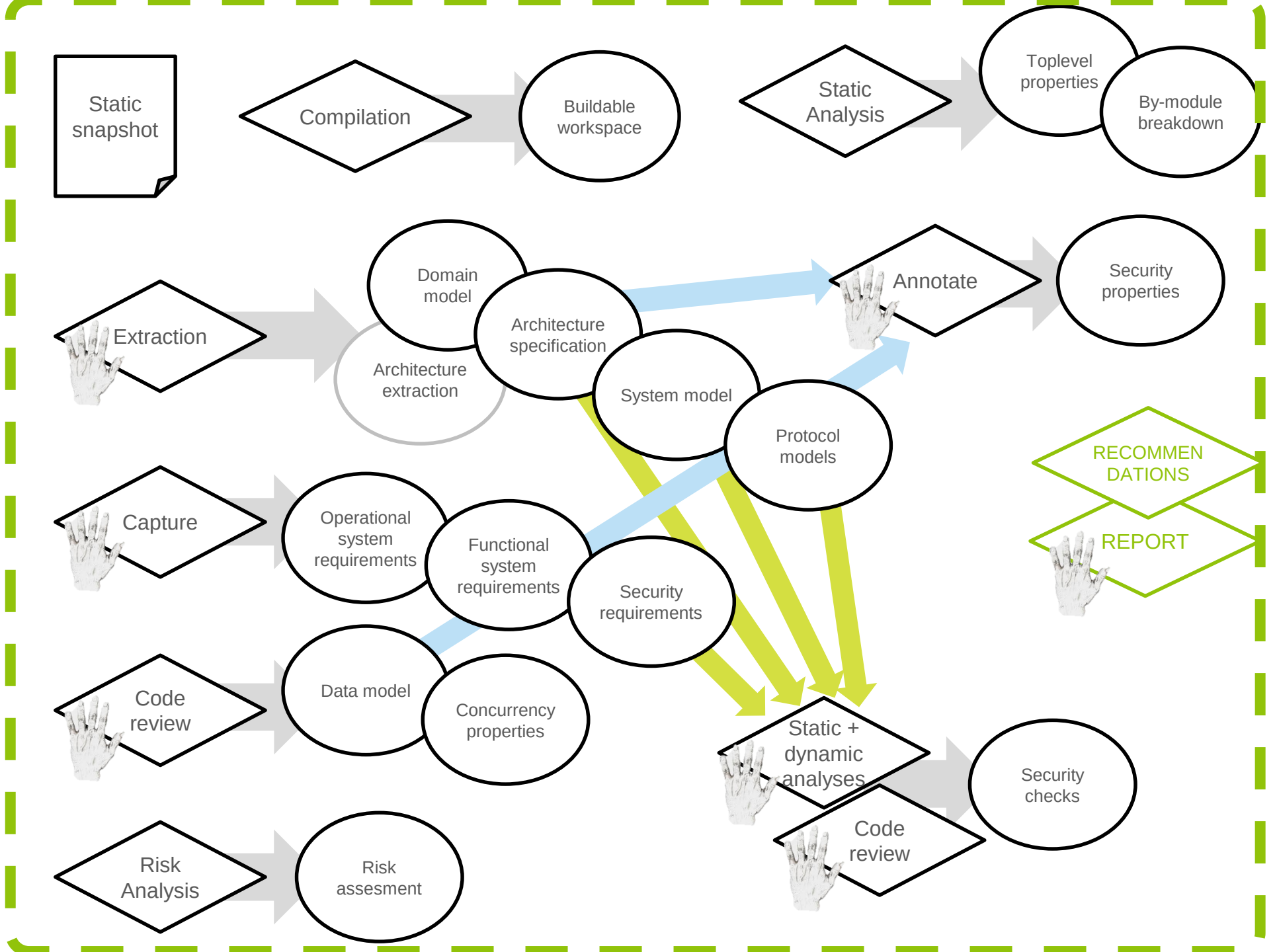


APPROACHES TO CYBERSECURITY ASSURANCE

- INPUT Static snapshop of the system
- INPUT « Bad things don’t happen »

- NO build
- NO system requirements
- NO model of the domain
- NO architecture specification
- NO specification of the source code
- NO expected security properties

- MAYBE source-level documentation
- MAYBE unit, subsystem tests


Static snapshot
Compilation
Buildable workspace
Static Analysis
Toplevel properties
By-module breakdown
Extraction
Domain model
Architecture extraction
Architecture specification
System model
Protocol models
Annotate
Security properties
Capture
Operational system requirements
Functional system requirements
Security requirements
RECOMMENDATIONS
REPORT
Code review
Data model
Concurrency properties
Static + dynamic analyses
Security checks
Code review
Risk Analysis
Risk assesment

QUEL EST L'ANCRAGE TECHNIQUE DU PROJET?

