D1.4

Second Year Management Report

Funded by
the European Union

Revision v1.0

Work package	WP1
Task	T1.1, T1.2, T1.3
Dissemination level	PU – Public, fully open. e.g., website
Deliverable type	R – Document, report (excluding periodic and final reports)
Due date	31-12-2024
Submission date	18-12-2024
Deliverable lead	BI
Version	v1.0
Authors	Nils Asmussen (BI), Thomas Bohn (NOK), Arantxa Echarte (AUS), Andreas Georgakopoulos (WINGS), Manuela Neyer (IFAG), Patrick Pype (NXP), Michael Roitzsch (BI), Markus Ulbricht (IHP)
Contributors	Work package partners and work package leaders (see below)
Reviewers	Marco Bertuletti (ETH)

Abstract

This document connects the deliverables submitted in year two to the project objectives. It reports work performed within the work packages, summarizes achievements and risks. Finally, we conclude by analysing feedback we received from the project's mid-term review.

Keywords

Deliverables, achievements, milestones, risks, mid-term review

Document Revision History

Version	Date	Description of change	Contributor(s)
v0.1	15-11-2024	Initial version and content outline	Michael Roitzsch (BI)
v0.2	17-12-2024	First complete version	Nils Asmussen (BI), Thomas Bohn (NOK), Arantxa Echarte (AUS), Andreas Georgakopoulos (WINGS), Manuela Neyer (IFAG), Patrick Pype (NXP), Michael Roitzsch (BI), Markus Ulbricht (IHP)
v1.0	18-12-2024	Review comments addressed	Michael Roitzsch (BI)

Contributing Partners

Abbreviation	Company name
BI	BARKHAUSEN INSTITUT
AUS	AUSTRALO
EAB	ERICSSON
IFAG	INFINEON TECHNOLOGIES AG
NXP	NXP SEMICONDUCTORS
WINGS	WINGS ICT SOLUTIONS
IHP	IHP MICROELECTRONICS
NOK	NOKIA NETWORKS GERMANY

Disclaimer

The information, documentation, and figures available in this deliverable are provided by the COREnext project's consortium under EC grant agreement **101092598** and do not necessarily reflect the views of the European Commission. The European Commission is not liable for any use that may be made of the information contained herein.

Copyright Notice

Executive Summary

This document marks the completion of the second year of the COREnext project. It connects the deliverables submitted in year two to the project objectives as promised in the project proposal. We also report the work performed within the work packages that resulted in these deliverables and summarize major achievements and managed risks. Because we already reported project progress in the mid-term report, we reuse material from this report, amended with a delta concerning the project months 19 to 24. The report concludes with an analysis of the feedback we received from the project's mid-term review.

Table of Contents

Introduction **8**

Progress Towards Project Objectives **10**

Work Performed in Year Two **14**

WP1: Management and Coordination 14

WP2: Trustworthiness and Use Cases Requirements 15

WP3: Trustworthy Disaggregated Computing Architecture 17

WP4: Digital Components 18

WP5: Trustworthy Analogue Components 21

WP6: Component Validation in Lab 23

WP7: Computation-Communication Platform Integration Roadmap 23

WP8: Outreach, Exploitation and Collaboration 24

Feedback from Mid-Term Review **27**

List of Figures

Figure 1: Main deliverable flow in year two 8
Figure 2: Structure of project objectives 10
Figure 3: Project timeline 14

List of Tables

Table 1: Deliverables and publications in relation to project objectives 13

Acronyms and Definitions

ASIP	Application-specific instruction set processor
AXI	Advanced extensible interface
DU	Distributed unit
FPGA	Field-programmable gate array
ISA	Instruction set architecture
LDPC	Low density parity check
O-RAN	Open radio access network
PE	Processing element
PHY	Physical layer
RAN	Radio access network
RISC	Reduced instruction set computing
RVV	RISC-V vector extension
TLS	Transport-layer security
VRF	Vector register file
WP	Work package

1 Introduction

COREnext focuses on trustworthiness and efficiency improvements for future 6G networks. In the three years of project runtime, we intend to address two key technical gaps:

- COREnext will offer efficient and scalable hardware accelerators, leveraging programmable components with domain-specific RISC-V extensions and reconfigurable processing on FPGA. The compute fabric will rely on power-efficient interconnects to meet sustainability targets while also serving the increasing throughput and latency needs of applications.
- COREnext will develop a trustworthy-by-design architecture, which protects user privacy and platform integrity, while supporting 6G compute demands in edge servers, base stations, and client-side devices.

In year two, the main technical deliverable flow (see Figure 1) continues the work from year one. Year one ended with D3.1 proposing a trustworthy disaggregated computing architecture, where we identified research gaps in the necessary building blocks. From these gaps, concrete research targets towards components for hardware security and heterogeneous acceleration were derived (D4.1). Year two was focussed on development of these components to initial prototype level in both work package 4 (digital) and work package 5 (analogue). The prototype status was reported in D5.1 for trustworthy analogue components, D4.2 for digital accelerators, and D4.3 for digital trustworthiness. From these component prototypes, the project architecture was finalized in D3.2. Key performance indicators were collected from component development and aggregated by D3.2 in preparation for validation activities in work package 6. Finally, D2.3 fits the prototypical project results back to the initial use cases, analysing the overall trustworthiness improvements.

