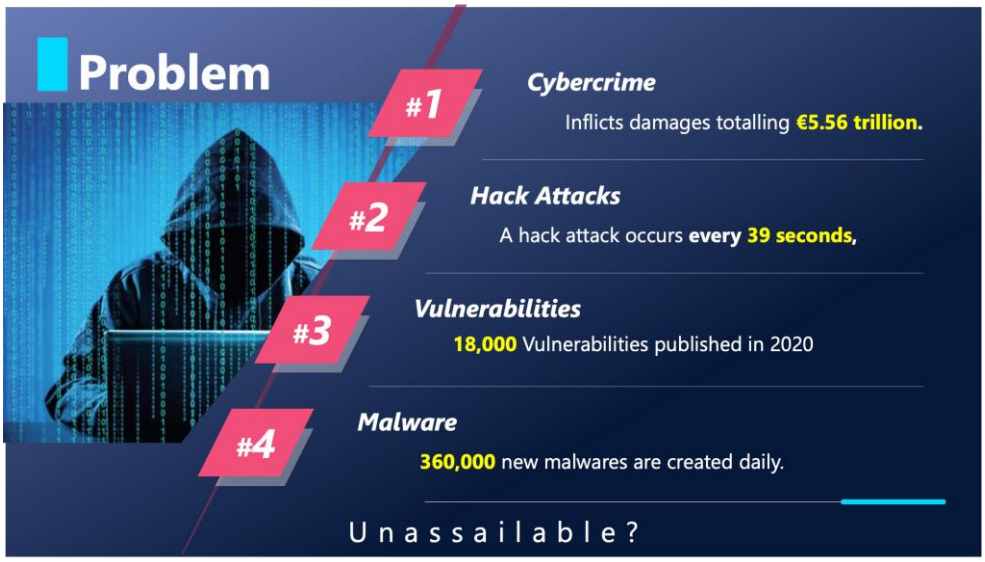
Zero Vulnerability Computing (ZVC) for Open Source Connected Devices
Acronym: ZVC4IoT

Horizon Europe Call (21st October 2021): Topic ID: HORIZON-CL3-2021-CS-01-02

#	Participant organization (acronym)	Type	Country	Expertise
P01	University of Piraeus Research Center, Dept of Informatics (UPRC)	UNI	EL	Project coordination, security architectures, malware analysis, threat analysis, applied crypto
P02	Blockchain 5.0 O.Ü. (BC5)	SME	EE	Product development, cybersecurity-by-design, software architecture, decentralization
P03	University of Thessaly, Dept. of Informatics & Telecom. (UT)	UNI	EL	Pervasive computing, Pervasive data science, Distributed Systems, Edge ML/DL, IoT
P04	Eurecat Technology Centre (EUT)	RES	ES	Medical Devices, IoT, Data and process management, AI
P05	CISPA Helmholtz Center for Information Security (CISPA)	RES	DE	Cybersecurity and Cryptography
P06	Zanasi Alessandro SRL (ZAS)	SME	IT	Cybersecurity, cyber risk assessment, ML and AI
P07	Ethniko Kentro Erevnas Kai Technologikis Anaptyxis (CERTH)	RES	EL	AI-based cybersecurity, IoT middleware, Apps in Health, User acceptance/human factors in research
P08	Autonio Foundation Ltd. (AFL)	NPO	UK	Artificial Intelligence, ML/DL, Decentralized AI, IPFS, P2P networking
P09	SBA Research Gemeinnutzige GmbH (SBA)	RES	AT	Cybersecurity, Penetration Testing, Data privacy, Machine Learning (ML), ML Security & Privacy
P10	Université de Lorrain, Laboratoire Lorrain Recherche en Informatique et ses Applications (UL)	UNI	FR	Architectural & Algorithmic integration of ML Tools, POD Management & Analytics, Intelligent Security Policy Enforcement



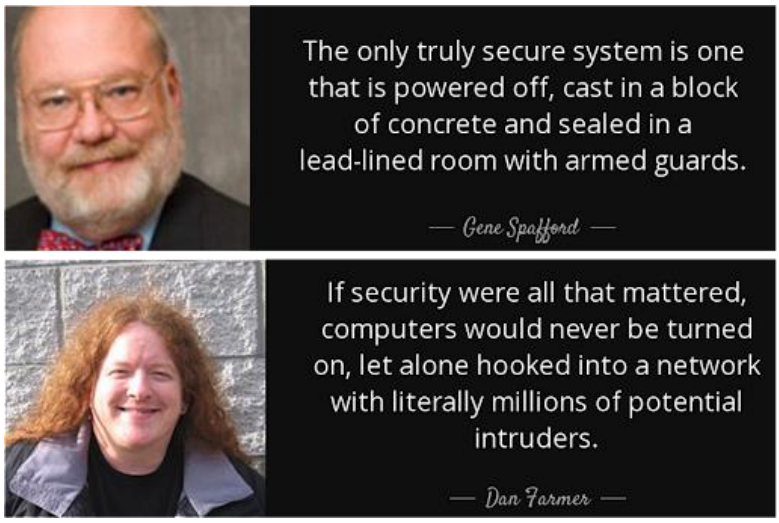


Table of Contents

Abstract:

Cybercrime costs the global economy €5.6 Trillion annually. This is essentially because fool-proof cybersecurity of personal data in a connected computer is impossible. We are challenging that maxim and disrupting the status quo in cybersecurity with Zero Vulnerability Computing (ZVC). Two mandatory design attributes make computers usable, but also render them vulnerable. These necessary evils are:

1) *The permissions that computers grant to 3rd party applications, which bad actors and threat agent often abuse to create attack surface and vulnerabilities that attack vectors may exploit;*
2) *The inherent vulnerability of data stored in-computer storage against an already compromised system.*

In typical computers neither the attack surface can be completely eliminated, nor can a connected device hold data offline, rendering fool-proof cybersecurity practically impossible. **ZVC4IoT** responds to the challenge of implementing zero vulnerability computing systems for specific environments, by designing, developing and integrating two radical paradigms:

- **Supra Operating System (SOS)**: a middleware software that obliterates the primary attack surface and,
- **In-Computer Offline Storage (ICOS):** a hardware module that isolates critical data requiring sporadic access, in cold storage *within the connected device* itself.

The combination of these two-novel encryption-independent security paradigms, when properly designed in specific execution environments such as IoT devices, may lead to a computing environment with a very high cybersecurity assurance, against very strong and capable adversaries.

Internet of Things (IoT) devices became the most commonly attacked computing devices in 2019. With the IoT devices on the rise, this trend is exponentially growing. This is further worsened by the restricted environment of IoT devices that impose limitations on implementing complex security schemes making IoT security a real challenge. ZVC's **"Cybersecurity by Design"** approach is based on a hypothesis that is currently under investigation at IMEC labs, Belgium, under H2020 grant. The main goal of **ZVC4IoT** is to establish the plausibility and efficacy of the ZVC framework in providing an end-user environment that will exhibit nearly zero exploitability for connected devices, particularly within the restricted *Edge-IoT environment*. As proof of concept, we will design and implement ZVC in a typical Edge Network architecture, with 3 use cases that will evaluate characteristic scenarios involving pure IoT devices (such as smartwatches), hybrid devices (e.g., mobile phones) and high capability computing devices (laptop, PC) as edge devices. The implementation of this ambitious goal will be supported through a well-defined and complementary consortium with strong background in cybersecurity that involves 6 participants from the 4 EU-funded pilot projects (**CyberSec4Europe**, **CONCORDIA, SPARTA & ECHO**) for developing Cybersecurity Competence Network along with other participants with strong background cybersecurity, cryptography, hardware, machine learning and dissemination / exploitation background.

ZVC
Zero Vulnerability Computing

1. Excellence:

1.1. Objectives and Ambition

Cybercrime inflicts damages totaling €5.6 trillion annually. A hack attack occurs **every 39 seconds,** and about **300,000** new malwares are created daily. Today over 4.5 billion connected devices remain at risk of cyber-attacks. With the exponential proliferation of IoT devices and the ever-growing vulnerabilities of connected devices, the cybercrime industry is poised for unstoppable growth. Experts unanimously agree that fool-proof cybersecurity is impossible, essentially because of the following two mandatory design attributes that legacy computers have to comply to make them usable:

(a) **Permissions** that 3rd party applications need to run, but which bad actors often exploit to introduce vulnerabilities resulting in an attack surface that is exploited by malware.

(b) **In-computer data storage** without which using, processing and saving data will become impossible. However, since most computers remain connected, the stored data is continuously exposed to hackers. Hence, any data stored in a networked computing device is considered a priori at risk.

Both these **necessary evils** are the main enablers of cybersecurity breaches. State-of-the-art cybersecurity techniques are limited to strategies that reduce the attack surface, and encrypt data stored in online devices to counter these evils. These approaches however have known limitations, and are often complex, making cybersecurity experts conclude that fool-proof cybersecurity is impossible[1]. Cybersecurity experts unanimously agree[2] that data within a connected device can never be entirely secure because network exposure can never be risk-free.

Future computing: Everything is a connected computer, everything is vulnerable: Advances in computer science and IoT computing are running at ultra-high speed. We are looking at a future where everything will become a connected computing device.[3] Toys, clothes, cars, door locks, contact lenses, clothes, toasters, refrigerators, washing machines, fish tanks, light bulbs, toothbrushes, glasses, helmets — you name it, are getting "smart." Everything is becoming a branch of computer science.

"Everything is now a computer. The digital nightmare is about to get much worse." Bruce Schneier in his latest book **"Click Here to Kill Everybody:**[4]

1.1.1. New World, New Rules: The challenge of Zero Vulnerability Computing

The architects of the legacy systems made perfectly reasonable engineering trade-offs for their world. But our world is very different. The rules governing the computers of their world may not be defensible or preventable, but the new world of **Zero Vulnerability Computing (ZVC)** is challenging those old rules with two new rules that deliver a defensible computing environment.

ZVC proposes a vision of a secure system with (nearly) zero vulnerability surface. Turning on a computer and still keeping the stored sensitive data inaccessible from attackers, is one 'impossibility' in the prior art that this proposal challenges by creating In-Computer Offline Storage (**ICOS**). Completely obliterating the attack surface of computing devices is also considered a de facto impossibility is cybersecurity research. The Supra Operating System **(SOS)** software layer envisaged by ZVC will respond to this research challenge by minimizing the attack exposure for various software layers. ICOS and SOS are therefore two radically novel components of ZVC, which will be combined with well-crafted encryption mechanisms, suitable for targeted computing environment, along with ML-enhanced security controls, to provide strong security guarantees for various cases of IoT computing devices.

1.1.2. Hackers' Double Jeopardy: ICOS & SOS

1.1.2.A) ICOS (In-Computer Offline Storage)

[1] Gene Spafford: "*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then, I have my doubts."*
[2] CLTC, Berkley: *This is a world in which the promise of secure digital technology turns out to be in many respects a poisoned chalice."*
[3] https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html
[4] *Steven Aftergood.* Governments want your smart devices to have stupid security flaws. *Nature* 560, 550-551 (2018). *doi: https://doi.org/10.1038/d41586-018-06033-9*

ICOS of the network vulnerabilities. secures in-computer data as a function of Zero Vulnerability Computing: directly threatens over 4.5 billion connected personal devices of citizens globally. Adding the 21.5 billion IoT devices, a total of over 25 billion connected devices remains at risk. Cybercrime No data is safe unless offline. But offline severely hassles data accessibility making us wonder why computers don't have built-in offline storage? Our answer is ICOS: the world's first in-computer offline storage (ICOS) device with an easy user-controlled instant OFF/ON toggle switch for secure data management. https://skfb.ly/oooIs

In the state-of-the-art all in-computer data storage mandatorily remains online if the computer is connected. There's no way for a networked device to keep data offline, and still stay connected. It is, for this reason, foolproof cybersecurity of computers, or for that matter, IoT is considered impossible. ICOS challenges the impossibility of designing a storage device that can be permanently hosted on any connected device and still remains offline and seamlessly accessible at all times via a toggle switch for instant accessibility.

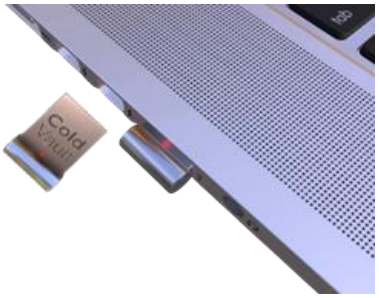


Figure 1: ZVC integrated to PC

In-Computer Offline Storage, our novel design delivers a major paradigm shift in hardware architecture of future computing devices, introducing for the first time in the history of computers, in-computer offline storage (ICOS) hardware for securing Personally Identifiable Information (PII) from the perils of cyberthreats.

Blockchain 5.0 Ltd recently disclosed in a patent application 5 iterations of ICOS (In-computer offline storage) hardware design to achieve zero vulnerability computing (ZVC, US patent Application 63/228,122, August 1, 2021). Two of those iterations can be adapted for IoT devices as illustrated in the following drawings:

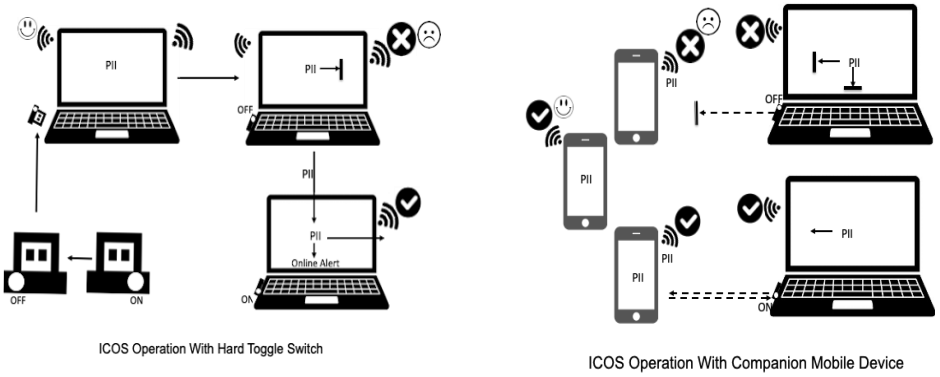


Figure2: ICOS operation in different settings

1.1.2.B) Supra OS (SOS)

Obliterating the attack surface: An attack surface is essentially the entire external-facing area of a computing environment. It contains all of the vulnerabilities or attack vectors a hacker could use to gain access to a computing system. The "attack surface" is simply the total digital resources that are exposed to threats across the enterprise. It may be exploited at hardware, firmware, at Operating System (OS) level (primary attack surface) or even via application layer (secondary attack surface). The magnitude of the attack surface is directly proportional to the density of vulnerabilities.[5]

[5] Younis, Awad A; Malaiya, Yashwant K. Relationship between Attack Surface and Vulnerability Density: A Case Study on Apache HTTP Server. Proceedings on the International Conference on Internet Computing (ICOMP); Athens : 1-7. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp). (2012)

As illustrated in Figure 3, the SOS completely obliterates the attack surface by banning all 3rd party permissions to install on the computer. However, it allows 3rd party applications to run remotely.

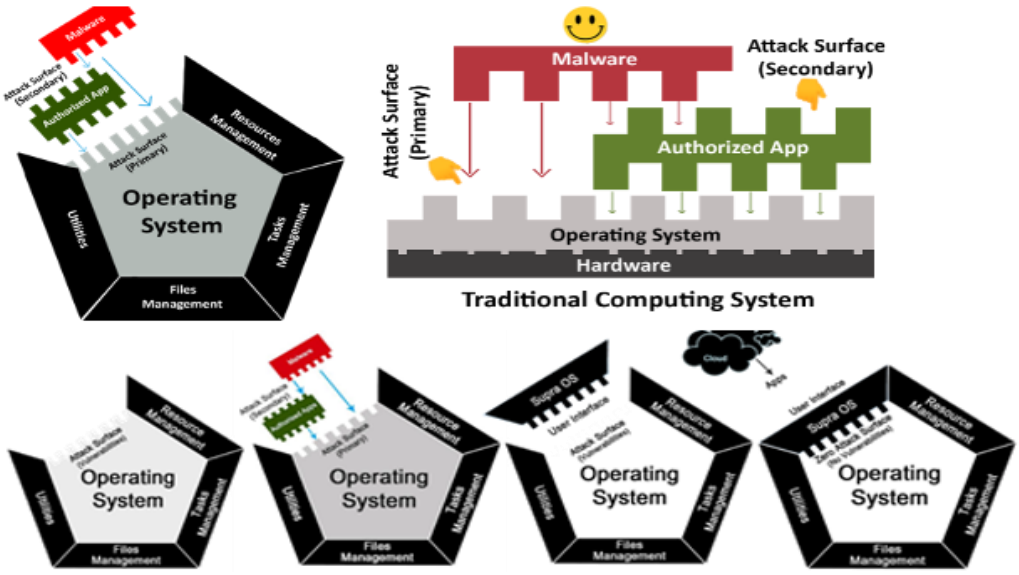


Figure 3: Illustration of the Attack Surface (OS &

The implementation of SOS in this project will be a lot more minimalistic than its implementation in the traditional computers, because most IoT devices operate in restricted computing environments, and may not even have a proper OS to run applications, which directly run on the firmware. Examples of such IoT devices are plenty viz. different types of sensors, cameras, drones and some of the home appliances.

***Attack Surface and the State of Cybersecurity*:** Since the birth of the Internet and the cybercrime industry, the attack surface has been growing. The severity of vulnerability or CVE (common vulnerabilities & exposures) is also growing. NVD (National Vulnerability Database)[6] provides qualitative severity rankings in the scale [*Low-Medium-High*] depending on CVSS (Common Vulnerabilities Scoring System) as defined in the CVSS specification,[7] which scores between 0-10 in increasing order of severity. Of the top 50 products[8] reporting the total number of distinct vulnerabilities in 2020, OSs were directly or indirectly responsible for almost all the reported vulnerabilities.