CODE ANALYSIS

```
void mpi_swap(mpi *X, mpi *Y) {
mpi T;  memcpy((void *)(& T),(void
const *)X,sizeof(mpi));
memcpy((void *)X,(void const
*)Y,sizeof(mpi));  memcpy((void
*)Y,(void const *)(&
T),sizeof(mpi));  return; }
```

```
/*@ requires
\valid(X);
requires
\valid_read(Y);
ensures (\result ≡
0 ∧ *Y ≡ \old(*X) ∧
*X ≡ \old(*Y));
```

frama C
Software Analyzers

Frama-C Kernel

Frama-C
Open Source
Distribution

SecureFlow Plug-In

Path-Crawler Plug-In

Impact & Slicing Plug-In

Value Plug-In

WP Plug-In

Aoraï Plug-In

E-ACSL

Information flows

Memory and pointer manipulation vulnerabilities

Functional verifications

Runtime monitoring

Sequence properties

Coq, Alt-Ergo
Why

Atos

MITSUBISHI ELECTRIC

Supélec

PARIS DIDEROT

ENS CACHAN

Verimag

Inria

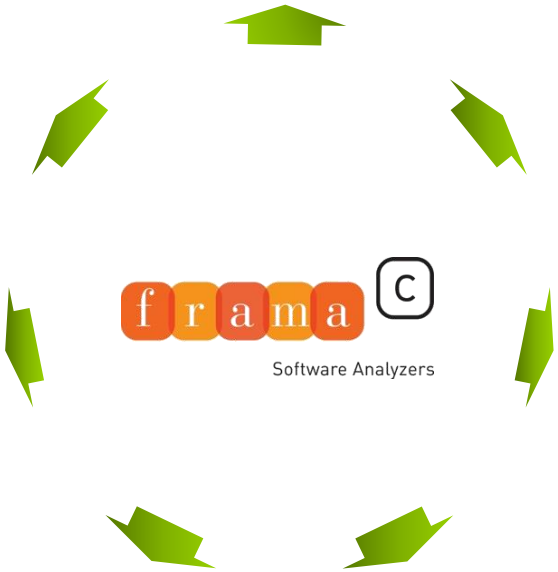
VESSEDIA - OBJECTIVES

1. Drastically improve security verification methods
2. Quantification of the verification process
3. Building collaborative and smart user interfaces
4. Training non-specialists for formal methods
5. Management of verification data
6. Higher-level models for verification
7. Building strong links with existing certification practices

COMMENT L’EQUIPE SE MONTE-T-ELLE ?

BUILDING THE ECOSYSTEM FOR SECURITY ASSESSMENT

Software assurance is decisive in securing added value in cybersecurity-related activities. Broad families of stakeholders can be projected on industrial sectors as diverse as aeronautics, energy production and distribution, marine and offshore, space, rail, banking, health, and defense.



OPERATORS

- EDF
- CEA

INTEGRATORS

- Airbus
- Dassault Aviation
- Thales
- Areva

RESEARCH AND INNOVATION

- Université Paris-Saclay
- Inria
- Verimag
- Fraunhofer
- KU Leuven
- NASA

CERTIFICATION AUTHORITIES

- IRSN
- NIST
- ANSSI
- DGA
- Bureau Veritas
- University Turku

frama C
Software Analyzers

TECHNOLOGY PROVIDERS

- Gemalto
- Thales
- Inria
- Atos

TOOL EDITORS

- Atos
- SafeRiver
- TrustInSoft
- Airbus EYY

SERVICE PROVIDERS

- Galois
- Adelard
- SII, AUSY, Atos
- TrustedLabs
- Oppida, Amossys
- Search Labs