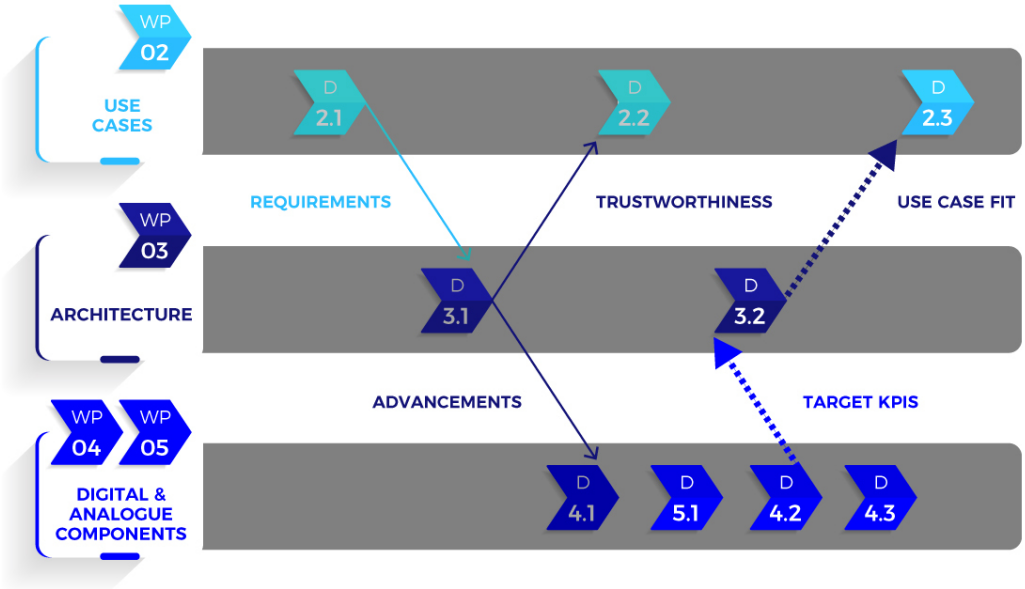


Figure 1: Main deliverable flow in year two

Additionally, in this period, the project produced 11 scientific publications (see Table 1 below for details) and the consortium members attended and presented COREnext-related content in 9

events including HiPEAC 2024, FGBS Spring 2024, EuCNC 2024, INF 2024, CICC 2024, ASPLOS 2024, RTAS 2024, IP-SOC 2024 and IEEE IMS 2024

In summary, this second-year management report outlines the progress towards the project's objectives as documented in deliverables and scientific publications. We summarize the work performed by the beneficiaries within the work packages, including major achievements and managed risks. This document concludes with an analysis of the feedback we received from the project's mid-term review.

2 Progress Towards Project Objectives

In this section, we connect the progress demonstrated by the deliverables and publications to the project objectives as outlined in the proposal and grant agreement. As the project work is organized towards the goals of efficiency and trustworthiness, for both digital and analogue components of the RAN, we can structure the objectives as shown in Figure 2:

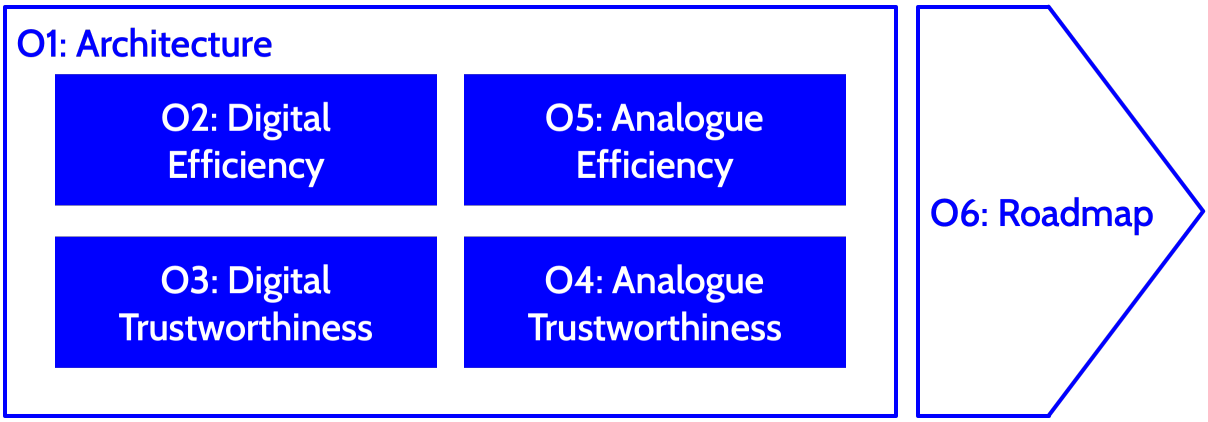


Figure 2: Structure of project objectives

Objective 1: Computing architecture for sustainable and trustworthy B5G/6G processing

This objective targets an open, multi-vendor, and multi-tenant RAN architecture. In D3.2, we have presented the final architecture concept. **In year two,** component development against the initial architecture concept (D3.1) was conducted within WP4 and WP5. The resulting component prototypes informed the architecture, leading to its finalization and the collection of associated KPIs for validation. As end-to-end trustworthiness is an intended result of this objective, in D2.3 we assess the trustworthiness improvements of the architecture. **In year three,** no further work directly on the architecture is expected. Consequently, the associated WP3 has ended. However, components will be validated in WP6 using KPIs informed by the architecture.