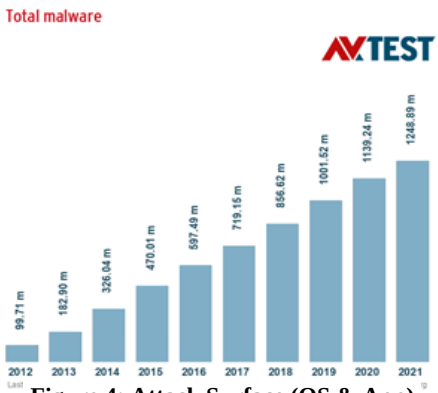


Figure 4: Attack Surface (OS & App)

With the advent of IoT and the proliferation of connected devices, attack surfaces and consequently vulnerabilities have exponentially grown. Every day, the AV-TEST Institute registers over 350,000 new malicious programs (malware) and potentially unwanted applications (PUA). Over the past decade, malware has grown from about 100 million in 2012 to 1.3 billion in 2021.[9]

In the current state-of-the-art, the approach to improving the security of a computer system is to measure the attack surface[10] of a computer system and minimize it with the following basic strategies: i) reducing

[6] https://nvd.nist.gov/vuln-metrics/cvss
[7] https://www.cvedetails.com/
[8] https://www.cvedetails.com/top-50-products.php
[9] https://www.av-test.org/en/statistics/malware/
[10] Canella, C. et al. (2019). "A systematic evaluation of transient execution attacks and defenses."In 28th USENIX Security Symposium, pp. 249-266.

the amount of code running, ii) reducing entry points available to untrusted users, and, iii) eliminating services requested by relatively few users.[11] The Zero Trust architecture by NIST is also suggesting a similar strategy.[12] Although attack surface reduction helps prevent many security failures, it does not mitigate the damage an attacker could inflict once a software vulnerability is found.[13]

Open Source, Open Specification Increases Exploitation Speed & Zero-Day Vulnerabilities: Code reuse is a common practice in software development due to its various benefits. Use of both commercial and open-source components in development increases vulnerabilities. However, such practice causes large-scale security issues since one vulnerability may appear in much different software due to cloned code fragments.[14] The rising trend has become a major reason for the constantly expanding attack surface in the past decade. Zhang et al[15] recently demonstrated that many seemingly unrelated software apps actually share a significant common attack surface. On top of the software development trends that increase the attack surface, the time frame of vulnerability exploitation has compressed by 93%. Now it is only 3 days before a vulnerability is exploited, compared to 45 days in 2006.[16] Cybersecurity Ventures[17] predict zero-day cyber-attacks to rise from one per week to one per day.

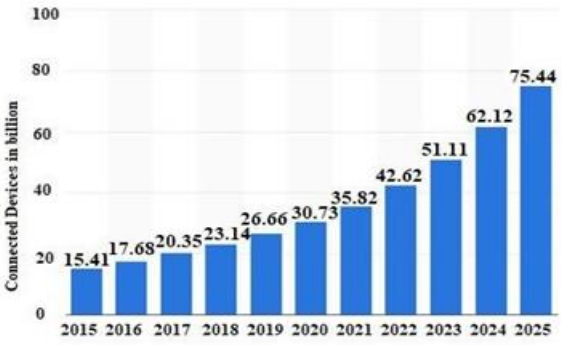


Figure 5: Vulnerability Exploitation

Cybersecurity Worsening: Recent reports forecast a surge at 12.6% CAGR by 2027. With the proliferation of IoT devices, predicted to reach 75 billion by 2025,[18] the attack surface will exponentially grow, increasing security vulnerabilities across the board. Such extraordinary growth of a problem that's already serious will warrant extraordinary measures. Are our current cybersecurity strategies enough? Let's review them.

1.1.3. Existing technologies for offline storage

In legacy systems, offline storage refers to any storage medium that must be physically inserted into a system every time a user wants to access or edit data. Offline storage can be any type of internal or external storage that can easily be removed from the computer.

Offline storage is any storage that is not currently online, live or connected to the computer. The data stored in offline storage remains permanently in the storage device even if it's disconnected or unplugged from the computer after the data has been stored. Offline storage is generally portable in nature and can be used on different computer systems. Common examples of offline storage include floppy disks, compact disks and USB sticks. Offline storage is also known as removable storage.

In computers of prior art data storage constitutes one of the key components of computer architecture. However, there is no provision or concept of offline storage within a computer. In other words, when a computer connects to the Internet, the stored data by default also goes online, exposing it to network risks. Hence, the state-of-the-art is

[11]Filho A.S., Rodríguez R.J., Feitosa E.L. (2020) Reducing the Attack Surface of Dynamic Binary Instrumentation Frameworks. In: Rocha Á., Pereira R. (eds). Developments and Advances in Defense and Security. Smart Innovation, Systems and Technologies, vol 152. Springer, Singapore.
[12] Stafford, V. A. "Zero Trust Architecture.", NIST Special Publication 800-207. Gilman, E. & Barth, D. (2017). Zero Trust Networks. O'Reilly Media, Incorporated.
[13]Manadhata, P.K., Wing, J. (2010) "An attack surface metric." IEEE Transactions on Software Engineering 37.3: 371-386.
[14]I. Stellios, P. Kotzanikolaou, C. Grigoriadis, "Assessing IoT Enabled Cyber-Physical Attack Paths Against Critical Systems", Computers & Security, 2021, 102316, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2021.102316.
[15]Zhang M., et al. (2019) CASFinder: Detecting Common Attack Surface. In: Foley S. (eds) Data and Applications Security and Privacy XXXIII. DBSec 2019: Data and Applications Security and Privacy XXXIII, *Lecture Notes in Computer Science* vol. 11559, pp. 338-358.
[16] https://www.kennasecurity.com/blog/the-new-application-attack-surface/
[17] https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
[18] Internet of Things (IoT) connected devices from 2015 to 2025 (in billions) https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/

completely blank in terms of the ICOS that we recently introduced in experiments conducted at IMEC under a Horizon 2020 grant (see Section 1.1.5 for more details).

1.1.4. Existing technologies for secure execution environments

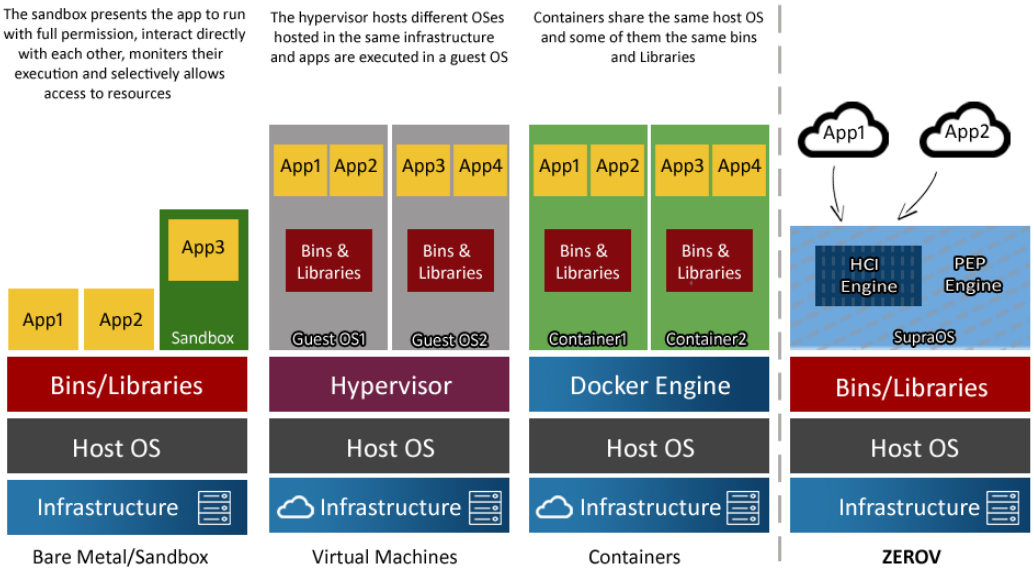


Figure 6: Existing Technologies for Execution Environment vs the SOS / ZEROV Architecture

To cope with the ever-increasing demand in hardware and provide solutions to the aforementioned exploitation of vulnerabilities in program execution, libraries and the OS APIs, different kinds of architectures such as sandboxes, virtual machines and containerized application systems have emerged (Figure 6).

Sandboxing was the first practice to establish the concept of running code in a safe, isolated environment that mimics end-user OS APIs. Sandboxes run as software in the application layer of existing OS, and execute potentially dangerous system calls inside a controlled environment. Sandboxes are inefficient in deploying complicated security policies, do not scale, and cannot protect the OS from various existing monitor bypassing attacks.

Virtual machines (VMs) are the typical building blocks for cloud infrastructures to gain higher hardware resources utilization while preserving execution isolation among different computing instances.[19] A host OS is isolated through a hypervisor engine, and Guest OS are run in a protected environment. Execution within a Guest OS only affects the Guest OS API and its underlying software without ever reaching the Host OS and its infrastructure. Still, from an execution perspective, having a dedicated OS for each VM and the full set of underlying software suggests that the attack surface and relevant security aspects for the VM themselves do not differ from that of physical machines9. On top of that, various attacks exist that can escape the isolated environment and attack the host OS by leveraging the abundant resources found within the Guest OS of a VM[20].

Containerized applications, such as Docker and LXC (Linux Containers), emerged as an alternative to VMs by providing a convenient way to deploy and isolate applications without installing a Guest OS and relevant auxiliary software necessary in a VM. Since there is no Guest OS virtualization in a container, the attack surface bound to each Guest OS and its software services cannot be exploited. However, as containers share the same underlying host kernel, access to containers is not easily secured, and even though docker isolates parts of the underlying Host OS API from containerized software can be an issue for multi-tenant security11.

[19] Zhang, Qi & Liu, Ling & Pu, Calton & Dou, Qiwei & Wu, Liren & Zhou, Wei. (2018). A Comparative Study of Containers and Virtual Machines in Big Data Environment. 178-185. 10.1109/CLOUD.2018.00030.
[20] Molina Zarca, A., Bernal Bernabe, Skarmeta, A. et al. (2018). Enhancing IoT security through network softwarization and virtual security appliances, International Journal of Network Management 28 (5), e2038

Conclusion: *"Complexity is the worst enemy of security, and this is especially true for computers & the Internet."*[21] Complexity opens up the door to vulnerabilities. Unfortunately, advancement in computers has always been associated with an increase in complexity. The more complex a system, the more vulnerable it gets to security threats. It's time we reversed the trend and got rid of all the complexities ingrained in the legacy systems. ZVC kills the complexities with two major structural changes in the basic design of computers. Firstly, it prohibits all third-party permissions at OS/firmware/application level; and, Secondly, it isolates personal data with offline storage within the connected device itself.

1.1.5. Zero Vulnerability Computing (ZVC): The first evidence

ZVC4IoT will explore and extend the initial results of a Horizon 2020 (Fed4Fire+) sub-grant pursuant to the H2020 grant agreement number: 732638 that the ZVC project won earlier this year to build ZVC's first proof of concept at IMEC's Virtual Wall testbed facility. These experiments demonstrate the efficacy of the ICOS and SOS modules in a highly restricted environment of a USB-mounted connected hardware wallet setting. The ICOS module keeps the data secure offline except when needed for processing. The SOS module completely obliterates the attack surface on the hardware wallet by banning all third-party permissions. While these findings are preliminary demonstrating potential feasibility of the ZVC concept, this new computing paradigm needs to be further tested and validated in more challenging mainstream computing environments such as the Edge-IoT networking environment in this project.

1.1.6. The Ambition

Digital disruption caused by malicious cyber activities, not only threatens our economies but also our way of life, our freedoms and values, and even tries to undermine the cohesion and functioning of our democracy in Europe. Regardless of the economic, political or personal motivations behind the cyber threats, securing our future wellbeing, freedoms, democratic governance, and prosperity depend on improving our capacity to shield the EU from malicious attacks and to address digital security weaknesses in general.

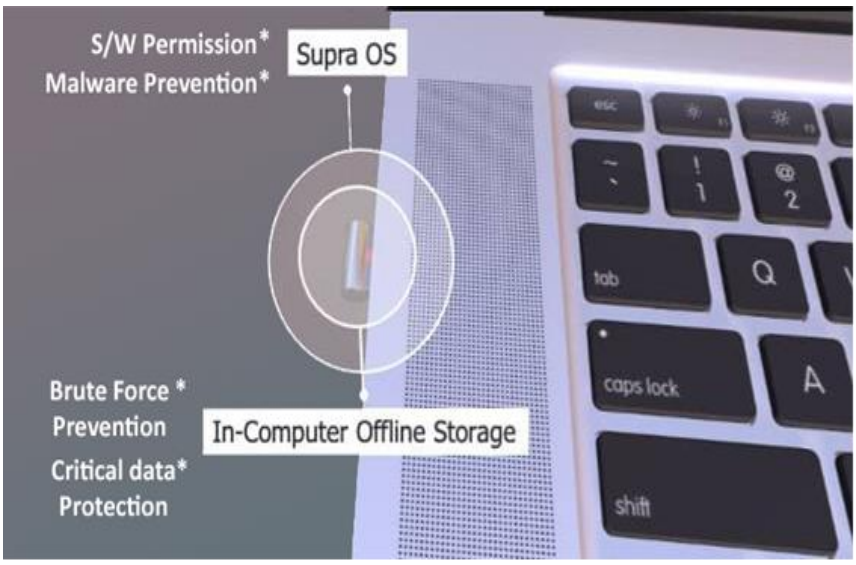


Figure7: The ZVC-powered Hardware Wallet Device with integrated SOS & ICOS attached to PC

The digital transformation requires improving cybersecurity substantially, so as to ensure the protection of the increasing number of connected devices and the safe operation of network and information systems that power our everyday activities, such as managing power grids, drinking water supply, distribution services, vehicles and transport systems, hospitals and the overall health system, finances, public institutions, factories, and homes. Europe must build resilience to cyber-attacks and create effective cyber deterrence while making sure that data protection and the freedom of citizens are strengthened. ZVC meets and exceeds those objectives and appeases EU ambition to gain a leadership position in electronic consumer devices in general and cybersecurity in particular. The ultimate long-term vision of ZVC is very ambitious to "place in every hand a computing device that will potentially eradicate cybercrime." ZVC4IoT is one of our baby steps towards that vision. Presenting a revolutionary new approach of creating in-computer offline storage (ICOS) within a network-connected device and completely obliterating the attack surface forcing hackers into double jeopardy.

[21] https://bdtechtalks.com/2016/11/29/what-bruce-schneier-teaches-us-about-iot-and-cybersecurity/

1.1.7. The Objectives

The main goal of the ZVC4IoT proposal is to unequivocally prove the plausibility and efficacy of the ZVC concept that will provide an end-user execution environment exhibiting (nearly) zero exploitability for restricted (IoT) connected devices, particularly within the restricted environment of Edge-IoT (Edge Node - End IoT Node) framework. As proof of concept, we will design and implement ZVC architecture on a typical IoT computing hub device such as a laptop, PC or a smartphone. Our envisaged TRL4 ZVC prototype will be used to validate the security assurance level that ZVC provides to the connected devices through extensive vulnerability and security testing. Following a well-defined communication and exploitation plan, the scientific results of ZVC4IoT will be further exploited by disseminating the concept & planning the next mission towards our vision.

Table 1.1.7: Specific objectives of the ZVC Research and Innovation Action

Specific objectives	Key deliverables	WPs
Technology: To define requirements/specifications & architecture of the ICOS and SOS components of the ZVC ecosystem as an enabling technology, and of its derivative use-cases.	- D2.2-4 Specifications & Architecture - D2.5 Innovation report	WP2 M1-36
Proof-of-Concept (POC): To build a ZVC framework prototype as POC, consisting of an Edge device (Laptop PC) with full ZVC implementation (SOS & ICOS components), and an End Node IoT device (Smartwatch) with SOS deployment.	- ZVC POC (PC and Smartwatch devices) - Mobile phone as alternate ICOS prototype - Audit ZVC Devices - Repository deposit	WP3 M7-29
Validation: To test & validate the ZVC framework in a controlled Edge (Laptop PC) - IoT (smartwatch) computing environment in BYOD (Bring Your Own Device) setting. Explore Mobile phones as alternate Edge Node / IoT devices. To review & secure IPR	Test & validate ZVC in PC-Mobile, PC-IoT, Mobile-IoT BYOD setting. `Filled patents ≥ 2`	WP4 M12-33
Communication, Dissemination and Exploitation: To involve stakeholder groups (See Section 2.2) via a wide range of activities, which will help us to exploit the project results and pave the way for their future market uptake.	D5.2 CDE Plan D5.4 E-learning materials EU Cluster Days	WP5 M1- 36

ZVC4IoT is a radical concept, and as such, it may face significant uncertainties in terms of cultural & socio-technical acceptability and the inherent technology risk. To address these uncertainties, our research approach will follow a risk alleviating strategy, while our research methodology will be based on a systematic and modular research approach and critical review of the intermediate results in a continuous, two-step *research-testing validation* process. Cross-functional collaboration between the consortium members will be the key to implementing the development methodology. Active participation of partners will be crucial at every stage for achieving all the project objectives. Our methodology observes high standards of research practices, maintainability, performance, and robustness, focusing on the following development tracks:

1.1.7.A) ZVC4IoT Framework – The Enabling Tech: In WP2, the state of the relevant research work and existing technologies will be thoroughly reviewed and properly extended. The results produced in WP2 will lead the detailed architecture of the core components of ZVC4IoT. In WP3, we build the hardware component (ICOS) and the software component (SOS, Post Quantum Crypto modules and ML-assisted security layer) of the ZVC framework in the context of Edge Computing Continuum for the connected IoT devices. The ICOS hardware is integrated with the Edge device (e.g. Laptop, PC), while the SOS software component of the ZVC framework installs on the End-

Node IoT device (e.g. Smartwatch – see Sect. 1.2.5). The backend of the ZVC ecosystem is decentralized to secure data using open-source SOLID (Social linked data)[22] based on Personal Online Data Storage (PODs) technology.[23]

The ICOS hardware integrated within the Edge device stores all confidential data requiring sporadic access in ICOS, a switchable offline storage that feeds the End Node IoT device as and when needed. The ZVC prototype devices are designed for testing and validating in a typical corporate BYOD setting as risk-mitigating hack-proof corporate devices. In order to be compatible with the heterogeneous computing environment, they need to rely on advanced cryptographic delegation (and reverse delegation) techniques beyond the state-of-the-art, such as fully homomorphic encryption[24] and laconic cryptography[25]. These techniques need to be specifically developed to suit the project and also to be integrated with the architecture and use cases. In particular, ICOS will protect data requiring sporadic access; homomorphic encryption will secure data at the edge side that require frequent access; and finally laconic encryption will secure the IoT-Edge communication in an efficient yet highly secure way.