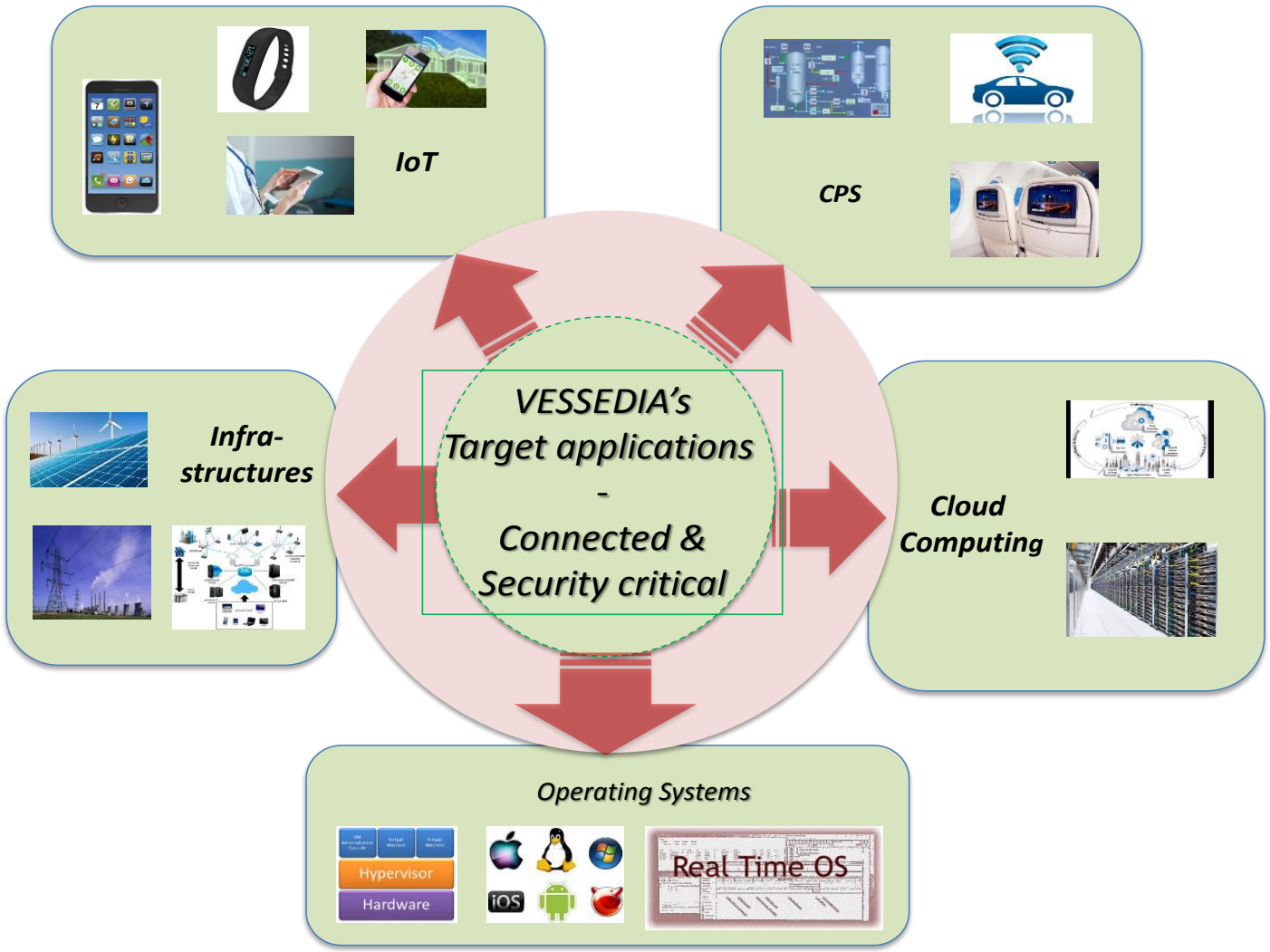
list
CEA tech

VESSEDIA'S
USE CASES

ContikiOS (Inria)

6LowPAN (CEA LSC)

Aircraft Maintenance System (Dassault)



Participant No	Participant organisation name		Beneficiary short name	Country
1 (Coordinator)	Technikon Forschungs- und Planungsgesellschaft mbH	SME	TEC	Austria
2	CEA LIST	RTO	CEA	France
3	DASSAULT AVIATION	Industrial	DA	France
4	Search Lab	SME	SLAB	Hungary
5	Fraunhofer FOKUS	RTO	FOKUS	Germany
6	Institut National de Recherche en Informatique et Automatic	RTO	INRIA	France
7	Turku University of Applied Sciences	University	TUAS	Finland
8	KU Leuven	University	KUL	Belgium
9	Fundacion Deusto	RTO	DEU	Spain
10	Amossys SAS	Certification	AMO	France