Objective 2: Infrastructure and signal processing capabilities for B5G/6G disaggregated virtualized network

This objective zooms in on efficiency of the digital processing. Novel accelerator designs for RAN functions, targeting the integration with RISC-V programmable components and extending their ISA for domain-specific tasks, or aiming for highly flexible, reconfigurable FPGA implementation, are being developed with the goal of an order-of-magnitude improvement in energy efficiency compared to off-the-shelf hardware. **In year two,** first prototypes of these signal processing components were developed, with D4.2 reporting on them. **In year three,** these components will be finalized within WP4 and handed off for validation in WP6. KPIs will be matched against architectural requirements to evaluate how the project delivers on its overall goals.

Objective 3: Enablers for trustworthiness, GDPR-by-design computation-communication platform

Focussing on the trustworthiness side of digital processing, this objective expects the design and development of hardware trust mechanisms for secure isolation in the presence of untrusted hardware components. **In year two,** work on trusted execution environments and virtualization for multi-tenancy has been conducted in WP4 to initial prototype status. Specifically, the M³ system can withstand attack scenarios such as DMA attacks by malicious actors on the memory bus, which was identified as an essential building block of the project architecture. D4.3 reported on these prototype components for digital trustworthiness. **In year three,** work on these components will be finalized within WP4 and handed off for validation in WP6. KPIs will be matched against architectural requirements to evaluate how the project delivers on its overall goals.

Objective 4: Analogue components and ML algorithms enabling trustworthy 6G connectivity

Identifying devices over a wireless connection by their analogue fingerprint is the target of this objective. Such identification already at the wireless interface improves connection integrity and thus trustworthiness at this first line of defence. **In year two,** radio fingerprinting was developed to prototype status and was reported D5.1. The matching signal processing needs are described in D4.3. **In year three,** the radio fingerprinting will be validated in WP6. The resulting accuracy will be evaluated against the architectural requirements.

Objective 5: Analogue HW solution enabling ultra-high speed data interconnect for B5G/6G infrastructures

This objective contributes to system efficiency from the analogue components side. A millimetre-wave data interconnect using plastic fibres as wave guides is designed, targeting a competitive energy consumption of less than 1pJ/bit. **In year two,** the interconnect was developed to prototype status, with initial validation already ongoing. In accordance with the project plan, the progress is not yet reported in a deliverable. **In year three,** this development will lead to D5.2, with validation being conducted in WP6.

Objective 6: Strategic roadmap for disaggregated communication-computing platform involving European microelectronics and telecommunications players

Within this objective, an integrated roadmap is expected to offer a path towards industry adoption of the results generated in the project. **In year two,** the corresponding work package WP7 delivered a first version of the roadmap (D7.1a), which will be publicly available on the COREnext website by January 2025. The project has also reached out to the larger expert community and delivered a white paper with title *Trustworthiness: The Key to Europe's Digital Future* to disseminate our ideas amongst key decision makers. **In year three,** these strategic publications and outreach efforts will continue, leading to the final industrial roadmap document in D7.1b.

The deliverables and the scientific publications are manifestations of the progress towards the project objectives as seen in Table 1:

Artifact	O1	O2	O3	O4	O5	O6
Deliverables						
D2.2: Definition and Impact of Trustworthiness	✓		✓	✓		·
D2.3: Final Report on Requirements and Trustworthiness	✓	·	✓	✓	·	·
D3.2: Integration of Trustworthy Disaggregated Computing Architecture	✓	·	·	·	·	
D4.2: Heterogeneous Acceleration for Efficient Processing		✓				
D4.3: Trustworthy Computation and Orchestration	·		✓			
D5.1: First Concepts for Trustworthy Radio Links Through HW Imperfections and Localization			·	✓		
D7.1a CCS Platform Integration Roadmap	·	·	·	·	·	✓
D8.2: Interim Impact Report	·	·	·	·	·	✓
Scientific Publications						
Core-Local Reasoning and Predictable Cross-Core Communication with M3	✓	·	✓			
Distributed Radar Network with Polymer Microwave Fiber (PMF) Based Synchronization					✓	
Circularly Polarized Sub-THz Antenna Design for Distributed Deployment					✓	
Towards Disaggregation-Native Data Streaming between Devices	✓	✓	·			
LRSC wait: Enabling Scalable and Efficient Synchronization in Manycore Systems through Polling-Free and Retry-Free Operation		✓				
An Energy-Efficient 56-Gb/s D-band TX-to-RX Link using CMOS ICs and Transmit array Antennas					✓	
TeraPool-SDR: A 1.89TOPS 1024 RV-Cores 4MiB Shared-L1 Cluster for Next-Generation Open-Source Software-Defined Radios		✓				
High-Performance Polymer Microwave Fiber Coupler in eWLB Package for Sub-THz Communication					✓	
Sensitivity Analysis of mm Wave Multiuser MIMO with Imperfect Analog Beamforming State Information				✓		
Twisting Effects on X-Shaped Millimetre-Wave Plastic Waveguides					✓	

Broadband Sub-THz Dielectric Waveguides Characterization					✓	
A Transmitter/Receiver Link for High Data Rate Polymer Microwave Fiber Communication at Y-band					✓	

Table 1: Deliverables and publications in relation to project objectives

3 Work Performed in Year Two

This section summarizes all work performed in year two towards the project objectives and deliverables. We group outcomes by work package, with Figure 3 giving an overview of the project until now. All work packages are progressing, with work packages two and three having completed.