In addition, security will be enhanced by utilizing a Machine Learning (ML)-based Intrusion Detection System (IDS) that: (i) identifies tampering attempts to the hardware components of the ZVC, and (ii) extracts behavioral characteristics of the users of the devices so that when malicious users access them to be identified and blocked. For that, ML as well as Deep Learning techniques will be utilized, based on previous methods and tools established by project partners[26]. Moreover, the user experience may be improved by implementing self-governing, legal, social and ethical rules that use ML/DL modules to compile, collate and analyze users' collective wisdom to boost AI. The usage of ML/DL models for boosting AI in cybersecurity from user data is emerging as a leading approach in the literature, and, mostly, the main challenges are *accuracy*[27] of the ML/DL tasks (e.g., classification, prediction, etc.) with respect to the complexity and the heterogeneity of models and data, and *scalability* of the ML/DL tasks with respect to computationally-expensive environments such as middleware and IoT. Although ZVC main security components (SOS and ICOS) are independent of cryptography and AI, these techniques are deployed to secure other components such as data requiring continuous access in the end devices, and to improve user experience. The ZVC Proof of Concept and use cases are tested and validated in WP4, while the validation results stimulate the second loop of testing and final validation.

1.1.7.B) Exploring mainstreaming of ZVC: Based on the research and validation results of the edge computing IoT scenarios tested in controlled BYOD settings, ZVC can be further explored through open-source specifications, for other potential mainstream deployments in diverse hardware and software configurations, as unhackable computing devices of the future. ZVC4IoT will represent a real testbed for future ZVC real-world use cases. The methodology will also explore the interoperability and platform-agnostic possibilities of the ZVC framework.

[22] Mansour, E., Sambra, A. V., Hawke, S., Zereba, M., Capadisli, S., Ghanem, A., ... & Berners-Lee, T. (2016, April). A demonstration of the solid platform for social web applications. Proc. 25th Int. Conf. on the World Wide Web (pp. 223-226).
23 https://solidproject.org/users/get-a-pod
[24] Joux, Antoine. "Fully homomorphic encryption modulo Fermat numbers." *IACR Cryptol. ePrint Arch.* 2019 (2019): 187.
[25] Döttling, N., Garg, S., Goyal, V., & Malavolta, G. (2019, November). Laconic conditional disclosure of secrets and applications. In 2019 IEEE 60th Annual Symposium on Foundations of Computer Science (FOCS) (pp. 661-685). IEEE.
[26] Iliou Christos, Kostoulas Theodoros, Tsikrika Theodora, Katos Vasilis, Vrochidis Stefanos, Kompatsiaris Ioannis. "Detection of Advanced Web Bots by Combining Web Logs with Mouse Behavioural Biometrics." *Digital Threats: Research and Practice* 2, no. 3 (2021): 1-26.
[27] Cuzzocrea, A., Fadda, E. & Mumolo, E. Cyber-attack detection via non-linear prediction of IP addresses: an innovative big data analytics approach. Multimed Tools Appl (2021). https://doi.org/10.1007/s11042-021-11390-1

1.1.8. The breakthrough beyond state-of-the-art: The ZVC4IoT architecture

The ZVC4IoT architecture depicted in Figure 9, will be a radical shift in designing future connected computing devices, aiming to eliminate the primary attack surface completely and significantly reduce the secondary and creating in-computer offline storage within any connected device. In contrast to existing program execution architectures that aim to minimize the attack surface by isolating program execution, the **SOS module** (Figures 6 and 8) prevents the exploitation of existing OS/firmware and application layer vulnerabilities on end-user devices, by acting as a middleware that isolates and fully controls access to the underlying OS (Figures 6 and 8). More specifically, the Supra Operating System (SOS) module piggybacks on top of the target device's host OS. It consists of two main modules: (i) the Program Execution Prevention (PEP) engine preventing direct installation and/or execution of malicious software programs. (ii) A Human Computer Interface (HCI) engine allowing 3rd party apps running on SOS, without the need for any installation on the host operating system. In this way, it controls 3rd party application execution and only allows applications delivered by the Cloud Layer and remotely executed as web progressive apps through its innovative remote execution HCI interface (Fig.9).

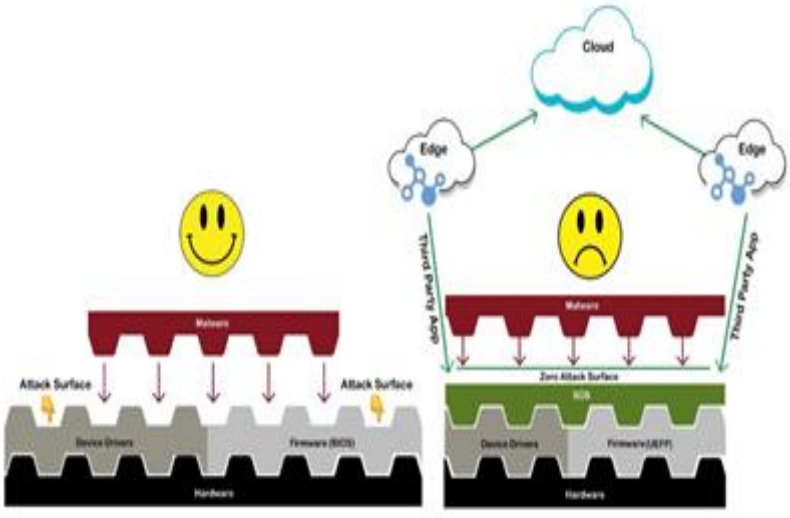


Figure 8: Legacy Vs SOS preventing app layer on the IoT firmware

In addition, non-permission-based exploitation of computers, such as brute force or authentication faking techniques can also be mitigated by deploying the in-computer offline storage **(ICOS module)** of the ZVC4IoT framework, which keeps the personal data, and other critical data requiring sporadic access offline, within the connected devices themselves. ICOS may provide strong security guarantees for various cases such as: (a) Enhancing authentication/authorization procedures that require human interaction. During the user interaction the ICOS

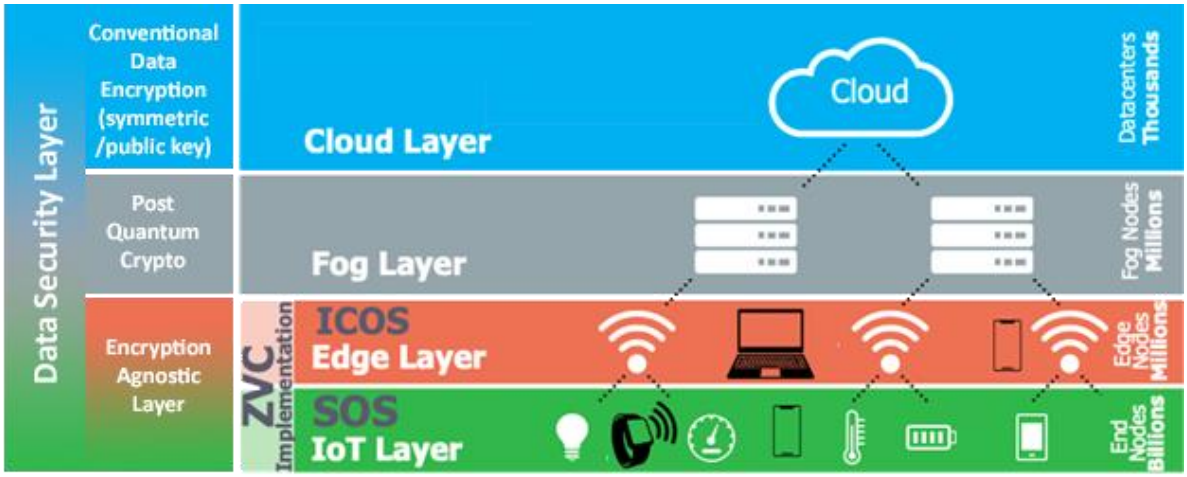


Figure 9: The ZVC4IoT architecture

module can be turned on, only during the strong authentication process. (b) secure sensitive data that require sporadic access only, again with user interaction (e.g., sporadic access to health data).

The **Post QC crypto** layer, will secure data that require continuous access, by employing cryptographic techniques that offer security without overloading the computation capability of the low-end IoT devices. This can be achieved using *reverse delegation* and *(fully) homomorphic encryption* techniques to offload computations to the Edge Computing Layer. Additionally, there is a need to achieve communication optimality by using well-chosen protocols, in particular, we want to study how the use of *laconic cryptographic protocols*[24] can contribute to this optimality. Note that this crypto layer targets both long-term objectives with asymptotically optimal systems and shorter-term ones with immediately accessible solutions, possibly offering a degraded security level compared to the long-term solutions. The security layer will be enriched with ML/AI techniques supported via the Cloud Layer. An ML-based IDS will protect: (i) the ICOS device from being tampered with, either physically, by opening the device or remotely, using specialized hardware, and (ii) the device that the SOS is installed on, by extracting behavioral characteristics of regular/baseline usage and identifying anomalies that indicate alien users are accessing the device. For the first, ML-based techniques, including clustering and multidimensional machine learning[28], will be used to define regular operation power consumption parameters and a model to detect outliers that indicate tampering. Concerning the user profiling, behavioral characteristics will be extracted, based on the keystrokes, mouse movement, the way they use the device, etc. Based on those, users will be profiled in ad-hoc classes, and ML-based models will be developed to detect anomalies and outliers, indicating that malicious users have access to the device and apply locks. However, ZVC security per se is not AI or encryption dependent. The following novel features of ZVC stand out in contrast to any state-of-the-art cybersecurity technique:

Table 1.1.8. ZVC4IoT comparison with the State-of-the-art

State-of-the-art Cybersecurity Techniques	ZVC4IoT architecture
Reduce or minimize the attack surface	SOS completely obliterates the attack surface
Reduced or minimized OS vulnerabilities	Prevent the exploitation of OS vulnerabilities
All SOTA approaches are policy/rule-based & complex, needs a specialist team monitoring	Cybersecurity-by-design delivers security by default, not policy-based with minimal or no expert supervision
Mostly server-based cloud implemented approach	Designed for client devices, although server deployment possible
Relevant to online scenarios only	Offline scenarios possible with pre-configuration
Maintains the status quo in the app market	Renders native app market obsolete as almost all apps executed at end node are cloud-edge delivered web apps
Personal data stored in a connected device is always at risk	ICOS maintains offline storage of personal data keeping it offline within a connected device
Brute force entry into computers is rewarding for hackers as personal data is accessible	Brute force attempts are protected by ICOS that secures personal data offline
Future Quantum Computing threatens the security of legacy systems	ZVC is by design resistant to future QC threats. SOS and ICOS components are crypto agnostic. The Post QC layer supports other crypto-dependent components.

Although ZVC was originally designed with mainstream computing devices in mind, recent experimentations funded under an H2020 grant (see Section 1.1.5), suggest that ZVC is perfectly suited for devices with limited computing environments. While PCs and mobile platforms have well-founded operating systems (OSs) which include inherent mitigation mechanisms, network devices have only a limited OS if any, with very little mitigations in place. Restricted environments of IoT devices impose limitations on implementing traditional security measures, such as detection and decommissioning of insecure components and vulnerabilities, delivering and implementing

[28] Cuzzocrea, Alfredo, Il-Yeol Song, and Karen C. Davis. "Analytics over large-scale multidimensional data: the big data revolution!" Proceedings of the ACM 14th international workshop on Data Warehousing and OLAP. 2011.

patches to fix vulnerabilities, effective inventory management and other complex protection schemes make the security of IoT devices a real cybersecurity challenge. In implementing ZVC in a highly restricted environment of a USB Flash device, we found that both SOS and ICOS components of ZVC were much easier to implement in such limited-resource devices as compared to full-scale ZVC implementation in full feature traditional computers for the following reasons:

- **Single Purpose or Limited Function Devices:** Most IoT devices are single purpose or limited function devices. Their restricted environment also restricts the application layer. As such they have very limited need or no need at all for mounting a variety of third-party applications. Such resource-constrained limited utility gadgets can be managed without third-party applications at all. This makes deploying SOS to completely obliterate their attack surface relatively less complex as compared to deploying SOS on a traditional full-featured computing device. However, if absolutely necessary third-party applications can run from the edge server and be delivered to the IoT device using the SOS interface.
- **Restrictions on spatial and computing resources:** IoT Interfaces are by compulsion simple and minimalist. Consequently, this makes the HCI components of the SOS less complex and minimal. And, the limited or zero need for 3rd party applications further simplifies the SOS implementation in IoT devices. Thus, in most small IoT devices, the SOS framework can be stripped down to a lightweight script directly running on the device firmware.
- **Sensitive data easy to segregate to Edge Device/Server & keep offline:** All personal data can be stored offline within a local IoT hub or an edge server device by deploying ICOS authentication and offline storage features at the edge device level such as a PC.

1.2. Methodology

We will use an agile product development strategy. Cross-functional collaboration between the consortium members will be the key to implementing the development methodology. Active participation of consortium partners will be crucial at every stage for achieving all the project objectives. Participation of the members of previously funded cybersecurity and IoT projects will add momentum to the ZVC4IoT development plan as their feedback will align with development strategies implemented in similar projects. The deployment of existing ZVC modules and components for development, validation and dissemination of the ZVC4IoT ecosystem will follow an **Agile Development Methodology** as described in detail in the next section. The methodology will be able to *demonstrate the technology in a relevant environment*, bringing our result to an overall level of TRL-5.

1.2.1. The Agile Methodology & the Innovation Cycle

Open-Source designs are frequently used in IoT technology and become more reliable and efficient with the number of developers that deploy them. The quality of open-source hardware and software for IoT and connected devices is improving. Paradoxically, while the quality of open-source hardware and software keeps improving, their zero-day vulnerability exploitation speed keeps decreasing because of the reuse of open-source codes, for their obvious benefits, as explained subsequently (Open-Source Code Reuse & Zero-Day Vulnerabilities). Although open-sourcing is a boon, its role in amplifying the attack surface and proliferating vulnerabilities cannot be overlooked. The management of this large collaborative development environment that Open Source represents is a real cybersecurity challenge.

As much as the propagation of IoT devices and their vulnerabilities is increasing, their restricted computing environment limits the deployment of the legacy security protocols. Many IoT devices do not allow the deployment of more complex protection schemes (e.g., Trusted Platform Modules, Sandboxing applications in managed memory partitions) and similar approaches that often rely on OS support to ensure cybersecurity.

A conceptual framing of the project methodology is depicted in Figure10. The starting point (01) aims for a fundamental understanding of the "**Improved security in open-source and open-specification hardware for connected devices**" call, its objectives, goals and associated policies and legislation in general and specifically pertaining to the scope to address the call challenge. And more particularly the fundamentals pertaining to the three use cases we selected for validating the concept of ZVC4IoT in the testing and validation for *Edge-IoT computing*.

1.2.1.A) The Use Cases: The motivation behind the selection of the particular use cases is to reveal the performance of the proposed architecture in an ecosystem of edge nodes (i.e., PCs) interconnected with IoT devices (e.g., mobile phones, smartwatches, etc.). Mobile phones, smartwatches or wristbands can collect physiological data (e.g., pulse, pulse-oximetry, temperature, blood pressure) or other personal data of their owners that are transferred to the edge device (e.g., a PC with the appropriate configuration). Our aim is to set up an ecosystem of edge nodes and IoT devices where we will apply and install our components to perform a set of piloting activities with the involvement of end users. Another goal for the selection of these representative edge-IoT types of devices for testing the ZVC4IoT architecture, was to be in line with the scope of the call objectives (see Sect. 1.2.2).

Scenario. The consortium will create a testbed with a number of edge nodes and IoT devices in order to host the envisioned functionalities and test the proposed components. ICOS will be placed at the edge nodes (PCs) and SOS will be incorporated into the IoT devices (smartphones). A list of PCs and smartphones will be selected based on the most appropriate 'representatives' in the market in order to meet the technical requirements derived by everyday activities of end users. The consortium will review and select a number of devices and define the means for their connection. Afterwards, we are going to involve end users (approx. 100-200 students) that will adopt our platform for a wide period. Users will be able to generate their data that will be secured by the edge nodes while the consortium records the outcomes related to significant KPIs. Data will be related to users' personally identifiable information (PII) and will be owned and processed by users themselves. For the experimentation, we will define a plan for applying simulated attacks on the infrastructure and record the outcomes related to the envisioned KPIs.

Use Case 1: PC-Mobile phone (PCMP) Configuration. The motivation behind this pilot is related with the frequent use of typical PCs and smartphones for data transferred in an upwards mode, i.e., from IoT devices to the Cloud through the mediation of the edge (PC, smartphone) infrastructure. However, there are certain risks involved with this growth, e.g., IoT devices are becoming targets of cybercriminals because of their widespread use and increasing computing power. A relevant interesting example is the fact that more than 60% of online fraud occurs through mobile phones. Apparently, there is an increased need to maintain the privacy of data and enhance the security aspects of the ecosystem to eliminate the potential attacks and breaches of the infrastructure. Given how vulnerable IoT devices are and that the threat from cyber-attacks is only expected to increase, ZVC4IoT comes into the scene to provide the means for end users protection offering ICOS and SOS as components dedicated to increase the security of IoT and edge infrastructures. The pilot will target to involve end users in a real setup and expose the advantages of the approach. We are going to present the immunity of the system over attacks and reveal our outcomes through a set of KPIs. Example KPIs (the final list will be concluded in T4.1) are: time to store the data (estimated value: ~ms); time to transfer the data to the edge node via laconic encryption (estimated value: ~ms); acceptance of cloud delivered applications via SOS (estimated value: ≥85%); response time of the platform for any service (estimated value: ~seconds). End users will adopt their smartphones to record/upload their data into our infrastructure. For the purposes of piloting, we will use anonymized data to avoid collecting personalized information being fully aligned with the GDPR regulation. Upon the provided infrastructure we will perform a vulnerability assessment and penetration testing adopting some fake attacks on both the edge nodes and the IoT devices. The plan for testing will be defined and concluded in T4.1 and the outcomes will be revealed in T4.4.