ETHIQUE DE TRAVAIL

FACTEURS TECHNIQUES

- **Coordination**
  - telcos fréquentes
  - espace de travail partagé
  - releases périodiques
  - planning et répartition du travail

- **Edition**
  - souci d'homogénéité dans la rédaction de la section B
  - nombreuses relectures critiques internes

- **Très forte maitrise du processus de montage et des relations avec la CE**
  - implication des PCN au plus tot

- **Efforts significatifs des partenaires lors de la production de la proposition**
  - 3 personnes au CEA
  - 3 mois de travail

THE MASTERPLAN

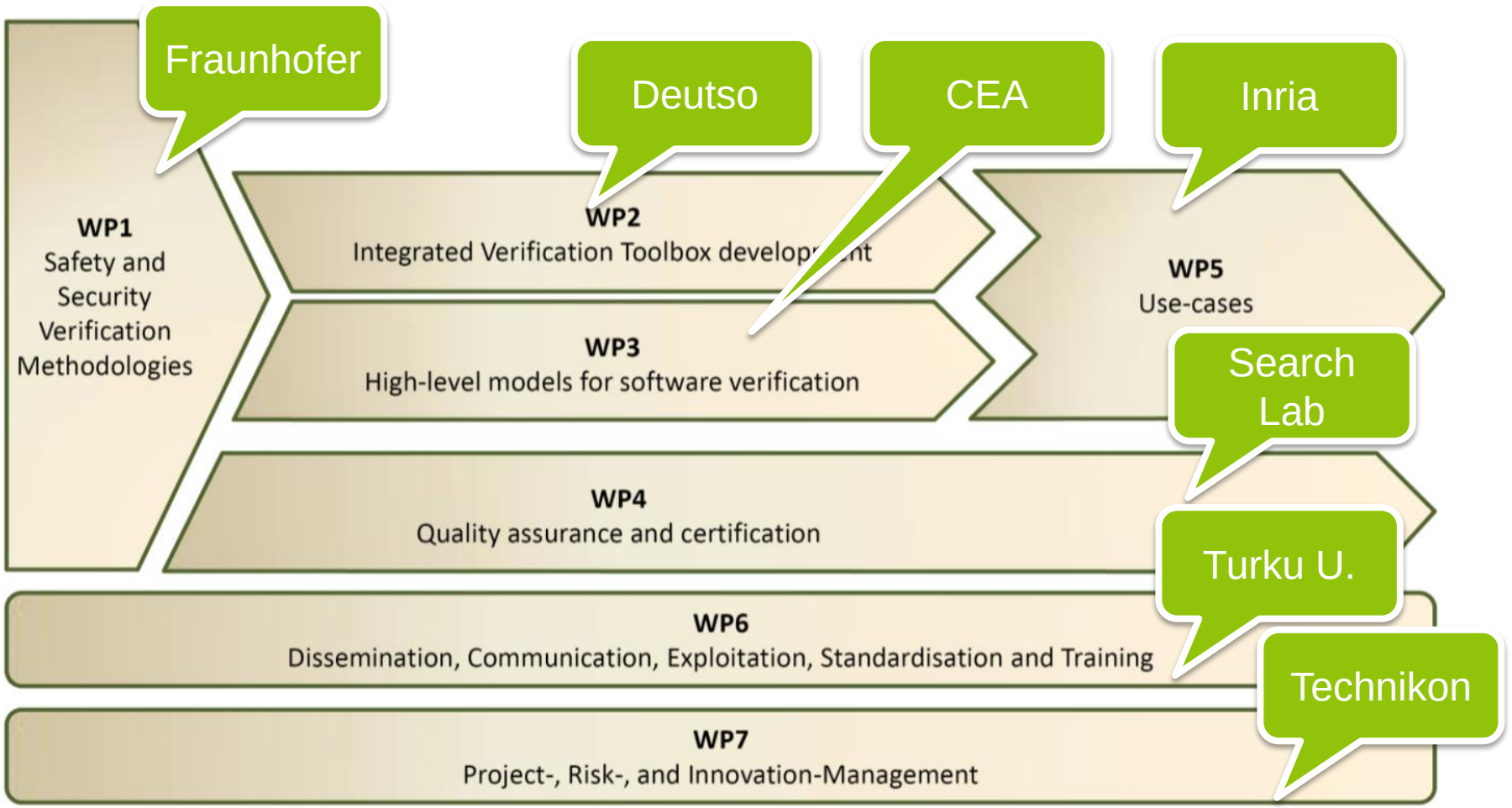
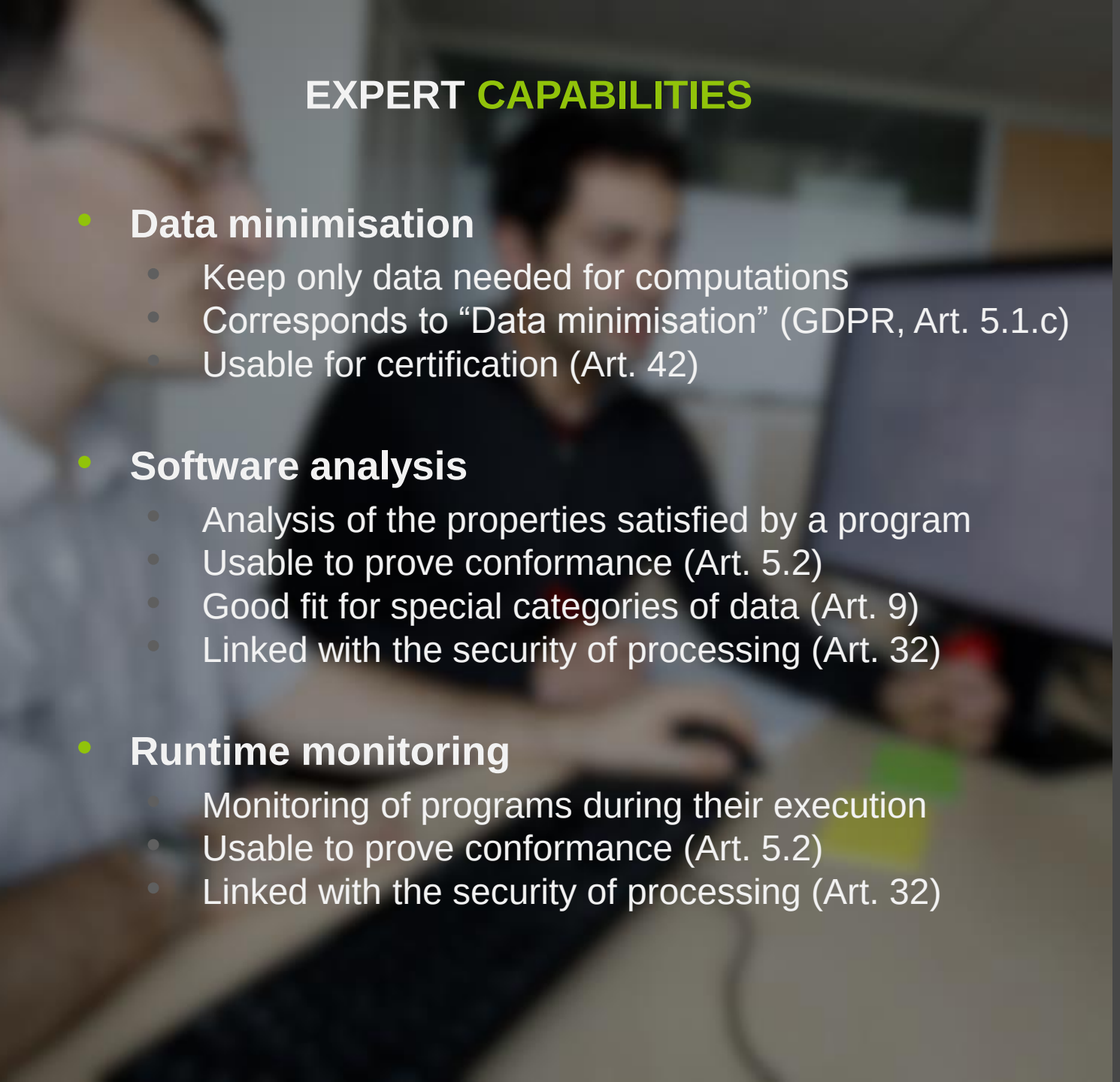