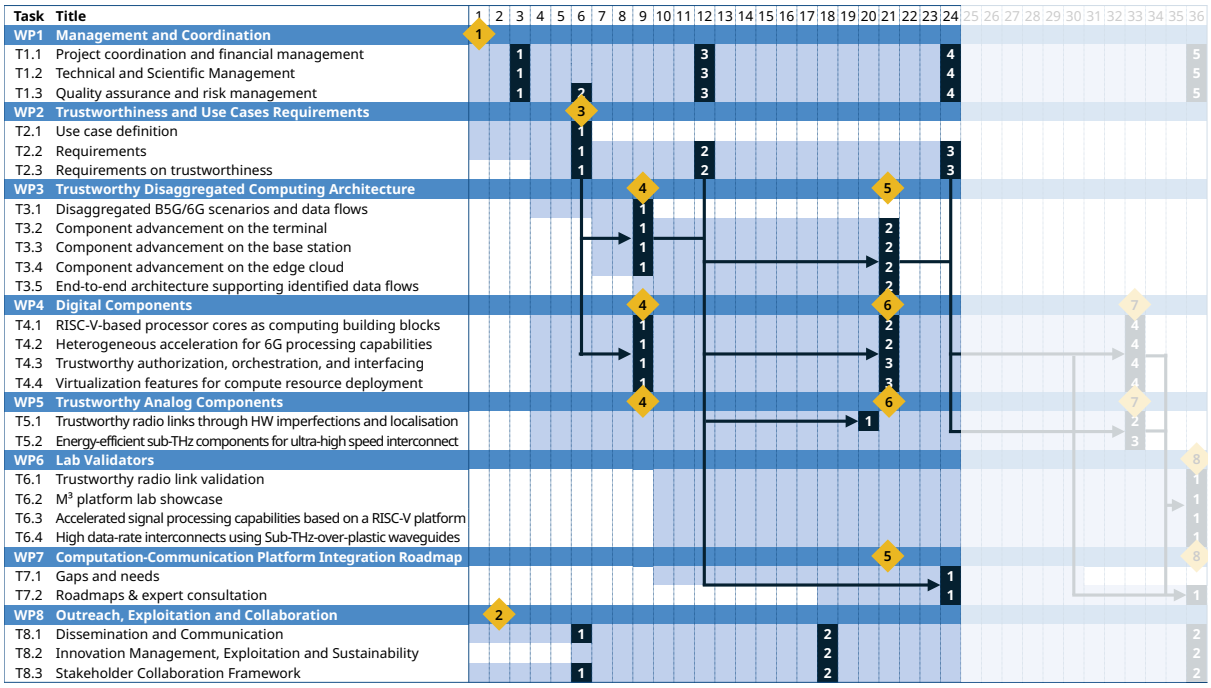
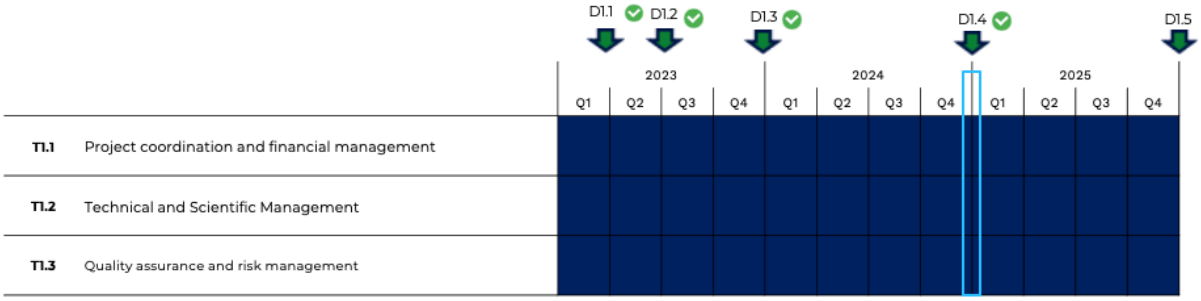


Figure 3: Project timeline

3.1 WP1: Management and Coordination



The management and coordination work package is responsible for ensuring overall scientific and technical excellence in the project. It coordinates between project bodies and manages the reporting to the European Commission. Apart from continued regular online meetings, the project partners met twice in person during the first year:

- for a plenary meeting in January 2024 in Athens and
- to prepare the mid-term review in June 2024 in Antwerp, co-located with EuCNC to reduce travel.

Achieved Outcomes

In the beginning of the first year, internal decisions by industry partners required changes to the leadership of project tasks, with corresponding shifts in project budget between partners. Decisions were taken at the plenary meeting in Athens, ensuring a smooth transition. For the remainder of the year, the management and coordination efforts of WP1 focussed on preparing and submitting the mid-term report as well as presenting the project in the review meeting with the commission and external reviewers.

The core team uses the predetermined project milestones to structure and guide the overall work and to set a clear work focus. All milestones in year two were achieved on time:

- Month 21: Definition of final architecture
- Month 21: First component prototypes

After the mid-term review meeting, the project received feedback from the external reviewers on the direction and progress of the project. A statement regarding this feedback is part of this deliverable.