Use Case 2: Mobile Phone-Smartwatch (MPSW) Configuration. A Smartwatch or wrist band collects physiological data (e.g. pulse, pulse-oximetry, temperature, blood pressure) and biometric data (e.g. accelerometer, gyroscope, magnetometer, GPS) which is usually used to infer healthcare and wellness related information (e.g. steps taken, food and water intake, calories burned, sleep movement, breathing) which is used in applications of Active and Healthy Ageing, Behaviour recognition and Behaviour change, Chronic care management, Home Hospitalization, Integrated Care, etc. Data collected and inferred from Smartwatch is personal and needs to be preserved with the highest standards of privacy and security. Smartwatches are usually connected to a mobile phone through a short-range telecommunication protocol, currently, LE Bluetooth is the most common. The mobile phone, usually with more computation capability, works as a hub of data collection and processing from the Smartwatch and other sensors, for example, complementary environmental and/or wearable or PoC medical devices. The motivation and aim for this use case is similar to PCMP and PCSW use cases, but the configuration scenario differs. The Mobile becomes the Edge device and smartwatch, the IoT device.

Use Case 3: PC-Smartwatch (PCSW) Configuration. The motivation and aim for this use case are similar to the PCMP use case. The scenario however deploys smartwatch as an IoT device and PC as the Edge device.

1.2.1.B) The Innovation Cycle: It is envisaged that different technical and regulatory implications will apply in each case that we selected to test and validate the ZVC4IoT ecosystem, owing to the unique procedural differences in the nature of the use case, offering and context. The fundamental objective in **Step (01)** is to both understand the technical and regulatory constraints as it applies to each of the 3 use cases within the focused scope of the call, as well as understand the variability and parameters for ZVC implementation that would apply in each of the 3 use cases. **Step (02)** deals with translating the fundamental understanding achieved in (01) to clearly define the requirements and technical specifications for designing the technical architecture of the ZVC4IoT concept.

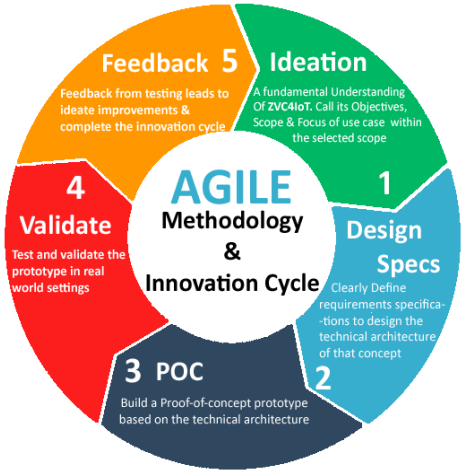


Figure 10: Methodology & Innovation Cycle

Once again, it is envisaged that different technical, procedural and regulatory implications will imply different approaches in use cases, owing to the heterogeneity in concept, capability and functionality of the 3 types of test environment we selected for field-testing (FT) the ZVC4IoT solution. The goal is to translate these into different modules that engage a user through a simple UI (and associated helper screens), to enable the user to methodologically set their preferences and navigate through the system. **Step (03)** then builds on these design decisions and produces a proof of concept (POC) that is field-tested and validated in 3 different use case scenarios in the Next **Step (04)**. The fifth and **Final Step (05)** provides crucial feedback from the users of the ZVC ecosystem leading to further ideating the improvements to complete or repeat the innovation cycle. The combined assistance from the cybersecurity, legal, ethical, and ICT expertise in the consortium will help navigate the project through the innovation cycle and deliver a robust solution.

1.2.2 Security by Design Implementation

Based on our initial work on SOS and ICOS, we will design an edge-IoT device computing framework with *zero attack surface* and *in-computer offline data segregation* to eliminate all potential vulnerabilities without much of a compromise in running application-layer that one needs to run, albeit in a different mode (remotely). In most legacy IoT devices the application layer may directly sit on firmware without the need for an elaborate OS. The firmware or device driver layer provides 3rd party permissions to run applications, which bad actors use as attack surfaces to create attack vectors that render the computing device vulnerable to malware. Hence using the combination of SOS and ICOS, along with the PQ crypto layer and the ML-supported security mechanisms, the IoT device can be fully sanitized against most malware or brute force attacks perpetrated to gain control of the device or its network. Implementation of ZVC to secure connected devices has all the advantages of "**Security by Design,**" and makes all the legacy security measures, either easier and less resource consuming, or renders them redundant, perfectly aligned with the call objectives (Table 1.2.2).

Table 1.2.2: ZVC4IoT response to the call objectives

Call objectives	ZVC4IoT response
Development of verifiable implementations of cryptographic solutions, authentication schemes, and, as relevant, software libraries that implement them securely in operating systems;	*SOS and PQ crypto layer integration*: The SOS layer will be integrated as a middleware layer between the underlying OS and the 3rd party apps and will be integrated with the QC encryption layer. *Robust Data Security:* Personally Identifiable Information (PII) stored in ICOS can be secured through the entire life cycle (storage, transmission, processing) using different homomorphic encryption or standard encryption schemes as circumstantially appropriate for authentication or any other data processing.

Develop mechanisms to mitigate hardware-related security vulnerabilities	The ICOS module will protect access to sensitive data in restricted environments, from hardware and software layer vulnerabilities.
Development of security auditing for connected devices	With ZVC effective security audits of connected devices become automatic, seamless, less complex and minimally resource consuming, particularly in restricted environments of IoT devices, via the SOS layer that isolate the underlying OS/firmware.
Development and advancing of verification methods for secure firmware updates and secure software patching in connected devices	The SOS component completely obliterates the devices attack surface prior to commissioning the device, eradicating all zero-day vulnerabilities.
Development of multi-factor authentication hardware and software solutions	The ICOS component of the ZVC ecosystem provides an integrated hack-proof method for secure multifactor hardware/software authentication, and the UEFI protocol boots the connected device to ensure secure communication within any networking environment. The ICOS component provides integrated multi-factor hardware/software authentication capabilities.
Development of the security upgrading of the connected devices within the life cycle (bootstrapping, commissioning, operational, upgrade etc)	Firmware updates can be authenticated and verified by the ICOS component of the ZVC, through secure bootstrapping and secure upgrade at any stage of the product's life cycle.

1.2.2.A) ZVC Implementation in Open Source Connected IoT Edge Network:

IoT devices became the most attacked assets for cybercriminals during 2019. And with the number of active IoT devices on the rise, this trend is only expected to increase. Smartphones can be considered as one of the most important IoT devices due to the popularity of smartphone-enabling technologies including sensors, ubiquitous connectivity, context-awareness etc. in the environment of IoT.[29] Moreover, smartphones act as the epicentre of the ever-growing IoT or rather IoX (Internet of Everything), as they usually act as the control device for various other IoT/IoX devices, at least in terms of their authentication and control as an Edge Node device. In today's IoT infrastructure, almost all IoT networks connect to Edge Node because it is closer to the IoT device and edge computing improves data management, reliable, uninterrupted connection at lower connectivity costs and better security practices. The Edge Node can be a full-scale server, a PC, a laptop or even a smartphone. Hence focusing on implementing the ZVC technology directly or indirectly in smartphones impacts the entire universe of IoT devices. That's not to say that ZVC cannot be directly implemented in individual IoT devices.

Figure 11: IoT Infrastructure

1.2.2.B) Heterogeneity of IoT devices & ZVC Edge Computing Use Cases:

There is so much diversity and heterogeneity in IoT devices that when designing, testing and validating ZVC edge computing, it is impossible to include a bunch of them. So, we selected 3 use case scenarios with PC, smartphone and smartwatch to represent the Edge and End devices in the Edge Computing Continuum. If we can demonstrate ICOS and SOS modules enabling ZVC Edge Computing Framework it can conceptually enable any open-source connected device scenario. Accordingly, three iterations of the ZVC edge computing framework are designed to test and validate 3 use cases discussed in more detail herein.

[29] Mehdia Ajana El Khaddar and Mohammed Boulmalf. Smartphone: the ultimate IoT and IoE device. Smartphones from an Applied Research Perspective, page 137, 2017. https://library.oapen.org/handle/20.500.12657/49223

1.2.3. Three Iterations of ZVC Edge Computing Framework

As much as it may be impossible to fully secure data in a networked device in legacy computing systems, ZVC creates in-device offline storage (ICOS) that is entirely under the data owner's control. Our ICOS design makes this possible without introducing any major structural changes to the device's motherboard or its housing. It introduces a switchable NAND flash memory chip using the existing USB or SD Card memory ports that users can easily control to keep their PII data offline right within their device itself while using the device for their normal online activities. Its tiny design virtually merges with the contours of the host computer, and remains mounted 24/7 without any risk of damaging itself or the host USB port. Our current design can be further improvised by mass production of miniaturized MUDP chips so that ICOS assembly of the ICOS chipset almost disappears in the host computer as illustrated in this animation (https://skfb.ly/ootNR), and the following illustration of an ICOS powered laptop device:

Figure 12: ICOS powered Laptop PC

Such ICOS powered laptop PCs serve as Edge Node servers to Smartphones / IoT devices for authenticated access within an edge network. Users can instantly bring their offline PII data online using the toggle switch whenever desired. During the short periods when the data in the ICOS is switched online, it may be further secured using cryptographic delegation techniques, including Homomorphic Encryption and laconic cryptographic protocols which can ensure that confidential data and algorithms cannot be accessed beyond their legitimate owners while allowing them to be used in global computations. Although ZVC introduces a new level of security to all types of computing devices, our proof-of-concept builds 3 prototypes around Edge Node-End Node components of a typical Edge Computing Continuum. Accordingly, we will design and build 3 use cases to test and validate the ZVC framework for connected devices. The device prototypes will include (1) ICOS-powered PC laptop; (2) SOS-powered Smartwatch; and (3) ICOS-powered Smartphone.

The ZVC prototypes developed will be tested and validated in the three (3) Edge Node - End Node - Cloud Continuum scenarios as real-world use cases, as described in Section 1.2.4.

1.2.4 Field Testing (FT) of the Use Cases

A use case is a software and system engineering term that describes how a user uses a system to accomplish a particular goal. It is basically a list of actions or event steps typically defining the interactions between an actor and a system to achieve a goal. A use case acts as a software modelling technique that defines the features to be implemented and the resolution of any errors that may be encountered. In software/hardware modelling literature there are basically two types of use cases depending on the user expectation and system performance:

i) Business Use Cases, and, ii) System Use Cases.

Business Use Cases are more about what a user expects from a system while System Use Cases are more about what the system does. The IoT device monitors users' vitals in real-time and transmits to peers in the network via always-on BLE5 mesh networking. Hence the PHAT and BLE5 are system use cases and Pre-Hospital Cardiac Preconditioning is a business use case.

1.2.5. ZVC Pilots to Field Test (FT) First Market Replication of ZVC4IoT

Conducting pilot testing of software is a good practice to validate the functionality of the system before going into production. The pilot testing group of users tries the software and hardware in totality, prior to its final launch or deployment. ZVC4IoT consortium will take the responsibility for piloting the ZVC4IoT ecosystem, at the end of which, the users will give feedback about the function, feel and the response of the software and hardware. Based on the feedback received after the completion of the pilot, the software will be tweaked and bugs removed, if any, to meet the end-user expectations. Thus, we will ensure that from the end-user viewpoint also ZVC meets all expectations. We will take care of the user experience: how easy it is for them to use the product.

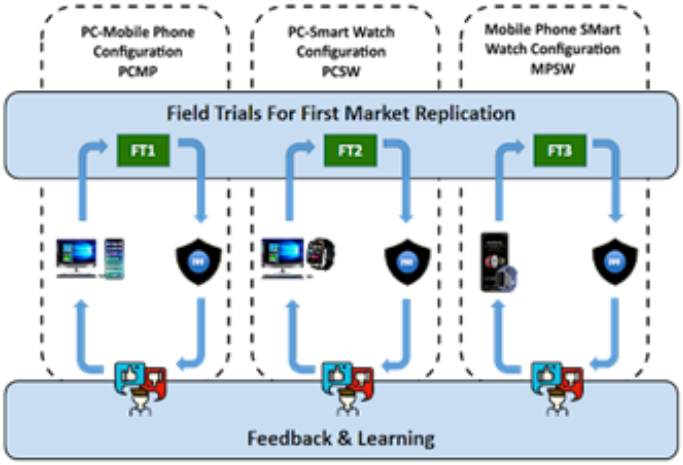


Figure13: ZVC4IoT Field trials

The consortium includes several partners with wide experience in device testing, including among others UTH, UL and EUT, who will lead the trials required to validate the 3 use cases and to demonstrate initial market replication of the ZVC4IoT infrastructure. These demonstrators will field-test the use cases in the following three Field Trials (FTs):

1.2.5.A) Use Case 1 Validation: PC-Mobile phone (PCMP)

The first iteration builds an Edge Computing network using PC as an Edge Node device and Mobile Phone as an End Node device.

Technology Deployed: In this ZVC configuration, the ICOS is implemented at the Edge Node (PC) storing offline the sensitive user data generated at the End Node, and serving it for processing when required. The ICOS chip mounts onto the host computer via either USB or SD port and functions as an in-computer offline cold storage vault with a toggle switch for the data owner to transiently switch on when data transfer or the processing is required. The Mobile Phone serves as the SOS powered End Node where data generation/processing takes place at the application layer. PCMP will be the most common configuration that users are likely to encounter in their daily lives.

Actors & Stakeholders: The main actors & stakeholders include mainstream computer and mobile phone manufacturers. UTH with experience in pervasive computing will conduct the field trial for testing and validating the SOS and ICOS components of ZVC.

Primary Objective: The primary objective is to test and validate the ZVC in a PC-Mobile Phone Edge Computing setting, wherein the ICOS is integrated into a PC / Edge server and the SOS is configured in the Mobile Phone device.

Figure14: ZVC4IoT Use case1: PCMP

Anticipated Improvements - KPIs

- Establishing an in-situ testbed for the ZVC4IoT framework with PC as the Edge device.
- Achieving a clear definition of the terms "Zero Vulnerability Computing" or “ZVC”.
- Achieving 100% connectivity between PC and Mobile Phone.
- Establish resilience of the ICOS hardware in terms of 100% failed brute force attempts.
- Establish complete obliteration of the attack surface on Mobile Phones with 100% failed attempts at running third-party applications or malware.

1.2.5.B) Use Case 2 Validation: PC-Smartwatch (PCSW)

In this ZVC configuration, like PCMP the laptop PC serves as the Edge Node device, but the End Node device is a Smartwatch. The ICOS is implemented at the Edge Node (PC) for storing offline the sensitive user data generated at the End Node online, and serving it for processing when required. The Smartwatch serves as the SOS-powered End Node where data generation and processing take place at the application layer. This configuration serves the users of Smartwatch and can be extended to any IoT device other than Smartwatch, such as Webcam, or home and computer accessories or sensors.

Figure15: ZVC4IoT Use case2: PCSW

Technology Deployed: In this ZVC configuration, the ICOS is implemented at the Edge Node (PC) storing offline the sensitive user data generated at the End Node, and serving it for processing when required. The ICOS chip mounts onto the host computer via either a USB or SD port and functions as an in-computer offline cold storage vault with a toggle switch for the data owner to transiently switch on when data transfer or the processing is required. The Smartwatch serves as the SOS powered End Node where data generation/processing takes place at the application layer. PCSW is likely to be a less common configuration that users are likely to encounter in their daily lives.

Actors & Stakeholders: The main actors & stakeholders include mainstream computer and smartwatch manufacturers. CERTH with experience in testing devices will lead the field trial for testing and validating the SOS and ICOS components of ZVC.

Primary Objective: The primary objective is to test and validate the ZVC in a PC-Smartwatch Edge Computing setting, wherein the ICOS is integrated into a PC / Edge server and the SOS is configured in the Smartwatch device.

Anticipated Improvements - KPIs

- Establishing an in-situ testbed for the ZVC4IoT framework with PC as the Edge device.
- Achieving 100% connectivity between PC and Smartwatch.
- Establish resilience of the ICOS hardware in terms of 100% failed brute force attempts.
- Establish complete obliteration of the attack surface on Smartwatch with 100% failed attempt at running third-party applications or malware.

1.2.5.C) Use Case 3 Validation: Mobile Phone-Smartwatch (MPSW)

In this ZVC configuration, a Mobile Phone is deployed as an Edge Node device, and the End Node device is a Smartwatch. The ICOS is implemented at the Edge Node (MP) for storing offline the sensitive user data generated at the End Node, and serving it for processing when required. A specially designed ICOS Chipset kit integrates into the MicroSD card slot of Mobile Phones as shown in the illustration. The Smartwatch serves as the SOS-powered End Node where data generation and processing take place at the application layer. This configuration serves the users of Smartwatch and can be extended to any IoT device other than Smartwatch, such as Webcam, or home and computer accessories or sensors.

Figure16: ZVC4IoT Use case3: MPSW

Thus, the path-breaking ZVC technology introduces zero vulnerability into computers strengthening European cybersecurity capacities and EU sovereignty in digital technologies, resulting in more resilient digital infrastructures, systems and processes, increased software, hardware and supply

chain security. This proposal will have a massive impact on the EU's IoT market share, especially since mobile devices and consumer electronics are mainly developed and manufactured outside the EU.