Figure 9: VESSEDIA work plan

VESSEDIA A ÉTÉ REMPORTÉ AVEC LES NOTES SUIVANTES

EXCELLENCE 5/5, IMPACT 4.5/5, IMPLÉMENTATION 5/5

TOTAL 14.5/15



EXPERT CAPABILITIES

- **Data minimisation**
  - Keep only data needed for computations
  - Corresponds to “Data minimisation” (GDPR, Art. 5.1.c)
  - Usable for certification (Art. 42)
- **Software analysis**
  - Analysis of the properties satisfied by a program
  - Usable to prove conformance (Art. 5.2)
  - Good fit for special categories of data (Art. 9)
  - Linked with the security of processing (Art. 32)
- **Runtime monitoring**
  - Monitoring of programs during their execution
  - Usable to prove conformance (Art. 5.2)
  - Linked with the security of processing (Art. 32)

SELECTED IMPACTS

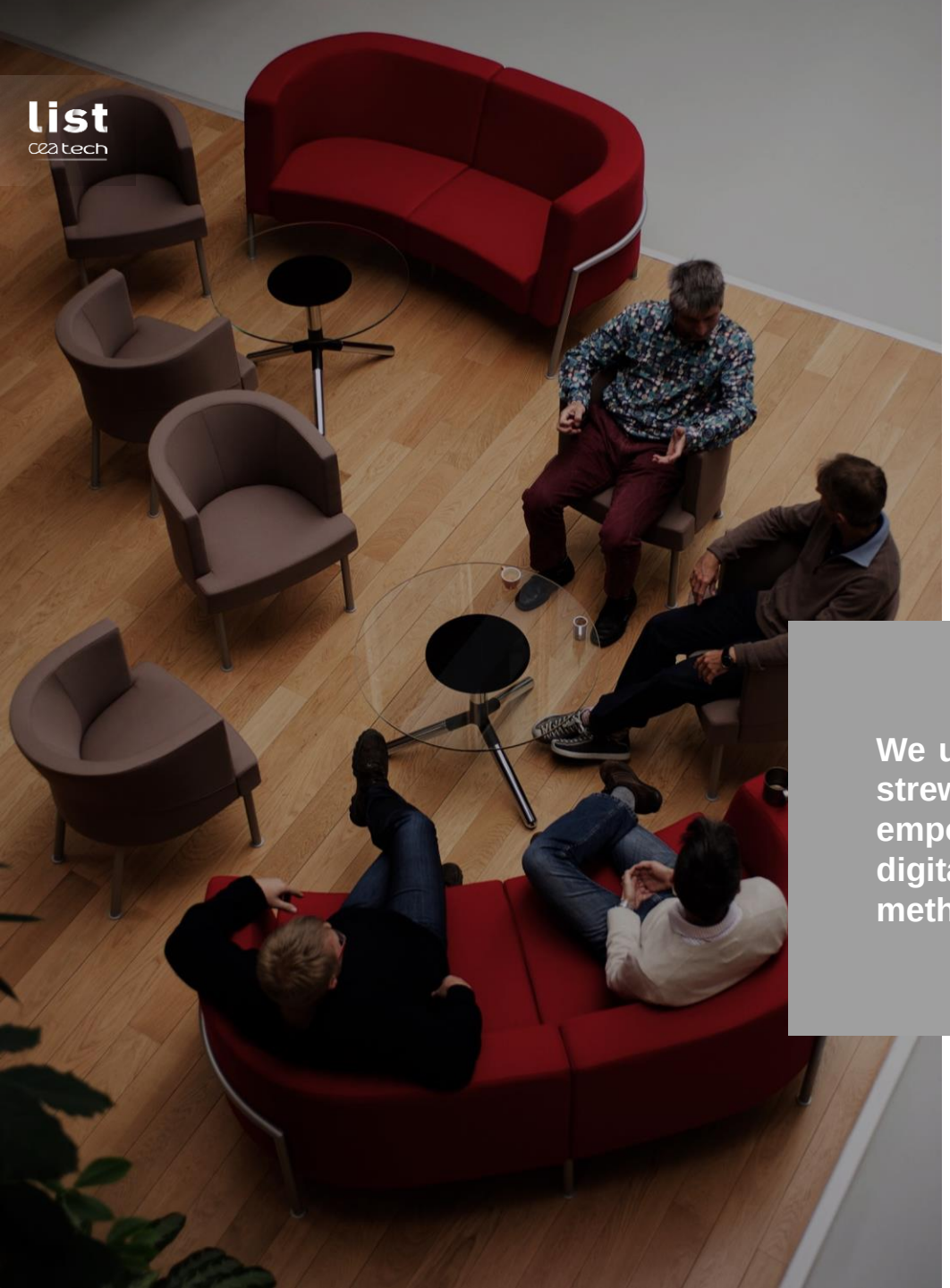
- **Short-term impact**
  - Cybersec & privacy risks in finance
  - Systems & proof of concepts to manage cybersec & privacy risks
  - Fast adoption of cybersec. & privacy best practices in finance
- **Long-term impact**
  - Trust chains among all entities in the finance ecosystem
  - Better implementation of the GDPR
  - Promotion of cybersec. & privacy in the whole EU finance ecosystem