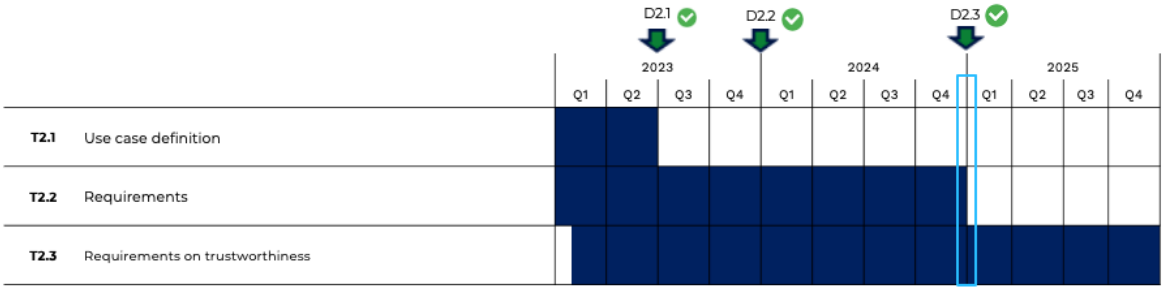
Risk Assessment

None of the foreseen risks have manifested. A challenge was posed by the fact that challenging legal negotiations towards a consortium agreement caused it to be signed only in early year two. With the agreement now signed, we can move forward steadily. All deliverables marked for public dissemination are now available on the project website and on Zenodo.

Deviations From Project Proposal

At the start of the second year, task leadership in WP5 and WP6 changed, because of company-internal decisions. Other project partners stepped in to ensure continuation. The change was agreed upon by all partners and quickly enacted, so there was no impact on project work.

3.2 WP2: Trustworthiness and Use Cases Requirements



In the second year, WP2 progressed well in the two active tasks defined for the work package:

- Task 2.2: Requirements
- Task 2.3: Requirements on trustworthiness

WP2 submitted **Deliverable 2.3: Final Report on Requirements and Trustworthiness** in December 2024, complying with all reporting obligations related to the work package.

Apart from the specific WP2 contributions, this work-package contributed to WP3 for feedback to architectural discussions and to WP4, WP5, WP6 for feedback to digital and analogue enablers as well as lab validators respectively.

WP2 holds regular meetings, and all partners contribute to this work package by:

- Attending meetings
- Actively contributing to the preparation of deliverables
- Reviewing state-of-the-art with respect to trustworthiness and use cases
- Contributing to discussions about the COREnext White Paper

Achieved Outcomes

WP2 submitted Deliverable 2.3 in month 24. It provided the final outcome of WP2 and used inputs from all tasks. This document highlighted additional updates compared to previous WP2 deliverables to requirements, further analysed trustworthiness requirements for both digital and analogue components, and the underlying lab validations to validate the architecture's robustness against emerging threats.

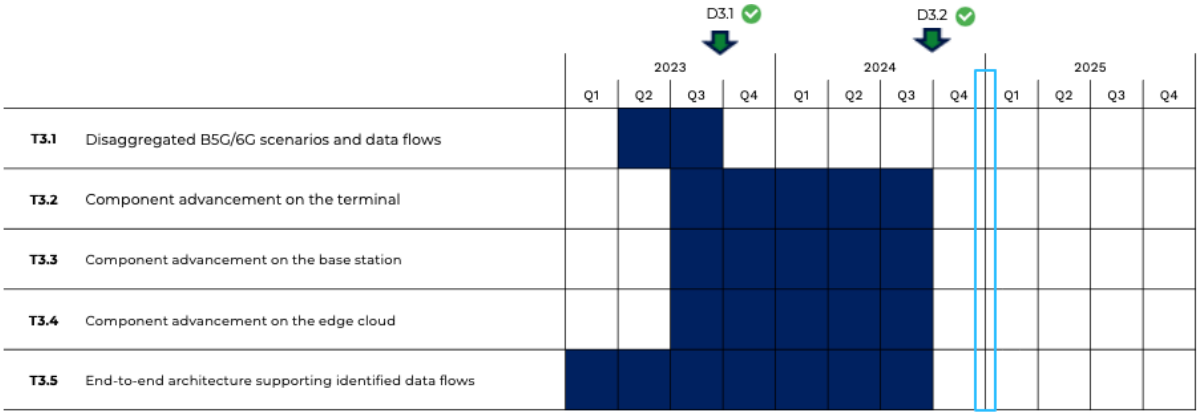
With respect to **Task 2.2: Requirements** we have continued working on the technical and non-technical ones (e.g., number of devices to be supported etc.). For the technical ones, both functional and non-functional system requirements were considered, along with key innovations, KPIs, and system performance metrics, all properly mapped to the use cases identified in the previous task. As a task outcome, the functional and non-functional system requirements, key innovations, KPIs, and system performance metrics to be used for driving the development of the use cases and components were provided.

Finally, regarding **Task 2.3: Requirements on trustworthiness** we continued working on trustworthiness aspects to enable service providers to combine equipment from different vendors and to enable hardware and system providers to deliver and integrate components of a system that provides trustworthiness for a society based on European values of privacy and data protection. This deliverable marks the formal end of technical work in WP2.

Risk Assessment

None of the generic risks were identified for WP2, i.e., underperforming partners, partners leaving, and restrictions due to COVID. Also, the two specific risks related to WP2, i.e., 'Proposed use cases become obsolete' and 'Delay in identifying the requirements and use cases' have not materialized so far. As a result, no mitigation actions were necessary during the year. Regarding the use cases, we are in touch with key stakeholders as suggested also by the project's external Advisory Board, to ensure that use cases are still important and up to date.