Technology Deployed: In this ZVC configuration, the ICOS is implemented at the Mobile Phone storing offline the sensitive user data generated at the End Node, and serving it for processing when required. The ICOS chip mounts onto the Mobile Phone via either USB or SD port and functions as an in-device offline cold storage vault with a toggle switch for the data owner to transiently switch on when data transfer or the processing is required. The Smartwatch serves as the SOS powered End Node where data generation/processing takes place at the application layer.

Actors & Stakeholders: The main actors & stakeholders include mainstream computer and mobile phone manufacturers. EUT with experience in hardware / IoT designing and testing will conduct the field trial for testing and validating the SOS and ICOS components of ZVC.

Primary Objective: The primary objective is to test and validate the ZVC in a Mobile Phone-Smartwatch Edge Computing setting, wherein the ICOS is integrated into a PC / Edge server and the SOS is configured in the Smartwatch device.

Anticipated Improvements - KPIs

- Establishing an in-situ testbed for the ZVC4IoT framework with Mobile Phone as the Edge device.
- Achieving 100% connectivity between Mobile Phone and Smartwatch.
- Establish resilience of the ICOS hardware in terms of 100% failed brute force attempts.
- Establish complete obliteration of the attack surface on Smartwatch with 100% failed attempt at running third-party applications or malware.

1.2.6. ZVC is by design resistant to Quantum Computing threats

Quantum computing (QC) is significantly affecting the security level of typical cryptosystems, as it may lead to linear solutions for cryptographic algorithms that require exponential computation time in the standard computing model. The unique properties of quantum computers would allow them to perform computations that are currently impossible with legacy computers. This could have a significant impact on the cybersecurity landscape. The ZVC4IoT architecture will provide strong QC resistance by design, by utilizing two main components as shown in Fig.9. ICOS will provide data security for data requiring sporadic access in an encryption agnostic way. The post-quantum crypto layer will secure data requiring online access with laconic encryption and homomorphic encryption techniques, specifically suited to the restrictions of each particular scenario.

1.2.7 Interdisciplinarity Approach

The domination of technological paradigms relies both on technical and socio-political forces. This calls for a stronger focus on the socio-economic and behavioural aspects of the innovation process, particularly if the tech is a radical departure from the status quo. As no paradigm shift can ever happen without multi-disciplinary engagement, ZVC will take advantage of the diverse expertise of its consortium, including software design, cybersecurity, advanced cryptology, AI and data science, machine learning and network engineering (Table 1).

The ZVC4IoT consortium has the necessary expertise to achieve the project's objectives. Interdisciplinarity can also be demonstrated in the application scenarios that could potentially benefit from the zero-vulnerability approach. These include medical IoT infrastructures, remote working and collaboration, social networks and smart cities, e-government and the new economy powered by decentralization technologies such as blockchain (e.g., cryptocurrencies).

Table 1.2.7: Overview of partners' expertise

Expertise Partners	Software Design	Cyber Security	Advanced Crypto	AI/Data Science	Machine Learning	Network Engineer.	Business / IPR	Diss./ Comm.
P01- UPRC	*	**	*	*	*	**		*
P02- BC5	**	**					**	
P03- UTH		*	*	**	**	*		**

P04- CERTH	**	**		**	**	*	*	**
P05- UL	*	**	*	**	**			*
P06- AFL	*			**	**			
P07- EUT	**	*		**	**		*	*
P08- CISPA		**	**					*
P09-SBA		**	*	**	**			
P10-ZAS	*	**		**	*		*	**

*: Sound Knowledge -- **: Expert Knowledge

1.2.8. Research data management

The aim of the data management in ZVC4IoT is to foster knowledge discovery and innovation and promote subsequent data and knowledge integration and reuse. Our consortium agrees at making our research data "as open as possible, as closed as necessary" and follows the guidelines of FAIR Data Principles. Therefore, the data will be **findable, accessible, interoperable, and reusable (FAIR).** We will also set up a **Data Management Plan (DMP, D1.2)** prior to the project start that will be updated while implementing the project proceeds. We will follow the structure of the template provided by the European Commission, which entails the following components: 1) Data summary, 2) FAIR Data, 3) Allocation of resources, 4) Data security, 5) Ethical aspects, and 6) Other procedures for data management. The DMP is a living document that will be updated as the project evolves. Table 1 provides a draft that specifies the type of data collected/generated, relevant standards, accessibility, and preservation.

Table 1.2.8.: Draft Data Management Plan

What type of data will the project generate/collect?
ZVC per se does not collect or process any personally identifiable information (PII). While its ML module may use local app-using data patterns for optimizing user experience, the PII data remains secure in HEPODs. All measures will be taken to ensure proper and sound management of the research data that will be collected, processed and generated (including any metadata)
What standards will be applied?
The ZVC framework will be GDPR compliant. Considering that some transmitted data may be regarded as sensitive, the highest security standards would be used.
How will data be exploited and/or shared/made accessible for verification and reuse?
Whether codes or project reports, all project outcomes will be made publicly available via GitHub repository, project website maintaining an access log to assure the proper use of accessed Research articles will be published in peer-reviewed journals.
How will data be curated and preserved?
ZVC4IOT will use state-of-the-art technologies for secure storage, delivery, and access of information, as well as managing the rights of the users. Some examples include public-key encryption and symmetric encryption with session keys negotiation over HTTPS.

2. Impact

2.1. Project's pathways towards impact

This proposal has significant innovation potential as its objectives and outcomes are complementary to actions under the Digital Europe Programme, Specific Objectives 3 and 4, which will strengthen EU cybersecurity capacity

by support to the deployment of cybersecurity infrastructures and tools across the EU, for public administrations, businesses, and individuals, and support digital skills in cybersecurity. Moreover, ZVC4IoT builds on the results of Horizon 2020 funded ZVC project[30] in particular and in general aligned with the pilot projects funded under SU-ICT-03-2018 that seek to establish and operate a pilot for a Cybersecurity Competence Network (CCN) to develop and implement a common Cybersecurity Research & Innovation Roadmap. All four projects funded under the EU's CCN initiative are represented in the ZVC4IoT consortium. ZVC also aligns with other relevant H2020 topics and cybersecurity activities such as those carried out by ENISA (https://www.enisa.europa.eu/) or relevant parts of the work of the EIT Digital (https://www.eitdigital.eu/). The activities of ZVC4IoT will also be aligned as relevant with the future objectives of the Network of National Coordination Centers (Commission proposal COM (2018) 630). Thus, the innovation potential of ZVC4IoT will substantially impact EU's ICT infrastructure in the following areas:

- Strengthened EU cybersecurity capacities and European Union sovereignty in digital technologies
- More resilient digital infrastructures, systems and processes
- Increased software, hardware and supply chain security
- Secured disruptive technologies
- Smart and quantifiable security assurance and certification shared across the EU
- Reinforced awareness and common cyber security management and culture

2.1.1. Key expected results, outcomes and impacts

The ZVC4IoT research lays down the foundation of a new enabling technology platform of future computing with the potential to revolutionize how computing devices will be designed to operate, how end-users access apps, and how user data will be secured from the perils of cyberspace. ZVC4IoT results carve out a credible pathway contributing to EU's Strategic Plan 2021-2024, for *"Increased cybersecurity and a more secure online environment by developing and using effectively EU and Member States' capabilities in digital technologies supporting the protection of data and networks aspiring to technological sovereignty in this field, while respecting privacy and other fundamental rights."*. ZVC4IoT achieves or exceeds all the expected outcomes that this increased cybersecurity call envisages, such as;

- *Reduced security threats of open-source hardware for connected devices*, by securing data access through the ICOS module and by securing the edge-IoT computing paradigm through the SOS module.
- *Effective management of cybersecurity patches for connected devices in restricted environments such as IoT devices*, through the SOS middleware layer that centrally controls 3rd party software installation.
- *Methods for secure authentication and secure communication for connected devices* in restricted environments, by designing and developing mechanisms for post-quantum yet efficient communications by exploring novel crypto mechanisms such as laconic key agreement protocols.

2.1.2. Resilience, Technological Sovereignty & Global Leadership

EU rules on the security of Network and Information Systems (NIS) are at the core of the Single Market for cybersecurity. The EU's critical infrastructure and essential services are increasingly interdependent and digitized. All Internet-connected things in the EU, whether automated cars, industrial control systems or home appliances, and the whole supply chains which make them available, need to be **secure-by-design**, resilient to cyber incidents, and quickly patched when vulnerabilities are discovered. This is fundamental to provide the EU's private and public sector with the possibility to choose from the most secure infrastructures and services. ZVC significantly impacts the cybersecurity future and affords the EU an opportunity to lead in the development of secure technologies across the whole supply chain. ZVC ensures resilience and stronger industrial and technology capacities in cybersecurity in order to mobilize all necessary regulatory, investment and policy instruments. ZVC's true **"cybersecurity by design"** framework for industrial processes, operations and devices can mitigate risks, potentially reduce costs to companies as well as to wider society, and thereby increase resilience. Due to its low presence in the consumer electronics industry, Europe is increasingly dependent on external providers in this area. ZVC is an opportunity for Europe to regain presence on the consumer electronics market,

[30] Foundational ZVC experiments were funded under H2020 Fed4Fire+ sub-grant (No. 732638)

2.1.3. ZVC4IoT may also impact future security threats from Quantum Computing

Strong cryptography is vital to overall individual and societal cybersecurity. It provides the foundation for secure transmission and data storage, and for authenticating trusted connections between people and systems. However, cybersecurity researchers and analysts are worried that a new type of computer, based on quantum physics, could break most modern cryptography. In addition, protecting from complex attacks such as malware or brute force attacks cannot only rely on typical encryption mechanisms. While a large amount of research is now focused on post-quantum cryptography (PQC) the vulnerabilities keep growing at a faster pace than ever. As much as cryptography remains vital to traditional cybersecurity, the main components of ZVC (SOS & ICOS) are inherently resilient to QC cryptanalysis attacks, as they are essentially encryption and AI dependent. Nevertheless, Personally Identifiable Information (PII) stored in ICOS can be secured through data's entire life cycle using post advanced post QC (e.g., homomorphic or laconic) encryption or standard encryption schemes.

2.1.4. Short-Long Term Contribution & Tangible Outcomes of ZVC4IoT

While ZVC4IoT achieves all the expected outcomes, it contributes tangible deliverables beyond the goals of the call HORIZON-CL3-2021-CS-01-02 that go beyond state-of-the-art as illustrated in the following table.

Table 2.1.4. ZVC contributions & tangible outcomes:

ZVC contributions	Tangible outcomes
Short Term (Achievable during the project implementation)	
a. **To the state of the art:** In the evolution of computers, attack surface vulnerabilities & in-computer online data risks have always existed as a necessary evil. ZVC's SOS and ICOS will be a path-breaking contribution to SOTA. b. **To Next Generation Internet (NGI)**: The decentralized architecture & Web 3.0 components collectively provide a Cyber Secure vision of NGI c. **To Cybercrime:** A hacking challenge (T5.3) will establish ZVC's unhackability d. **To IoT Industry**: An alternate high-security computing paradigm e. **To Computer industry**: ZVC deployability across all computing domains	- World's first zero-vulnerability computing framework for connected devices. - A secure Web 3.0 design for connected IoT devices - A functional ZVC framework for connected devices (D4.3). - A malware resistant computing framework. - ICOS & SOS powered Edge/IoT devices pave the way for future ZVC devices.
Medium to Long Term vision (Beyond the duration of the project)	
a. To cause a considerable dent in the cybercrime industry b. To computer industry's gradually transitions away from offline installable applications c. To acceleration of decentralization and transition of Web 2.0 to Web 3.0 d. To future of cybersecurity in the Quantum Computing era	·Downfall of Malware industry ·Decline of Legacy App Industry ·Computer with built-in Web 3.0 features -Quantum resistant computers

2.1.5. Key expected results of ZVZ4IoT project & IP Protection

The ZVC4IoT consortium partner BC5 owns the background IP and is responsible for subsequent IP protection measures.

Table 2.1.5: ZVC expected key results and their foreseen protection measures

#	Owner	Key result and IP protection	Target groups (timing)
1	BC5	ZVC architecture and specifications	The scientific community, IoT vendors, computer / Smartphone manufacturers, Netizens among others (WP2; M10)

2	BC5	Child patents on alternate use cases	Cybersecurity stakeholders, Computer, Smartphone and IoT industries (WP1, M20)

2.1.6 Potential post-funding barriers impacting long term ZVC4IoT achievements

ZVC has the potential to become a de facto standard for trusted computer systems across the globe. Potential barriers beyond the scope and duration of this project cannot be accurately foreseen or predicted. Nevertheless, any requirements and potential barriers - arising from factors beyond the scope and duration of the project - that may determine whether the desired outcomes and impacts are achieved.

Table 2.1.6 Potential post-funding barriers Contingencies | P: Probability, I: Impact

	Description of the barrier	P / I	Mitigation measures
B1	Follow on funding will be required for global deployment of ZVC to make it a commercial success.	Low/ High	ZVC will be spined off as a separate venture to make it more attractive to venture capitalists.
B2	Freedom To Operate (FTO) may be restricted by adversarial IP rights.	Low /Medium	The ZVC4IoT consortium already has an IP strategy in place which includes securing full IP protection and FTO analysis before the conclusion of the project.
B3	Jurisdictional regulatory restrictions: In most jurisdictions' cybersecurity may be territorially regulated by local governments. The requirements may substantially vary.	Medium / Low	ZVC4IoT infrastructure components are modular in design, which makes it possible to customize the platform to the local needs of the law enforcement authorities.
B4	The project does not deliver solution matching the goals of the consortium and needs of the stakeholders	Low / High	ZVC4IoT deploys a user-centric design and the use-cases selected are conservative and achievable, rather than as a new competing paradigm of the future.
B5	Budget (time/cost) issues due to complexity and possible changes as the requirements for optimum solutions evolve.	Low / Low	The scope has been discussed, agreed, defined, using outputs from existing projects. Resources are allocated accordingly. An agile development will keep the project on track.

2.2. Measures to maximize impact - Dissemination, exploitation and communication

Exploitation measures to translate research into innovations

The ZVC4IoT consortium has defined an exploitation plan and a set of activities to facilitate future exploitation of project results within and beyond the project lifespan. The exploitation plan will be refined towards the end of the project with the preparation of an exploitation roadmap (WP5; D5.5; M32).

ZVC involves key actors with the potential to lead the translation of new research into successful innovations. These include **(1) early-career computer scientists** that will be employed throughout the project and whose research career will be supported and enhanced by the specific measures identified below; **(2) experienced researchers** in research organizations (**UPRC, UL, UTH, CERTH and EUT**) who will further enhance and consolidate their expertise (see Section 3.1) and integrate project results into their curricula at the BSc, MSc and PhD levels; **(3)** the **SME partner BC5**, who owns several IPs within the Web 3.0 and ambitious to become a front runner in EU's ambition and commitment to become the leader of the Next Generation Internet and device manufacturing; (4) The **industry partner AFL**, which will contribute to AI, IPFS components of ZVC and feed early adopters from its DeFi (decentralized finance) community aspires to earn global leadership within the DeFi space; **(5)** the **SME partner ZAS**, with long-standing experience in acquiring EU funding for R&I projects, thus supporting the uptake of new knowledge generated in ZVC into follow-up projects; **(6)** A multisectoral and interdisciplinary **External Advisory Board** whose members will be appointed at the project kick-off.

To ensure internal exploitation of results and the sustainability of the project, we have also already planned the following three internal exploitation activities (WP5, Task 5.4):

- **Market assessment and stakeholders mapping**: BC5 and ZAS will jointly map relevant stakeholders and assess the market environment including a comprehensive analysis of environmental forces and entry barriers (PESTEL), opportunities and risks (SWOT) as well as market trends and competition.
- **Strategic Grant Planning (SGP)**: ZAS will advise partners on potential funding opportunities relevant to the ZVC technology and its various components through its SGP service. Within this frame, ZAS will guide ZVC researchers and SMEs on how to plan for follow-up projects.
- **Exploitation roadmap (D5.5)**: BC5 will coordinate the preparation of an exploitation plan that will include a plan for commercial and non-commercial use of the project results and a series of exploitation tools such as updated PESTEL and SWOT analyses and stakeholder map.

To further facilitate the exploitation of project results, we will build on end-user/industry involvement and use existing networks and communication channels to implement the following key exploitation supporting activities:

- **Policy brief (D5.4)**: ZVC will positively affect EU security by operationalizing cybersecurity guidelines (such as the upcoming NIS 2.0 and ENISA blueprint on Data Privacy and Certification) to protect company assets' operations, therefore producing effective infrastructure preventive action and emergency plans, minimizing recovery time and maximizing business continuity; ***Target audience:*** EU and national policy bodies, including the European Union Agency for Network and Information Security (ENISA); ***Expected impact:*** Knowledge sharing. Briefing policymakers about possible legal barriers for implementing the ZVC technology; ***KPIs:*** One policy brief (D5.4, M32); ***Assessment:*** Nb. of contact addresses to which it is distributed, Nb. of downloads.
- **Horizon Cybersecurity Cluster Day**: ZAS will organize a Cluster Day that brings together ongoing Horizon 2020 and Horizon Europe projects in the field of cybersecurity to facilitate knowledge exchange and promote new synergies; ***Target audience:*** Computer scientists and industry involved in EU-funded projects; ***Expected impact:*** New partnerships and synergies with other EU consortia; ***KPIs:*** Occurrence of the Cluster Day (T5.4; M24); ***Assessment:*** Nb. of EU projects and members represented.