CHALLENGES


Post-quantum computing
Adaptative security
Whitebox cryptography
Hardware – software security
Fast intelligent flaw detection and response
Blockchains & Smart contracts
Lightweight access-based encryption
Unified risk assessment
Smart compilation
Assessment management

Software Safety and Security Laboratory
Software & Systems Engineering Department
CEA LIST

Florent Kirchner
florent.kirchner@cea.fr



SYSTEMS + SOFTWARE ENGINEERING

We understand tomorrow’s intelligent and connected systems will not be strewn hastily together, but carefully designed and verified. We believe in empowering people to reach this goal, putting them in control of their digital environments. Our teams research and develop the world’s leading methods and tools for engineering high-confidence software and systems.

ADVANCED SOFTWARE ANALYSES

Cyber-attacks largely rely on software flaws. Software trust is becoming a cornerstone of business requirements and normative compliance

TRADITIONAL TECHNIQUES

Rely on reviews and tests to try to find flaws faster than attackers do

BREAKTHROUGH

Frama-C/Value is the world's first tool to pass NIST's Ockham Criteria for the exhaustive detection of common security flaws

FRAMA-C AND BINSEC

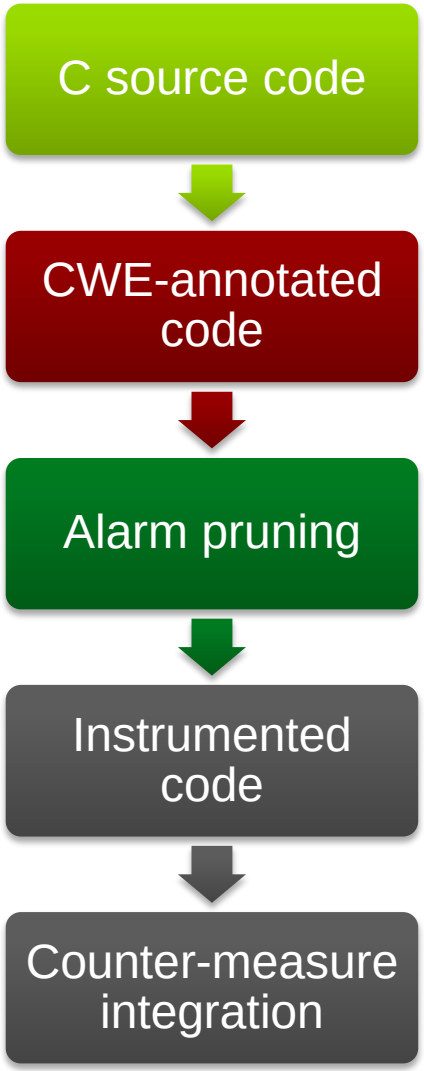
Code analysis platforms based on advanced reasoning, providing strong mathematical security proofs

IMPACT

List's software analysis platforms are used across CEA, and by teams from DGA, Airbus, Dassault Aviation and Thales

RUNTIME CODE MONITORING

By automating security weaknesses detection and counter-measure generation on critical components, security engineers can strengthen the code to resist them



IDENTIFY SECURITY FUNCTIONS

Lightweight code scans pinpoint potential code weaknesses and annotate the code with safe scenario requirements

MONITOR SYNTHESIS

From these annotations Frama-C/EACSL generates executable code that monitors vulnerabilities during execution. Custom counter-measures can then be linked to them