3.3 WP3: Trustworthy Disaggregated Computing Architecture



During the second year, WP3 oversaw the technical work on the component innovations identified in year one to be necessary to implement the project architecture. WP4 and WP5 worked on components for trustworthiness and efficiency in the digital and analogue domains. The focus for year two was on the third work package objective: Analyse and balance the trade-off between trustworthiness and efficiency.

The tasks contributing to this work were:

- Task 3.2: Component advancement on the terminal
- Task 3.3: Component advancement on the base station
- Task 3.4: Component advancement on the edge cloud
- Task 3.5: End-to-end architecture supporting identified data flows

The component developments in WP4 and WP5 were monitored for their fit to the architecture tiers terminal, base station, and edge cloud. Finally, the architecture was refined using initial prototypes of the component developments. The result of this refinement was reported in **D3.2: Integration of Trustworthy Disaggregated Computing Architecture.** This deliverable also prepared the project's validation activities in WP6 by deriving validation criteria from the architectural perspective. Furthermore, WP3 contributed an analysis of the security implications of the architecture to Deliverable 2.3.

WP3 in its final months shifted from conducting dedicated bi-weekly meetings to a joint meeting with WP6. This change was made, because both WP3 and WP6 were monitoring development progress of WP4 and WP5 and WP3 was contributing validation criteria to WP6.

Achieved Outcomes

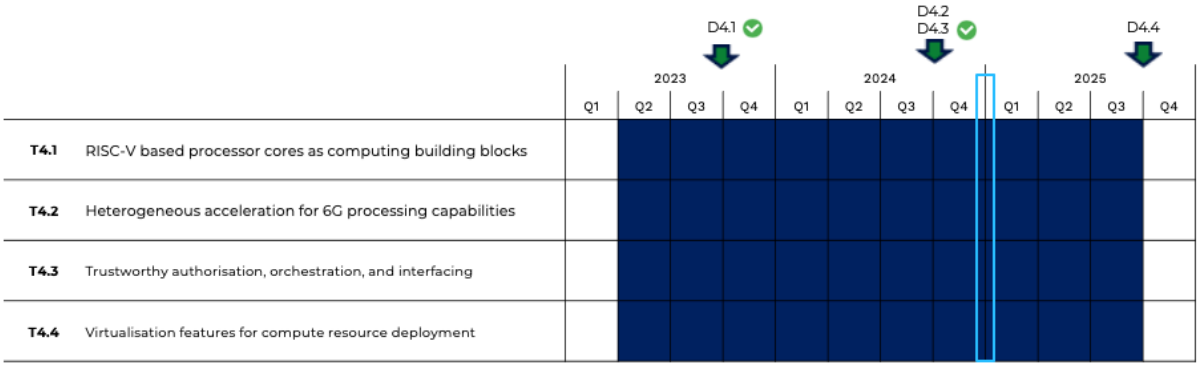
We submitted **Deliverable 3.2** in month 9, which takes the component prototypes from WP4 and WP5 to refine the overall project architecture. This marked the completion of milestone 5. The architecture contains both the COREnext hardware platform, which minimizes the trusted computing base and thereby maximizes the trustworthiness but also takes existing hardware platforms and their secure integration into account. Prototype components were integrated into the three architecture tiers: terminals (**Task 3.2**), base stations (**Task 3.3**), and edge clouds (**Task**

3.4). A wholistic, data-flow-oriented view (**Task 3.5**) led to a security analysis contributed to Deliverable 2.3 and to validation criteria reported in Deliverable 3.2 and contributed to WP6.

Risk Assessment

The two risks specific to WP3 ('Prohibitive energy impact of disaggregation/virtualization' and 'Bad trade-off between resilience/trustworthiness and energy consumption') did not manifest so far. The corresponding validation metrics have been reported to WP6 and will be monitored there.

3.4 WP4: Digital Components



During the second year, WP4 activity focused on the following work package objectives:

- WPO 4.1: Increase in computing capabilities to meet B5G/6G performance and efficiency demands.
- WPO 4.2: Virtualisation features for disaggregation, multi-tenancy, and multi-vendor requirements.
- WPO 4.3: Deeply embedded trustworthiness primitives for enhanced privacy and integrity.

In the second year, WP4 supported the achievement of milestone 5 in month 21 by contributing to D3.2: Integration of trustworthy disaggregated computing architecture. In the same month WP4 successfully delivered **D4.2: Heterogeneous acceleration for efficient processing,** and **D4.3: Trustworthy computation and orchestration**, thereby contributing to the achievement of milestone 6.

The following sections summarize the achieved results, outputs, outcomes, and assessed risks for the different components developed in WP4 and link the work to the different tasks listed above.

Achieved Outcomes

WP4 progressed well in all four tasks defined for the work package, namely:

- Task 4.1: RISC-V based processor cores as computing building blocks
- Task 4.2: Heterogeneous acceleration for 6G processing capabilities
- Task 4.3: Trustworthy authorization, orchestration, and interfacing
- Task 4.4: Virtualization features for compute resource deployment

The work on these four tasks is aligned to two main research directions, which we present below.