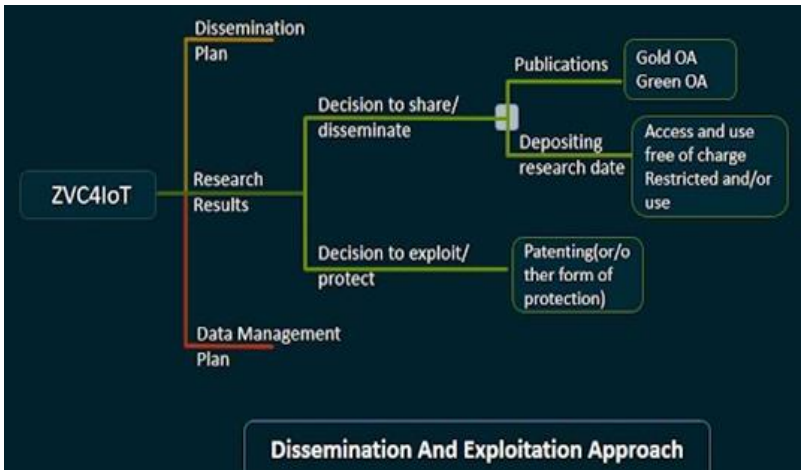
Further measures to support the project results uptake by early-career researchers, SMEs and relevant actors are described in the Communication and Dissemination activities.

2.2.1. Communication and Dissemination

Measures to maximize impact will be delivered within WP5, led by ZAS and closely supported by CERTH, UL and BC5. In terms of communication and dissemination, our goal is to disseminate the research results generated in the technical work packages (WP2-WP4) to the cybersecurity community and raise awareness and provide information on the ZVC technology and its potential impact on society.
As developers of a pathbreaking cybersecurity technology ZVC4IoT, the consortium aims to be the first to publish our findings, because it is through dissemination that the work realizes its value. In line with the Horizon Europe rules and current trends in IP management and publication strategies, the ZVC4IoT consortium is committed to full **open access**. This implies that all partners agree with the principle that all peer-reviewed research publications are made immediately open access. The budget has been allocated accordingly for open access fees. Partners will be required to give prior notice of any planned publication.

Communication and dissemination activities will be using the language, tools and channels most suitable for a specific target group's interest, needs and ability to comprehend the content. The **Communication, Dissemination and Exploitation Strategy** (CDES, D5.2) will provide further structured guidelines for all project partners on stakeholder engagement, communication, dissemination and exploitation activities including defining the appropriate tools, channels and messages to engage with the following target groups: Early career and experienced computer scientists, cybersecurity experts, software developers, computer manufacturers, early adopters, policymakers and netizens.

2.2.1 A) Communication and dissemination activities



During the project, ZVC4IoT partners will be actively involved in a wide range of activities to maximize the uptake and public awareness of the project results. ZV4IoT partners are all already engaged in various communication and public engagement activities. This project will exploit synergies by using them as a platform to make the action known to experts and wider audiences. The following activities will be further elaborated and assessed in the CDES and its update (D5.2).

Table 2.2.1A) Communication / Dissemination and their desired impact

#	Communication & Dissemination activities	Impact / KPI	Assess./Lead	Target groups
1	**Project website and social media** ● The initial source of information to ensure project visibility ● Information on the overall objectives of the project, the network, events, and scientific results.	Dissemination of project results, increase awareness / 300 visitors p/year, a total of 200 external followers	User statistics (Google Analytics) / ZAS	All
2	**PR & communicational material** ●Press releases on various related topics and latest project achievements ●Print/digital materials to be distributed at Events and available on the website	Awareness-raising, visibility and increased interest in the project / 2 press releases, 50-150 downloads on the website	Press monitoring; user statistics / UPRC	All
3	**Scientific articles and presentations** ● Publication of scientific results in peer-reviewed open access journals ● Talks at key international conferences, such as S&P, Euro S&P, ESORICS etc.	Knowledge sharing, validation of results & feedback from peers, increase awareness / 6 publications, 5 talks given, 500 video views	Monitoring of publications and other dissemination activities / CERTH	Computer scientists, cybersecurity experts
4	**GitHub repository** ● ZVC codes & related documentation provided to the developer community via GitHub	Knowledge & project resources sharing / 20 entries, 4,000 user accesses	Nb. of accesses to the repository / BC5	Computer scientists, software developers
5	**ZVC dissemination events and workshops** ● Disseminate results & foster dialogue within workshops (online / physical)	Knowledge sharing, validation of results and feedback from peers / 20 external participants	Nb. of participants and feedback / CERTH	Computer scientists, cybersecurity experts, early adapters, computer manufacturers

6	**E-learning modules** ● Website integrated raining content ●Topics: Cybersecurity, Vulnerabilities, NGI	Knowledge sharing, / 60 individual accesses views	Nb. of views / CERTH	Early-career researchers, BSc/MSc students
7	**Young Women in Computing** ●The event including engaging activities to promote women's role in computer science and attract young female students into this field	Increase visibility and promote female representation in IT / 30 participants	Nb. of participants and feedback / UL	Prospective female IT students
8	**Global hack ZVC challenge** (M34) ● Open challenge to hack the ZVC system	Increase project visibility and interest in ZVC / 50 participants	Nb. of participants and winners / UL	Computer scientists, software developers, netizens
9	**Researchers' Night events** ● Exhibit ZVC technology at local public events such as the European Researchers' Nights ● Encourage young people to study computer science	Increase interest in cybersecurity for students and the general public / 50 visitors physically/virtually	Number of visitors in every booth / UL	School-age students and young people

2.2.2 Intellectual property management strategy

BC5 is responsible for the overall innovation management and intellectual property (IP) monitoring. A Consortium Agreement, which will define the rights and obligations of all members in terms of IP, will be signed prior to project start. The ZVC partners have already agreed on the following common rules: 2.2.1 **Confidentiality**: All information provided by a partner to other partners within the project is confidential unless it was already known to the partner before the negotiations started, or the information provided is public property, or it is explicitly specified otherwise by the originator of the information;

i. **Existing IP (Background):** The respective partners remain the exclusive owners of any data and information held prior to this project, as well as copyrights or other IP rights pertaining to such information (BC5 owns 3 patents covering the ZVC technology as background IP);

ii. **Access rights / Use:** All partners will grant access to their background knowledge to other partners on a royalty-free basis if needed by the requesting partner for performing project tasks. Any disclosure of confidential information to a third party requires the explicit consent of the originator of that information;

iii. **Ownership/IP Protection (Foreground):** The generating partner will solely own IP, while jointly generated IP will be jointly owned and based on a separate Joint Ownership and Management Agreement between the partners concerned.

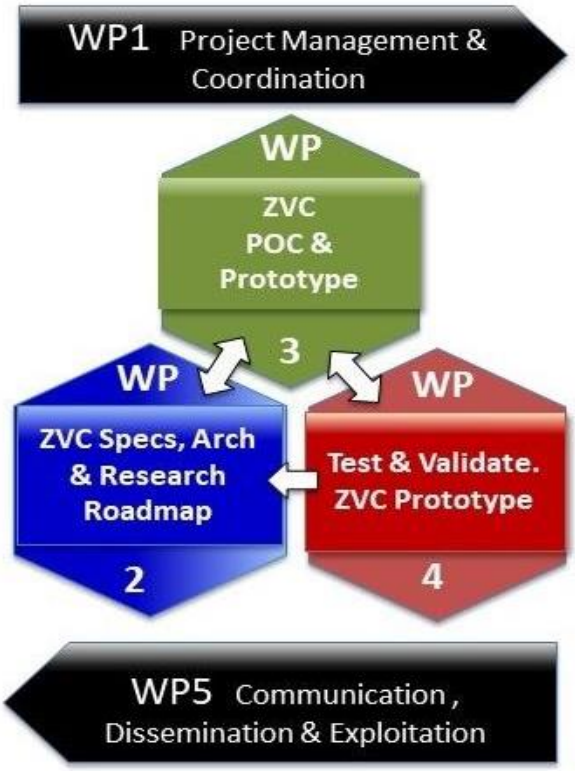
Additionally, the academic project partners will work with their local TTO to explore and ensure the protection of ZVC IP, especially the registration of patents. The process of securing IP has already been initiated with a provisional patent application on the SOS and ICOS components of ZVC, which will be converted to non-provisional seeking worldwide protection within 12 months. IPR review will be held and child patents will be file as in Table 2.1.5. A freedom to operate (FTO) analysis will be conducted by an IP firm and a business plan will ensure that ZVC IP is adequately secured.

3. Quality and efficiency of the implementation

3.1. Work plan and resources

ZVC4IoT is structured in five WPs. In WP1, UPRC will be coordinating all activities of the project, ensuring links and work consistencies according to the plan and the financial follow-up. BC5 is leading WP2, developing the full specifications and architecture of the enabling ZVC technology, while UTH leads the development of a proof-of-concept (POC) and the research on exploring at least three use cases in WP3. The deliverables of WP3 will be tested

and validated in WP4 under the leadership of EUT. In WP5, led by ZAS, the consortium will exploit, communicate and disseminate the results among the research community and the wider public.



PERT CHART

The overall organization of WPs and their relations is illustrated in the PERT Chart.

Work Plan Scheduling of WP Tasks & Milestones (Gantt chart)

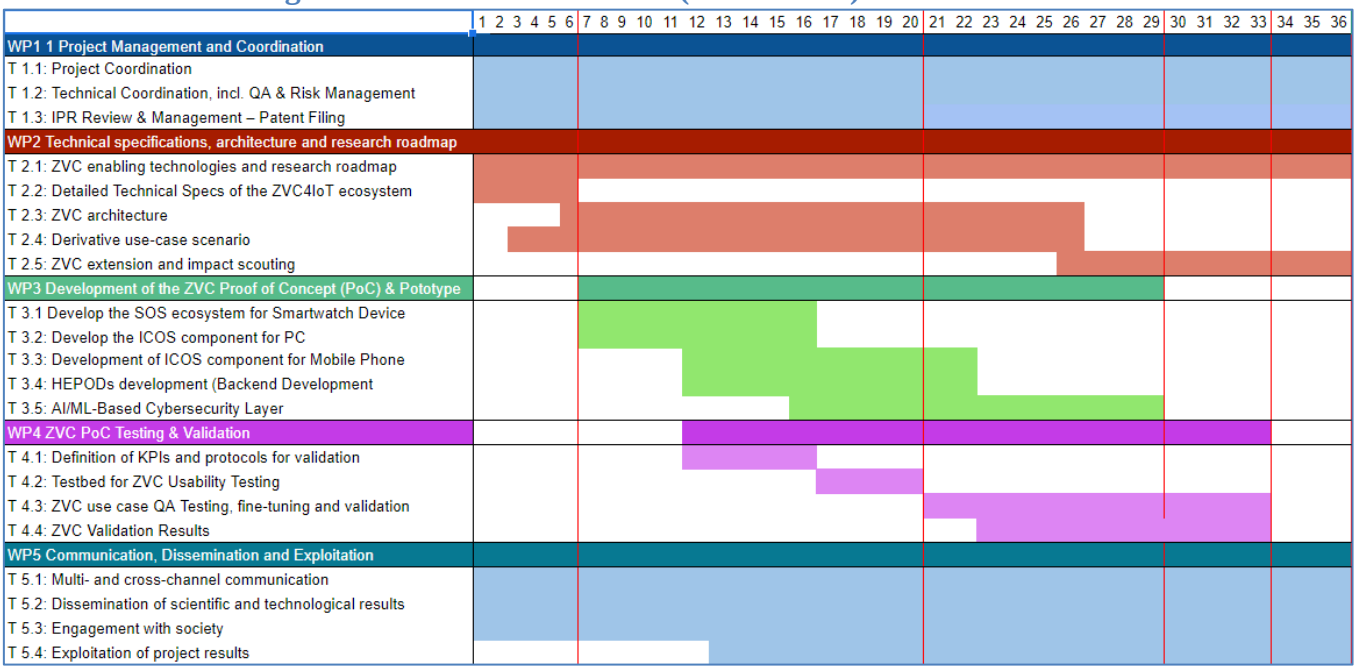


Table 3.1b: List of work packages

WP No.	WP Title	Leader		Person Months	Start Month	End Month
		No.	Name			
1	Project Management / Coordination	1	UPRC	40	1	36
2	Research Roadmap, Tech Specs & Architecture of ZVC components	2	BC5	143	1	36
3	ZVC Proof of Concept (POC) & Prototype with Edge device & End Node IoT device	3	UTH	129	7	29
4	ZVC POC Testing, Validation & IPR Review	7	EUT	103	12	33
5	Communication, Dissemination and Exploitation	10	ZAS	70	1	36
	Total Person Months			**485**		

Table 3.1b: Work package description

Work Package 1

WP No.	**1**		**Lead beneficiary**		UPRC					
WP Title		Project Management / Coordination								
Participant No.	1	2	3	4	5	6	7	8	9	10
Participant	UPRC	BC5	UTH	EUT	CISPA	ZAS	CERTH	AFL	SBA	UL
Person months /participant	17	8	3	3	1	2	1	1	1	3

Start month	1	End month		36

Objectives

WP1 led by UPRC ensures the completion of all deliverables in time, within budget & to the required QA standard. It involves administrative, technical, innovation, quality, ethics and data management.

Description of work

Task 1.1: Project Coordination (lead: UPRC; participants: all) (M1-M36): UPRC will be responsible for the overall project coordination of the Consortium Partners, incl. the management of all administrative, financial, contractual and legal aspects of the project, as well data management, ethical or security issues. ZAS and UL will support the coordinator for these tasks based on its expertise in EU projects, while each partner will be responsible for its relevant tasks at an organization level. UPRC is responsible to ensure the project is managed according to the rules & regulations set by the EC.

Task 1.2: Technical Coordination, incl. QA & Risk Management (lead: UPRC; participants: BC5, UTH, EUT, ZAS) (M1-M36): UPRC will be responsible for the overall technical coordination of the project including monitoring of the technical progress and deliverables of the project. The WP Leaders will support the quality assurance of all the deliverables, in alignment with the research and innovation goals. UPRC ensures proactive measures are taken to mitigate risks against the planned outcomes.

Task 1.3: IPR Review & Management – Patent Filing (lead: BC5; participants: UPRC) (M1-M36): UPRC and BC5 will ensure the review of innovations produced to examine for potential patent management and protection.

Deliverables

D1.1: Project Handbook - Quality Plan (T1.1, UPRC, ZAS, M2)

D1.2: ZVC4IoT Research ethics and Data Management Plan (DMP) V1. (T1.1, UPRC, M6)

D1.3: ZVC4IoT Research Ethics and DMP V2. Final version of the handbook (T1.1, UPRC, M18)

D1.4: IPR- Patent Filings IPR Report with 2-3 Patents filings along with child patents produced after the final validation (T1.3, BC5, M20, updated in M36).

Work Package 2

WP No.	**2**			**Lead beneficiary**			BC5		
WP Title		Research Roadmap, Tech Specs & Architecture of ZVC components							
Participant No.	1	2	3	4	5	6	7	8	9	10
Participant	UPRC	BC5	UTH	EUT	CISPA	ZAS	CERTH	AFL	SBA	UL
Person months /participant	16	26	14	12	12	12	11	14	12	14
Start month	1			End month			36			

Objectives

- Build and deliver the overall technical requirements, specification and architecture of the ICOS and SOS components of the ZVC ecosystem that will be used in the development of ZVC use cases and their integration into a cyber-secure computing ecosystem.
- Define the scenario for the ZVC proof of concept on the 3 use cases mentioned in sec1.6 and explore possible extension to other computing environments.
- Draft the research roadmap with specific research challenges within and beyond the scope of the project

Description of work, lead partner and role of participants

Task 2.1: ZVC4IoT enabling technologies and research roadmap (lead: UPRC, Participants: UTH, CISPA, UL, ZAS, CERTH, SBA) (M1-M36): In this task, led by UPRC, we will perform a deep dive in security and cryptographic related technologies and state-of-the-art research to identify the updated state of the methods, APIs, frameworks, algorithms and assess their relevance to ZVC. We will then prioritize their adoption in ZVC based on functionality and maturity criteria. This will provide developers with the technological solutions that will facilitate the development of ZVC and streamline the gaps in research where the academic partners will devote their resources. Targeted research on key aspects of ZVC will be performed to fill in the gaps of the literature including but not limited to the design of new algorithms, development of new cryptographic primitives and protocols, where deemed necessary, automation of vulnerability identification, and ML/AI application in cybersecurity. Since the ZVC architecture involves many actors with different levels of computing power while targeting system-wide security, CISPA and UPRC will research for cryptographic techniques that are lightweight, yet secure enough for the low-end devices, such as reverse delegation, (fully) homomorphic encryption and communication optimal protocols. Other participants (UL, CERTH, AFL) will be involved in the analysis of architectural and algorithmic requirements of ZVC, regarding ML/DL enabling technologies, enriched by AI tools and focused on cybersecurity issues.

Task 2.2: Detailed Technical Specs of the ZVC4IoT ecosystem (lead: BC5, Participants: ZAS, UPRC, UTH, SBA, EUT) (M1-M6): BC5 will draw up detailed textual specifications of the overall architecture, consisting of the ICOS and SOS components, their responsibilities, platform-internal interfaces, and specify the precise role of the foundational components of the ZVC platform, their interaction with each other, and their potential use-dependent variations. All technical partners will provide their respective input.

Task 2.3: ZVC4IoT architecture (lead: BC5, Participants: UTH, UL, UPRC,) (M6-M26): In this task, we will produce the detailed general architectural design of the ZVC ecosystem in two rounds (initial and final architecture). While BC5 leads this task, the other participants will provide their input to optimize ZVC usability. UL will contribute to this task via the definition of the ZVC architecture, along with detailed analysis of scalability requirements (and possible limitations) of the architecture.

Task 2.4: Derivative use case scenario (lead: ZAS, Participants: UTH, EUT, UL, UPRC) (M3-M6): We will detail the three derivative use case scenarios of ZVC in terms of expected inputs and outcomes, design criteria, usage scenarios and means of verification. UL will cooperate to this task with the UTH, EUT and UPRC, by highlighting the relationships among the various actors (e.g., procedures, devices, users, etc.) of the derived use case scenarios.

Task 2.5: ZVC4IoT extension and impact scouting (lead: CERTH, Participants: All) (M26-M36): CERTH will evaluate the possible impact of the ZVC design on different aspects like usability. commercial, legal, ethical, social perspectives, and will also consider how the architecture could be extended to other kinds of computing environments other than the 3 designed use cases. In this respect, UL will investigate how the architecture can be exploited to deal with other middleware components by adapting its DL/ML modules to innovative requirements.