EARLY RESULTS

R&T experiments with code analysis and counter-measure generation at Dassault Aviation were conclusive

list
cea tech

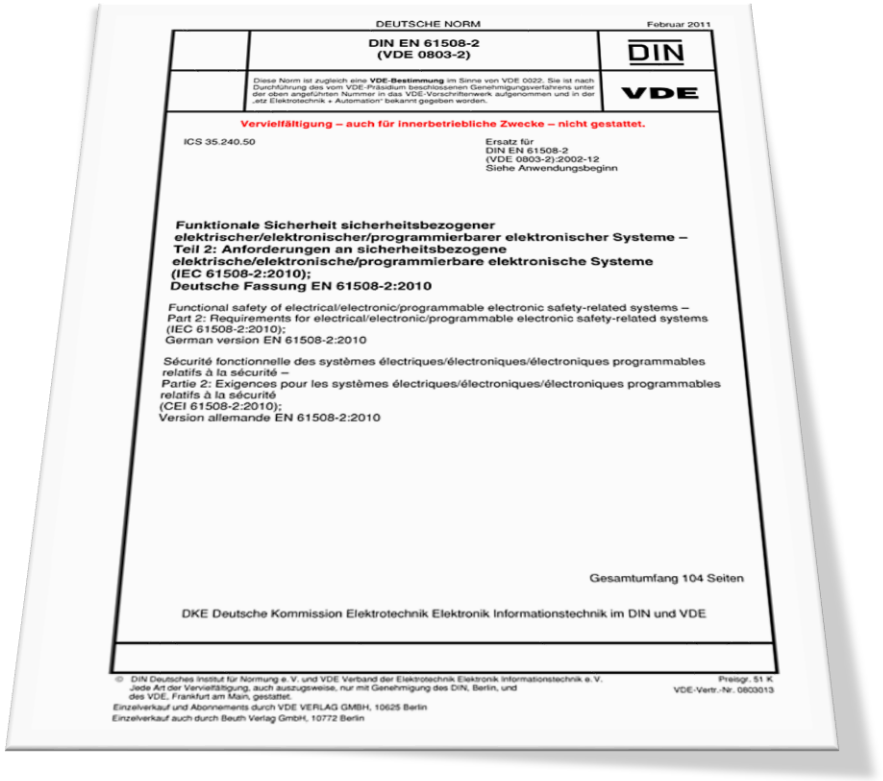
FUNDAMENTAL PROPERTIES – EXAMPLES

- **Code implements sanitation on all relevant control-flows**
  `sanitize() is run on a and b before calling g(a,b)`

- **Code data-flow meets its specifications**
  `f() writes its output from parameters a and b`

- **Code is free of runtime errors**
  - `&ptr;`
  - `buf[i+1]`
  - `num / den_nz;`

- **Numerical accuracy stays within specified bounds**
  `float f = 0.1;`



DEUTSCHE NORM Februar 2011

DIN EN 61508-2
(VDE 0803-2)

DIN

VDE

Diese Norm ist zugleich eine **VDE-Bestimmung** im Sinne von VDE 0022. Sie ist nach Durchführung des vom VDE-Präsidium beschlossenen Genehmigungsverfahrens unter der oben angeführten Nummer in das VDE-Vorschriftenwerk aufgenommen und in der „etz Elektrotechnik + Automation" bekannt gegeben worden.

Vervielfältigung – auch für innerbetriebliche Zwecke – nicht gestattet.

ICS 35.240.50

Ersatz für
DIN EN 61508-2
(VDE 0803-2):2002-12
Siehe Anwendungsbeginn

Funktionale Sicherheit sicherheitsbezogener elektrischer/elektronischer/programmierbarer elektronischer Systeme – Teil 2: Anforderungen an sicherheitsbezogene elektrische/elektronische/programmierbare elektronische Systeme (IEC 61508-2:2010); Deutsche Fassung EN 61508-2:2010

Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems (IEC 61508-2:2010); German version EN 61508-2:2010

Sécurité fonctionnelle des systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité – Partie 2: Exigences pour les systèmes électriques/électroniques/électroniques programmables relatifs à la sécurité (CEI 61508-2:2010); Version allemande EN 61508-2:2010

Gesamtumfang 104 Seiten

DKE Deutsche Kommission Elektrotechnik Elektronik Informationstechnik im DIN und VDE

Einzelverkauf und Abonnements durch VDE VERLAG GMBH, 10625 Berlin
Einzelverkauf auch durch Beuth Verlag GmbH, 10772 Berlin

Preisgr. 51 K
VDE-Vertr.-Nr. 0803013