Acceleration of the RAN

For **Task 4.1: RISC-V based processor cores as computing building blocks,** moving from the preliminary analysis on computational complexity and arithmetic precision of the 5G lower-PHY, ETH devised a set of floating-point (32b, 16b, and 8b) RISCV ISA extensions for wireless workloads. We added instructions targeting complex number arithmetic and SIMD instructions to increase the performance on low-bit precision (16-8b) workloads to the ratified zfinx RISC-V set. We implemented these extensions in the processing elements of the TeraPool, a Many Core cluster for software-defined wireless processing with 1024 cores and 4MiB of fully shared L1 scratchpad. We tested PPAs on a fully placed and routed instance of the cluster and we evaluated the end-to-end BER performance of MMSE-detection in floating point 16b and 8b precision.

As part of task **T4.1** CYB researched modifications of current computer architecture enabling self-protecting data such that security properties can be realised without extensive dependencies on system level software.

For tasks **T4.1** and **T4.2: Heterogeneous acceleration for 6G processing capabilities**, TUD investigated the utilization of vector processors based on the proposed RISC-V vector extension (RVV) for communications signal processing in general and the High-PHY processing of the O-RAN Distributed Unit (DU) in particular. The aim is to build an efficient programmable accelerator that lies between general-purpose processors and fixed-function accelerators, or application-specific instruction set processors (ASIPs) on the performance-flexibility trade-off curve. The initial investigation is presented in deliverable D4.1. TUD have identified the vector register file (VRF) as a bottleneck in contemporary vector processors. When the vector processor is running with high utilization, the VRF must support many concurrent accesses. While banking reduces some of the access conflicts, state-of-the-art static bank layout leave room for improvement. TU has analysed the bank conflicts and proposed dynamic bank layouts to either improve performance or save area-expensive operand queues with loss of performance. A paper on this topic was accepted for publication in an ACM journal.

As part of **Task 4.2,** an extension of the Kalray toolchain (compiler, assembler, linker, simulator, debugger) and of the GCC RISC-V compiler were developed so that OpenMP Offload directives in the RISC-V source code would transfer execution for accelerated processing on the Kalray processing elements (PEs). In addition, the Kalray PE architecture called KVX has been improved to deliver the compute capabilities required by L1 PHY processing in a Distributed Unit (DU) in the 5G New Radio architecture, specifically Channel Estimation and Channel Equalization.

Also, as part of **Task 4.2,** the characterization of the LDPC decoder has taken place. The design has been verified in 28 nm CMOS technology with the maximal clock frequency up to 2000 MHz, assuming worst-case conditions (slowest process, 0.9V, 125 C). Due to a fully unrolled, pipelined architecture, the accelerator can deliver decoding throughput up to 1200 Gb/s for coded stream and 1000 Gb/s for uncoded data.

Furthermore, in **Task 4.1 and 4.2,** we are delving into AI accelerators as an energy-efficient solution for MAC schedulers. To investigate the possible use of reinforcement learning (RL) agents for Resource Block Group (RBG) allocation to connected User Equipment (UE), we integrate 5G-

LENA–a 5G network simulation framework based on the well-known discrete-event simulator NS-3–with OpenAI's Gym environment for deep reinforcement learning (Deep-RL). The goal is for the agent to replace classical allocation algorithms like round robin, maximum rate, or non-AI-based QoS-aware allocators within the MAC scheduler. This setup is intended to provide deeper insights into resource consumption (e.g., the size of the artificial neural network) and performance with respect to fairness, throughput, and latency before any deployment to a real-world system, while allowing for a direct and fair comparison to existing allocators. To gain a more precise and realistic understanding of its application in sub-THz bands, we further integrate NYUSIM as a wireless channel simulator. This combined approach allows us to evaluate the feasibility and performance of RL-based RBG allocation under conditions that closely reflect the challenges of next-generation wireless networks.

Furthermore, our aim is a thorough investigation and a closely integrated implementation with a RISC-V processor through ISA extension. In collaboration between IHP and ETH, work has begun by examining various PULP-based platforms as the foundation for our implementations. Considering criteria like multi-core support, Linux compatibility, an AXI interface, and more, we explored several options before settling on the Cheshire platform. Currently, we are familiarizing ourselves with the platform and the CVA6 cores while exploring diverse possibilities to incorporate the MAC accelerators.

Virtualization and Trustworthiness

In **Task 4.3: Trustworthy authorisation, orchestration, and interfacing,** solutions towards FPGA virtualization are being developed. Current FPGA virtualization solutions do not address authentication, even less so in a multi-tenant context. We are working on an authentication protocol proposal based on OAuth 2.0, which is modified to include FPGA context usage. The protocol allows for the establishment of a secure channel between the FPGA instance and the client, with a transport layer security (TLS) session set up for secure communication with perfect forward secrecy between the FPGA and the client.

In **Task 4.4: Virtualization features for compute resource deployment,** setting up the experimental infrastructure analogue to a production base station started. Equipment was provisioned according to the scale and purpose of the experimental appliance. Operation of the appliance started in the end of the year. In parallel of setting up the infrastructure, the OpenAirInterface software stack used within this appliance was improved to leverage the capabilities of production computing architectures. The knowledge obtained from setting up and operating this infrastructure will be disseminated among other way through the software and documentation of OpenAirInterface which is a leading community software and research tool in the field of mobile communications.

As part of **Tasks 4.2, 4.3, and 4.4,** Trusted Execution Environments (TEEs) are a major contribution and a building block in the overall COREnext architecture. BI is continuing to develop its M³ platform, a microkernel system for a tile-based hardware platform, extending it with a notion of a trusted execution environment (TEE). An initial prototype for M³-based TEEs is implemented in a software simulator. We published on accelerator integration on the international Workshop on Heterogeneous Composable and Disaggregated Systems (HCDS) and on M³ capabilities for real-

time systems at the IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS).