Deliverables

D2.1: ZVC4IoT research roadmap (UPRC, M12, M24, M36**);** Periodic reports of research challenges and results.

D2.2: ZVC4IoT enabling technologies and technical specs (BC5, M6); Report of enabling technologies and technical specifications for ZVC architecture

D2.3: Initial Architecture of SOS and ICOS components, use case Framework and Testbed (BC5, M8)

D2.4: Final ZVC4IoT Generic Architecture, Use Case Framework and Testbed (BC5, M26);

D2.5: ZVC4IoT continuous research and innovations report which presents the key innovations; both research and technological, introduced in ZVC (ZAS, M36)

Work Package 3

WP No.	**3**			**Lead beneficiary**			UTH			
WP Title	ZVC4IoT Proof of Concept Prototype with Edge device & End Node IoT device									
Participant No.	1	2	3	4	5	6	7	8	9	10
Participant	UPRC	BC5	UTH	EUT	CISPA	ZAS	CERTH	AFL	SBA	UL
Person months /participant	12	18	20	13	16	4	18	13	8	7
Start month	7			End month			29			

Objectives

WP3 aims to realize the Proof of Concept (POC) of the envisioned system and conclude a functional framework that meets the requirements and specifications set by WP2. WP3 aims to build the ZVC framework prototype as POC, consisting of Edge devices (PCs) with full ZVC implementation (ICOS component), and End Nodes, i.e., IoT device (Smartwatch) with SOS deployment. The following list depicts the objectives of the WP in detail: To develop the SOS ecosystem ready to be incorporated into the IoT devices; To implement the ICOS module ready to be incorporated into the edge nodes; To implement an ICOS version to be incorporated into smartphones as an alternative to PCs; To develop the required backend system for the management of interactions between the envisioned components; To implement the required AI functionalities that will enhance the cybersecurity aspects of the proposed framework.

Description of work

Task 3.1: Develop the SOS ecosystem for Smartwatch Device (Lead UTH, Participants: CISPA, UPRC, EUT, CERTH, BC5, AFL): In this task, the involved partners will implement the SOS infrastructure based on the requirements and the design performed in WP2. Specific interfaces will be adopted to connect the proposed infrastructure with the operating system and other components present on IoT devices. The required functionalities in the SOS components will become reality. The outcome will be a ready to use system that will be installed in the desired devices being adopted into our pilots. We have to notice that we will also implement the necessary interfaces for connecting the ecosystem with the edge infrastructure. UTH will monitor the overall development and integration of the SOS module over the smartwatch firmware. The development of the SOS program will be supported by BC5 in particular whereas the other partners will deliver their expertise in specific modules development.

Task 3.2: Develop the ICOS components for PC (Lead CISPA, Participants: UTH, UPRC, EUT, CERTH, BC5): This task refers to the development of ICOS hardware and its complimentary software and its incorporation in the edge nodes. Specially designed switchable NAND flash memory chipset will be fabricated to seamlessly integrate into the

USB port of PC as an edge device supporting the novel ZVC4IoT framework. The ICOS device will be designed to be easily controlled by users to keep their PII data offline right within their PC itself while they use the PC for their normal online activities. Its tiny form factor virtually merges with the contours of the host PC permanently. The ICOS hardware will be further secured with advanced security mechanisms specially during the sporadic data access for data processing. The task will realize the functioning of the ICOS component being connected with the hardware/software present at the edge nodes. CISPA will be entrusted with the task to develop the ICOS cryptography component for the edge node and ensure its integration with the remaining modules, considering the specific use case scenarios mentioned in the field trial sections. UTH & UPRC will analyze and ensure the ICOS coherence with the field trials whereas BC5 and CERTH will assist CISPA in testing the specific components.

Task 3.3: Development of ICOS component for Mobile Phone as an alternate ICOS prototype (Lead UTH, Participants: CISPA, UPRC, EUT, CERTH, AFL): The task focuses on the provision of an ICOS alternative that can run in a smartphone (mobile phone). The task will involve the deeper research into design and implementation aspects of the ICOS components for mobile phones which imposes different requirements compared to the implementation of the ICOS for PCs. In this task, the participating partners will analyze and develop the required modules in order to have a running version of the ICOS. Mobile phones' characteristics will be studied and a set of parameters will be defined to depict the running environment of the ICOS hardware and its complimentary software along with its incorporation in the mobile phone as an edge node. Specially designed switchable NAND flash memory chipset will be fabricated to seamlessly integrated into the MicroSD slot that most mobile phones are endowed with. Thus, mobile phone can be redesigned as an ICOS-powered edge device supporting the novel ZVC4IoT framework. The ICOS device will be designed to be easily controlled by users to keep their PII data offline right within their mobile devise itself while they use the mobile phone for their normal online activities. Its tiny form factor virtually merges with the contours of the host mobile phone permanently. The ICOS hardware will be further secured with advanced security mechanisms specially during the sporadic data access for data processing. The task will realize the functioning of the ICOS component being connected with the hardware/software present at the edge nodes. Then, the implementation activities will realize the discussed components being fully integrated with the hardware and software of mobile phones. The task will be led by UTH whereas, EUT, AFL and CISPA will perform the ICOS system testing in different mobile phone settings to expose the applicability of the approach.

Task 3.4: HEPODs development (Backend Development): (Lead: BC5, Participants: UTH, CISPA, ZAS, EUT, CERTH, AFL, UL) (M16-M29): In this task, the ZVC backend architecture will be developed based on a decentralized open-source SOLID PODs technology (See Sec 1.1.7A and footnote 23) for data management. It is critical to develop all the necessary software modules to meet the requirements and the design principles defined by WP2. The back-end infrastructure will act as the core point where data will be managed and exposed to any interested component. The task is coordinated by BC5 and supported by CISPA incorporating new results derived from T2.1. BC5 will manage the development of the PODs module for securely decentralizing the data collected while CISPA will participate in the task offering functionalities related to the homomorphic encryption of the acquired data. The backend will be extended by UTH, CERTH, UL and AFL implementing a set of ML/DL modules that will be applied upon the available data. The target of the ML/DL modules is to support an automated extraction and execution of self-governing legal, social & ethical rules for privacy / anonymity. This way, the project will provide an 'intelligent cover' around the involved PODs and enhance the autonomous functioning of the proposed platform. It is a kind of an intelligent API that will control the access on the available data. The participating partners will study and apply the most appropriate ML/DL models in order to meet the requirements of our use cases.

Task 3.5: AI/ML-Based Cybersecurity Layer (Lead: CERTH, Participants: AFL, UL, SBA.)**:** Although not mandatory requirement for ZVC, an additional level of intelligence is related to the Cyber-security aspects of the framework. This task aims to enhance the security of the ZVC framework by developing a ML-based IDS that protects (i) the ICOS device from being tampered with, either physically, by opening the device or remotely, using specialized hardware, and (ii) the device that the SOS is installed on, by extracting behavioral characteristics of regular/baseline usage and identifying anomalies that indicate alien users are accessing the device. For the first, ML-based techniques, including clustering and multidimensional machine learning, will be used to identify regular operation power consumption parameters and a model to detect outliers that indicate tampering. Concerning the user profiling,

behavioral characteristics will be extracted, based on the keystrokes, mouse movement, to create a profile of the way they use the device. Based on those, users will be profiled in ad-hoc classes, and ML-based models will be developed to detect anomalies and outliers, indicating that malicious users have access to the device and apply locks.

Deliverables

D3.1: ZVC4IoT POC (PC and Smartwatch devices) (UTH, M16)

D3.2 Mobile phone as alternate ICOS prototype (UTH, M22)

D3.3 HEPODs backend infrastructure and additional AI/ML-based Cybersecurity (BC5, M22)

D3.3 Audit ZVC Devices (CERTH, M24)

D3.4 Repository deposit (BC5, M29)

Work Package 4

WP No.	**4**			**Lead beneficiary**			EUT			
WP Title		ZVC4IoT POC Testing, Validation & IPR Review								
Participant No.	1	2	3	4	5	6	7	8	9	10
Participant	UPRC	BC5	UTH	EUT	CISPA	ZAS	CERTH	AFL	SBA	UL
Person months /participant	9	8	10	22	10	8	10	8	8	10
Start month	12			End month			33			

Objectives

To test & validate ZVC4IoT framework in a controlled Edge (Laptop PC) - IoT (smartwatch) computing environment in BYOD (Bring Your Own Device) setting. Explore Mobile phones as alternate Edge Node / IoT devices.

Description of work

Task 4.1: Definition of KPIs and protocols for validation (lead: EUT, Participants: UTH, ZAS, UPRC, CERTH, CISPA, UL, AFL) (M12-M16): A detailed definition of KPIs and protocols for usability and technical validation of ZVC4IoT and the use case will guide the work of this whole validation WP. KPIs will be selected to be measurable and quantifiable and protocols will describe the involvement of users and the validation process. EUT will lead the selection, definition and description and will ensure with UTH, UPRC, CERTH, UL and AFL the compliance with KPIs and protocols. UL has an extensive experience in multidimensional analytics, and will contribute in the definition of aggregate-based KPIs in the context of user-classes/privacy-threats matching and analysis.

Task 4.2: Testbed, ZVC4IoT Usability Testing: (lead: CISPA, Participants: UTH, EUT, UL, CERTH, AFL) (M17-M20): The delivered testbed is expected to be used to test the usability of ZVC4IoT and the derivative use case. To carry out this task, UTH will lead the recruitment and involvement of users following the established protocol to measure the defined KPIs. The result of the usability test will iteratively feedback the development of WPs 2 and 3 and will be reported with the support of especially EUT and the rest of partners.

Task 4.3: Derivative use case QA Testing, fine-tuning and validation (lead: CERTH, Participants: UTH, EUT, UPRC, UL, AFL, SBA) (M21-M33): In this task, we will test and validate each component of the ZVC POC (ICOS &

SOS) & derivative IoT use case prototype (PC-Mobile, PC-IoT, Mobile-IoT BYOD setting) following rules published by ISO and EU data protection directives, KPIs and protocols. CERTH will lead QA testing and EUT will complement the iterative fine tuning and validation process to feed back the whole implementation to WPs 3 and 4, with support of UPRC, BC5, AFL and SBA. This technical testing will comprise functional, security (pen-testing), performance and integration testing and will be measured and quantified through the pre-defined KPIs.

Task 4.4: ZVC4IoT Validation Results (lead: EUT, Participants: UTH, ZAS, UPRC, CERTH, CISPA, UL) (M23-M33): GitHub repository will be shared and used for the whole validation process. Usability and technical tests will produce results which besides providing necessary feedback to the research and development WP will be reported according to the pre-defined KPIs and protocols. IPR review will be undertaken for securing appropriate IP protection in collaboration with T1.3

Deliverables

D4.1 ZVC4IoT validation KPIs and protocols for both SOS and ICOS components (EUT, M16)

D4.2 ZVC4IoT Testbed for usability testing (UTH, M20)**;**

D4.3 ZVC4IoT & derivative use case initial Testing Interim Report (CERTH, M23)**;**

D4.4 ZVC4IoT & derivative use case Final Validation Report (EUT, M33).

D4.5 ZVC4IoT patent filing (2 or more) (BC5, M20)

Work Package 5

WP No.	**5**			**Lead beneficiary**			ZAS			
WP Title		Communication, Dissemination and Exploitation								
Participant No.	1	2	3	4	5	6	7	8	9	10
Participant	UPRC	BC5	UTH	EUT	CISPA	ZAS	CERTH	AFL	SBA	UL
Person months /participant	6	10	4	6	4	14	10	5	4	7
Start month	1			End month			36			

Objectives

- Develop a strategy for the dissemination of project results and implement target group specific measures.
- Facilitate the use of project results and pave the way for their future commercial exploitation.
- Raise awareness for ZVC research and its possible implications on cybersecurity, industry and society by communicating project related information to different target groups and via different channels (digital/print/personal).

Description of work

Task 5.1: Multi- and cross-channel communication (lead: ZAS; participants: All) (M1-M36): ZAS and CERTH will set up a multi-channel **communication, dissemination and exploitation strategy** with input from all partners (D5.2). ZAS will set up and maintain the **project website and digital channels** (D5.1). **Press releases** will be issued regularly to reach and inform specialized and/or generalist media on activities and results achieved in ZVC, in collaboration with partners' PR departments. ZAS will also prepare print material and visual content such as videos and infographics.

Task 5.2: Dissemination of scientific and technological results (lead: CERTH; participants: BC5, CERTH, UPRC, UL, EUT, SBA...) (M1-M36): All research partners will disseminate project results, key findings and technology updates through **open access publications** and at national and international scientific **conferences** and events coordinated by CERTH. BC5 will provide all codes and related documentation in the **GitHub repository** to maximize the spread of the software platform world-wide. All research partners will organize a series of **dissemination events and workshops** targeting the cybersecurity R&D community, incl. industry-oriented events. CERTH together with UL, with input from all research partners, will develop **e-learning** material to train computer scientists and/or end users on how to configure, use and secure the ZVC platform using a blended module approach (D5.3).

Task 5.3: Engagement with society (lead: UL; participants: All) (M1-M36): UL and SBA will coordinate the organization of the **Open Hack Challenge** and the **Young Women in Computing** events (see Section 2.2.1). ZVC partners will participate in different science vulgarization events such as the **Researchers' Nights** as well as similar outreach events such as the ones organized within the European Cybersecurity month. UPRC will coordinate the preparation of a **policy brief**, incl. recommendations on cybersecurity policy guidelines.

Task 5.4: Exploitation of project results (see Section 2.1.3) (lead: BC5; participants: All) (M13-M36): BC5 and ZAS will jointly **assess the market environment** including a comprehensive analysis of environmental forces, and entry barriers (PESTEL), opportunities and risks (SWOT) as well as market trends and competition. ZAS will implement its successful **strategic grant planning** to identify future funding opportunities for the ZVC technology and its components. ZAS will organize a **Horizon Cybersecurity Cluster Event** that brings together running Horizon 2020 and Horizon Europe projects in the field of cybersecurity, to facilitate knowledge exchange and promote new synergies. BC5 and ZAS will develop an **exploitation plan** for efficiently and effectively bringing the ZVC computer environment closer to the market (D5.5).

Deliverables

D5.1: ZVC4IoT website (T5.1, ZAS, M2);

D5.2: Communication, Dissemination and Exploitation Strategy (Task 5.1-.3, ZAS, M6, update and assessment in M18);

D5.3: eLearning materials developed specifically for computer scientists (T5.2, CERTH, M36);

D5.4: Policy Brief (T5.3, UPRC, M32);

D5.5: ZVC4IoT exploitation plan (T5.4, BC5, M32)

List of deliverables (table 3.1c)

	Deliverable Name	WP	Lead	Type	Dissemination Level	Delivery Month
D1.1	Project Handbook - Quality Plan	1	UPRC	R	PU	M2
D1.2	Research Ethics & DMP Handbook Ver.1	1	UPRC	R	PU	M6
D1.3	Final Research Ethics & DMP Handbook	1	UPRC	R	PU	M18
D1.4	IPR- Patent Filing (2 or more)	1	BC5	DEC	PU	M20
D2.1	ZVC4IoT research roadmap	2	UPRC	R, Other	PU	M12, M24,M36
D2.2	ZVC4IoT enabling technologies and technical specs	2	BC5	R, Other	PU	M6

D2.3	Initial Architecture of SOS and ICOS components of ZVC4IoT, use case Framework and Testbed	2	BC5	R, Other	CO	M8
D2.4	Final ZVC4IoT Generic Architecture, Use Case Framework and Testbed	2	BC5	R, Other	CO	M26
D2.5	ZVC4IoT contin. research and innovations report	2	ZAS	R, Other	CO	M36
D3.1	ZVC4IoT Proof-of-Concept (PC and Smartwatch devices)	3	UTH	DEM	CO	M16
D3.2	Mobile phone as alternate ICOS prototype	3	UTH	DEM	CO	M22
D3.3	HEPODs backend infra & additional AI/ML based security	3	BC5	R, Other	CO	M22
D 3.4	Audit ZVC4IoT Devices	3	CERTH	R, Other	CO	M24
D 3.5	Repository deposit		BC5	R, Other	CO	M29
D4.1	ZVC4IoT validation KPIs and protocols	4	EUT	R	CO	M16
D4.2	Testbed for usability testing	4	UTH	R	CO	M20
D4.3	ZVC4IoT & use case QA testing Interim Report	4	EUT	R	CO	M23
D4.4	ZVC4IoT & use case Final Validation Report and IPR Review	4	EUT	R	CO	M33
D4.5	ZVC4IoT patent filing	4	BC5	R	CO	M20
D5.1	ZVC4IoT website	5	ZAS	Other	PU	M2
D5.2	Communication, Dissemination and Exploitation Strategy (CDES)	5	ZAS	R	PU	M6,M18
D5.3	eLearning materials	5	CERTH	R	PU	M36
D5.4	Policy Brief	5	UPRC	Other	PU	M32
D5.5	ZVC4IoT exploitation plan	5	BC5	R	CO	M32

List of milestones (table 3.1d)

MS#	Milestone Name	WPs	Lead	Means of verification	Month
MS1	Effective project start	All	UPRC	Establishment of communication and collaboration channels, web presence, clarification and reposition of ZVC4IoT based on market needs.	M4
MS2	Establishment of ZVC4IoT architecture and initial research challenges	2	BC5	Reassessment of research challenges according to state of the art. Delivery of the blueprint of ZVC4IoT along with the clarification of all technical details of components, modules and establishment of interoperability protocols.	M8

MS3	First Periodic Report submitted to the EU	1	UPRC	Report accepted by the EU.	M14
MS4	Alpha release	2,3,4	UTH	Deployment of the first release candidate of ZVC4IoT.	M23
MS5	Beta release	2,3,4	EUT	The ZVC4IoT prototype will be successfully released after thorough testing and validation.	M33
MS6	Communication and Dissemination tasks executed as planned	5	ZAS	Timely submission of D5.1. D5.2. D5.4 and D5.5.	M32

3.2. Capacity of participants and consortium as a whole

The ZVC4IoT consortium bridges different domains of advanced product development with a well-balanced mix of experience and skills in diverse disciplines such as software design, cybersecurity, post-quantum/homomorphic cryptography, AI/ML, data science, network engineering, business innovation, and communication.

3.2.1 Overall Multidisciplinary Capacity: Of the ten partners, two universities (UPRC & UL) and three research organizations (CISPA, EUT, CERTH) and one SME (ZAS) have a strong background in cybersecurity as participants of CCN projects with well-funded cybersecurity research infrastructure that has been utilized in EU flagship European Cybersecurity Centres of Excellence pilot projects, among several other funded projects in cybersecurity. Two other universities (UTH & CERTH) support Eurecat's (EUT) computer hardware design and development capabilities offering their long expertise in ML, AI, data management and cybersecurity. CISPA will mainly contribute through its expertise in advanced cryptographic functionalities. BC5 founder has over three decades of ICT product development experience, and AFL (successfully collaborated with BC5 in ZVC project with AI / crypto contribution) brings its success in designing AI agents for DeFI applications, along with a community of early adopters for ZVC dissemination and exploitation, which ZAS can maximally exploit with its excellent track record in past Horizon projects. The consortium includes one partner from non-EU associated countries, namely AFL (UK). AFL will bring its core expertise in designing and implementing the AI/ML modules in WP2 and WP3 and in performing Quality Assurance (QA), based on its QA and testing experiences for Autonio Trading Terminal and Autonio Decentralized exchange. ZAS will bring its expertise and experience in dissemination activities addressed to both specialist and non-specialist audiences (WP5), notably via the organization of Cluster Events for EU projects based on previous successful experiences in the fields of digital health manufacturing, and renewable energy.

3.2.2 All Four CCN Projects Represented in ZVC4IoT Consortium: Six of the ten ZVC4IoT consortium partners represent all of the four projects funded under the EU's CCN initiative that this call explicitly mandates.[31] UPRC has a long experience in R&D research in cybersecurity, like threat modelling, malware analysis, IoT security, applied cryptography, and ML techniques in security, gained from its participation and coordination of various R&D projects. UPRC is also a participant of **CyberSec4Europe** (Cyber security competence centres for Europe), one of the 4 Cybersecurity Competence Network (CCN) projects funded to develop and implement a common Cybersecurity Research & Innovation Roadmap. UPRC's participation aligns ZVC4ToT with the CCN objectives. BC5 key participants have spent the previous two decades on cybersecurity approaches that circumvent OS vulnerabilities resulting in several patents[32] and eventually conceiving the ZVC concept. UTH will bring its expertise in IoT, distributed intelligence, AI modelling, edge computing and pervasive computing to the ZVC infrastructure. CERTH delivers support in the research areas AI, ML and network engineering and assists in disseminating project results. UL has expertise in cybersecurity, advanced cryptology, AI and data science, and ML, besides being a CCN expert participant in project **CONCORDIA**. EUT is also a CCN expert as project **SPARTA** participant with extensive IoT and edge computing experience via its core technologies and products in Medical Devices and Digital Health solutions based on IoT, data science and AI. CERTH holds strong experience

[31] This call explicitly scopes building on projects funded under SU-ICT-03-2018 (Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap).
[32] **https://www.bc5.eu/DrFazal-Patents/**

in AI and IoT middleware as well as cybersecurity as well as pilot applications with a focus in digital health and medical devices. CERTH is also a CCN expert as project **ECHO** participant along with ZAS.

3.3.1. Management Structure

Overview

The decision-making structure is consistent with the size & complexity of the project, and based on sharing of responsibilities. The decision-making body is the Steering Committee (STC), with a majority vote mechanism, composed by 1 representative for each party, at management level. The STC will approve/decide on strategic matters, on time (schedule), cost and financial aspects, and will approve the reports to the EC. The Project Coordinator (PC) will report to the STC and act as advisor to its chair (appointed among members, at the first STC meeting), and will prepare the meetings and agendas.

The PC will be responsible for the overall organization, planning, and control of the project, deliverables, the reporting and the exploitation & dissemination of results. The Project Management Team (PMT: WP leaders + PC) will be in charge of the daily management of the project and of technical problem solving, meeting not less than once per month. Web meetings will be used as much as possible to minimize travel costs. Decisions will be taken by consensus, and if not possible, by majority of votes. The consortium will make considerable efforts to ensure gender balance and to support and promote young scientists and women through a range of activities such as "**Young Women in Computing**" organized under WP5 (D5.3). One female member of the consortium will lead these programs.

The management of the project has the following goals: (*i*) To ensure that the project is conducted in accordance with EC rules; (*ii*) To reach the objectives of the project within the agreed budget and time scales; (*iii*) To coordinate the work of, and ensure effective communication between the partners; (*iv*) To maximize the potential for exploiting results & active involvement of industry via an External Advisory Board; (*v*) To set the quality policy, including quality objectives for the project as well as for Deliverables; (*vi*) To manage properly Foreground and IPR matters; (*vii*) To ensure that decisions are made on the basis of data and factual information; (*viii*) To solve any problem or conflicting situation; (*ix*) To set the quality policy, including quality objectives for the project; (*x*) To ensure that an infrastructure is set up in order to support the above.

The mandatory internal Consortium Agreement (CA) will be finalized and signed prior to project start. It will describe, among others, the composition, decision-making procedures and responsibilities of the Project Coordinator, General Assembly, and Management Committee; it will also provide clear guidelines to govern the IPR questions and Knowledge Management amongst the consortium.

At the project outset, we will issue 2 documents, which will establish the rules of project management:
Project Handbook - Quality Assurance Plan [D1.1]
The document provides useful information for project partners including procedures and instructions for reporting and using the project management tools. Annual quality reports are included in the periodic project progress reports. It will set the day-to-day rules of the project: documents and deliverables handling, project planning and manpower, meeting organization, internal reporting and information management, external information management, list of personnel with corresponding responsibilities. Finally, it will detail beyond the terms of the EC grant agreement and the Consortium Agreement, the internal project rules and guidelines concerning the daily management of foreground IP and IPR.
ZVC Data Management Plan (DMP) Handbook V1 & V2 [D1.2 & 1.3]
A DMP for ZVC4IoT project activities will be initially produced at M6 and updated at M18 and M24. Both documents will be updated throughout the project life. All the deliverables, the work and resources effort for the internal project management is covered and described in WP1.

3.3.2. Project Structure and Governance Scheme

The Project Management structure shown in the following figure has been agreed among the partners. It has been adapted to the project size, and already implemented with success in past similar projects.

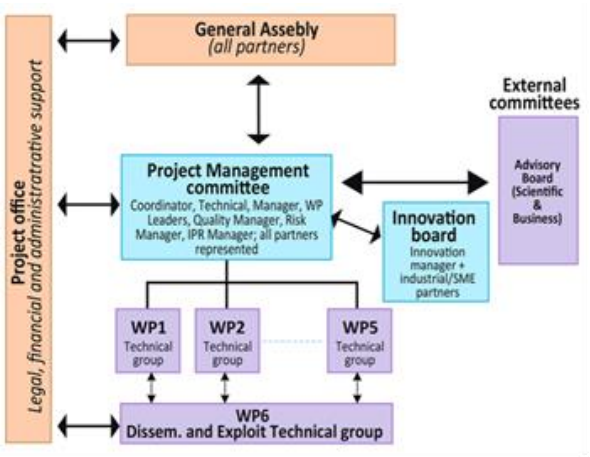


Figure18: project Structure & Governance Scheme

The operational groups are the following:

- *General Assembly:* chaired by the coordinator, approves the project budget and the general annual objectives.
- *Project Management Committee:* chaired by the Technical Manager is the project's executive body.
- *Advisory Board:* chaired by the Project Business Development Manager is the informal strategic body.
- *WP technical groups:* chaired by the WP Leader, they ensure the day-to-day WP technical work.
- *The Project office* supports the several operational groups in all non-technical tasks.

3.3.3. Main Management Roles

1. Project Coordinator

The project coordinator is UPRC, who will act as the focal point for contacts and coordination with the EC, and with other relevant EU and national projects, and for external relationships with relevant bodies and other related activities. The major tasks are: (*i*) Supervision of the overall project progress; (*ii*) Consortium Agreement coordination, organization of the General Assembly, Preparation of minutes, and follow-up of its decisions; (*iii*)· Preparation with the support of the Project Management Committee of the reports, cost statements and project documents required by the EC; (*iv*) Organization of EC review meetings; (*v*) Coordination of IPR and knowledge management. (*vi*) Representative of the consortium to events. (*vii*) Coordination of the dissemination and communication activities.

2. Project Technical Manager

The Project Technical Manager coordinates the activities of all partners in the project according to the technical work plan. The Project Technical Manager is Dr Panayiotis Kotzanikolaou (UPRC). Technical manager will have the following responsibilities (*i*) Chair of the PMC; (*ii*) Liaisons between the PMC and the GA; (*iii*) Supervision of the overall technical progress of the project; (*iv*) Consolidation of the technical reports and coordination of all technical WPs; (*v*) Transmission of any documents and information connected with the project between the partners.

Table 3.3.2 Work package leader assignments

WP	Partner	WP Leader
WP1	UPRC	Panayiotis Kotzanikolaou, PhD (M)
WP2	BC5	Fazal Raheman MD (M)
WP3	UTH	Konstantinos Kolomvatsos, PhD (M)
WP4	EUT	Felip Miralles (M)
WP5	ZAS	Paola Fratantoni (F)

3. Quality Manager [QM]

To keep ZVC4IoT focused on its objectives of high-quality technical outputs, market proximity and openness, the Project Steering Committee will appoint Felip Miralles of EUT as the Quality Manager. In the line of the Project Quality Assurance Manual (D1.1), the Quality Manager will be asked periodically to review technical progress such that the project remains innovative, open to collaborations and to market needs, forward looking. That will ensure that ZVC4IoT is producing work of high technical quality.

4. Innovation Manager and Innovation Board

Rudolf Meyer of SBA will be appointed Innovation Manager. Industry players of main market segments that are driving innovation in ZVC4IoT will form the Innovation Board and will review innovation aspects in the technical

research and propose enhancements whenever necessary. The board includes marketing and strategic people from the industrial organizations involved in ZVC4IoT and will be responsible for analysis of market factors, early product concepts, threats and opportunities of commercialization, etc. Due to that fact, that innovation aspect highly depends on proper IPR, Innovation Board will also support IPR management. The Innovation Board will be chaired by the Innovation Manager assigned by the consortium.

5. Risks Manager

Having in mind that risk may have an impact on the project schedule and project objectives and finally may lead to contractual issues, a Risks Manager will be appointed by the Project Steering Committee at the project start. He/She will be asked periodically to review the project progress and the risks items table to ensure that ZVC4IoT remains online with its main technical objectives. He/She will be in charge of keeping up-to-date the Risk Management Table that will be produced by the WP1. He/She will interact with the PMC and WPs in this task.

6. Data Protection Officer

ZVC4IoT consortium will appoint a Data Protection Officer (DPO) to ensure that the processes, personal data of staff, customers, providers or any other individuals (data subjects) is in compliance with the applicable data protection rules. The appointment of the DPO will be done in accordance with the applicable Data Protection Regulation[33] (Regulation (EU) 2018/1725). Consortium will pay particular attention to his/her expert knowledge of data protection while assigning this role.

3.3.4. Addressing effective innovation management

In order to keep the innovation potential and capacity at a maximum level, the project shall establish a simple, yet effective procedure for the analysis of developments in each of the envisioned architecture systems, subsystems and components.

Thus, the Consortium has decided to establish the procedure of periodical reviews of all critical blocks foreseen by the architecture envisioned by the ZVC4IoT project. This analysis shall combine technical and marketing points of view and will answer the following questions:

- are the targeted KPIs still relevant?
- does the architecture concept (still) have the potential to ensure the envisioned KPIs?
- do sub-systems and components (still) have the potential to ensure the envisioned KPIs?
- have competitive alternatives (architectural, sub-systems, components) been identified?
- do market factors promote the commercialization of the developed sub-systems or components?
- do regulations/standards promote/threaten further development?

Such assessment of viability will be performed for at least the following most critical systems, sub-systems and components of the ZVC framework, viz ICOS and SOS. With this knowledge, the Consortium will be able to make informed decisions that address both technical and business challenges and reduce innovation risks of the project. The assessment will be done every 6 months and be reported by the minutes of the Innovation Board meetings. The described assessment will be made in the specially introduced Innovation Board, chaired by the Innovation Manager. The project involves the collective use of resources and infrastructure proposed by the consortium partners. The IoT expertise of EUT will be utilized during the field trials of ZVC4IoT consisting of Smartwatch and end node PC/Mobile setting. Apart from this, UPRC SecLab will successfully support and implement ZVC research in its infrastructure. UTH will utilize its academic infrastructure in creating a testbed for testing core ZVC devices.

3.4 Critical Risks for Project Implementation

Although risks are quite diverse and, in some occasions, unpredictable, a common process for tackling them does exist, which starts with the identification and classification of the risk, continuous with the resolution approach and implementation, and is completed with monitoring and evaluating its effectiveness. In general, risks can be broadly classified into two categories, one related to the smooth execution of the project work-plan by the collaborating partners and a second regarding specific technical/research obstacles/limitations appearing during the project. For the former category specific project management actions will cope with those issues, while for the latter category

33 https://edps.europa.eu/sites/edp/files/publication/reg_45-2001_en.pdf

technical resolutions will be provided. Table 3.2 below presents the major risks and respective management/contingency plans

Critical Risks for Implementation: The risks identified & scored for the project will be assessed by PMT, reviewed by STC, and monitored at set milestones. In case a threat is realized, mitigation actions already identified will be proposed under PMT responsibility and implemented to minimize impact, as such the good performance of the whole project will not be affected, if absolute trial targets are not fully reached.

Table 3.4 Critical Implementation Risks & Contingencies | P: Probability, I: Impact

#	Description of risk	WP	P / I	Proposed risk-mitigation measures
R1	Device manufacturers/vendors will see ZVC as competition causing hostility	4, 5	High/ /medium	Introducing ZVC4IoT in a niche non-intimidating BYOD market does not threaten computer manufacturers/vendors.
R2	Users & testing/validating labs may not have full grasp of ZVC4IoT concept	4, 5	High /medium	Properly communicate to end-users how ZVC implements cybersecurity/privacy. White paper, publications, and informative documents will help in mitigating this risk.
R3	Computer OS, Apps & hardware industries do not want to let ZVC4IoT go mainstream	4, 5	High / medium	The business model will not target mainstream computing, but focus on niche segments, such as BYOD. The impact of this risk will be mitigated with targeted market strategy.
R4	The project does not deliver solution matching the goals of the consortium and needs of the stakeholders	2-5	Medium / Low	ZVC deploys a user-centric design and the use-cases selected are conservative and achievable, rather than as a new competing paradigm of the future.
R5	Budget (time/cost) issues due to complexity and possible changes as the requirements for optimum solutions evolve	1	Low / Medium	The scope has been discussed, agreed, defined, using outputs from existing projects. Resources are allocated accordingly. An agile development will keep the project on track.
R6	Critical delays in deliverables and work plan and/or deliverables do not meet sufficient quality standards	All	Low / Medium	Quality procedures, templates and guidelines are key elements for mitigating this risk, as well as the experience of the key partners through previous projects.
R7	Partner leaving the project or conflicts within the consortium	All	Low / High	Consortium Agreement fully covers conflict resolution & consortium changes. If risk materializes, all partners will help find a new partner with similar capabilities to finish work.
R8	Technical specs & requirements of ZVC4IoT device may be ambiguous to some partners	2-4	Low / Low	The project begins with clear specs (T2.1) & architecture (T2.2) approved by all partners (T2.3). The iterative process to be established will drastically mitigate this risk.

3.5 Resources to be Committed

The duration of the project is 36 months and the total budget requested to achieve its objectives is **€3.84 Million**. The ZVC budget does not contain further (additional) funding from neither national nor other programs. The personnel share of the total budget is **70.88%,** which is usual for a design intensive project. This cost includes the manpower for the manufacturing of the ZVC4IoT PoC and its use case prototypes. The staff effort is summarized in Table 3.5.

The total project effort is **485** person-months. The effort distribution is proportional to the WP workload and to the involvement of each partner in the project, but the differences in total effort per partner cannot be taken as an indicator of higher or lower involvement in the project objectives. The effort per WP distribution is also consistent with the project objectives and the characteristics of the work to be carried out. WP2 concentrates the highest effort, since it involves the core research activities pertaining to SOS and ICOS components of ZVC.

Table 3.5 showing number of person months required

Participant	WP1	WP2	WP3	WP4	WP5	Total PMs /Participant
1. UPRC	17	16	12	9	6	**60**
2. BC5	8	26	18	8	10	**70**
3. UTH	3	14	20	10	4	**51**
4. EUT	3	12	13	22	6	**56**
5. CISPA	1	12	16	10	4	**43**
6. ZAS	2	12	4	8	14	**40**
7. CERTH	1	11	18	10	10	**50**
8. AFL	1	14	13	8	5	**41**
9. SBA	1	12	8	8	4	**33**
10. UL	3	14	7	10	7	**41**
TOTAL	40	143	129	103	70	**485**

Other direct costs include acquisition of secretariat consumables, office equipment, IoT devices, manufacturing and fabrication cost for ICOS modules for Mobile & PC, and costs due to dissemination, training, travelling (project progress, conferences, technical or dissemination meetings). Other direct costs also include the audits subcontracted to specialized companies to be conducted as per the rules of the Commission (audit certificates mandatory for EC contributions larger than 325K Euro). Most of the meetings will be made by videoconference.

The equipment costs are **0.57%** of the total, **travel** expenses are kept below **5.05 %.** The "other direct cost" items do not exceed 15% of personnel costs for any of the ZVC4IoT participants hence does not require any additional justification.