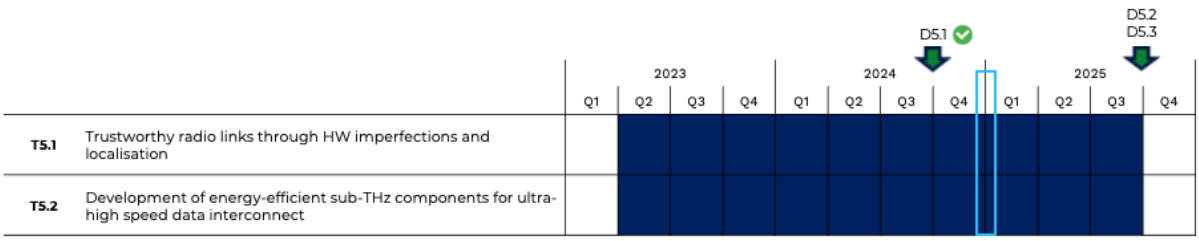
Task 4.3 additionally addresses Radio Frequency Fingerprinting, a device authentication method leveraging hardware-related impairments. Over the summer, extensive data from two identical SDR-based transmitters (USRP B205mini-i) connected to an SDR-based receiver (USRP B210) were collected by our colleagues from W5.1. Tests included five frequency bands (1.5 to 5.5 GHz) each at multiple high-gain settings. Our initial experiments with CNN and CNN-LSTM models demonstrate near-perfect (>99%) accuracy in distinguishing two devices, even under varied training/test conditions and payloads. These methods are also being evaluated in a (E)Pix 5G end-to-end link simulator, facilitating future integration into complex communication systems. We further extended these studies by introducing external power amplifiers (PAs) to the SDRs. This setup, influenced by varying supply voltages and non-linear behaviours, provides a more challenging scenario. While differentiating completely distinct SDRs remains straightforward, distinguishing the same SDR fitted with different external PAs is more difficult.

Risk Assessment

While virtualization and disaggregation are expected to enhance the trustworthiness and efficiency of networks, the actual benefit may not be sufficient (Risk: Prohibitive energy impact of disaggregation/virtualization). Therefore, one of the objectives of the project until its completion will be to assess to which extent these architectural choices are beneficial to networks and under which conditions (WPOs 6.1, 6.2, Tasks 4.2, 4.3, 4.4, 6.1, 6.2, 6.3). Moreover, the energy impact of disaggregation/virtualization is yet to be studied in the context of vector processors.

Additionally, implementing a major experimental infrastructure comes with some risks (New risk: Key features are not delivered on time in the demonstration infrastructure, Likelihood: Medium, Severity: Low; WP4, WP6). Despite the effort invested in the delivery and integration of COREnext and third-party components in the demonstration infrastructure, some components may be not featured or even delivered at the completion of the project. Fortunately, one benefit of standard virtualization and disaggregation is that they enable multi-vendor architecture where any implementation of a component can be replaced by a competing implementation.

3.5 WP5: Trustworthy Analogue Components



In WP5, the partners develop concepts, methods, and circuits to increase the trustworthiness of communication links. WP5 is connected to WP4 (assess digital compute requirements for communication, sensing and PHY layer security), and WP6 (physical verification of hardware and postprocessing using developed algorithms, design support for high-speed data interconnect, including circuit-package co-design based on manufacturing and packaging requirements).

WP5 consists of two main tasks:

- Task 5.1: Trustworthy radio links through HW imperfections and localisation
- Task 5.2: Development of energy-efficient sub-THz components for ultra-high speed data interconnect

Monthly WP5 meetings and individual task level meetings have taken place online.

Concerning **Task 5.1**, the following activities are ongoing:

- Development (jointly with T6.1) of a sub-6GHz "HW-in-the-loop" hardware platform, based on software defined radio and external components to emulate devices and create datasets for WP4.3, perform studies and support concept developments in WP5.1, and for demonstration/validation activities in WP6.1, in the context of RF Fingerprinting
- Development (jointly with T6.1) of a sub-10GHz "BS TX PA -in-the-loop" simulation and measurement platform to generate data showing random but static variations due to semiconductor production or system assembly
- Development of a multiuser MIMO DL link-level simulation platform for the D-band
  - to assess robustness, beam accuracy and beam leakage in the Sub-THz frequency bands
  - as one of the sources of experimental data for RF fingerprinting
  - as the potential basis for the sub-THz "HW-in-the-loop" POC in T6.1 and accordingly develop the additional required signal processing to compensate the HW non-idealities in the D-band RF chip.

Deliverable 5.1: First Concepts for Trustworthy Radio Links Through HW Imperfections and Localization has been filed as foreseen in M20.

The work in **Task 5.2** can be summarized as follows:

- Y-band Sub-THz SiGe BiCMOS Tx/Rx design in B11HFC and B12HFC technology, characterization and measurements
- Waveguide-to-PMF transition design for D-band and H-band
- Design of stacked Micro-PCBs in-PCB transitions for D-band
- Implementation of Air-Filled Substrate Integrated Waveguide (AFSIW) passives and interconnection at D-band and beyond
- Design of RFIC to PMF coupling
- Embedded Wafer Level Packaging (eWLB), where the transition is implemented in the form of antennas radiating into the fibre

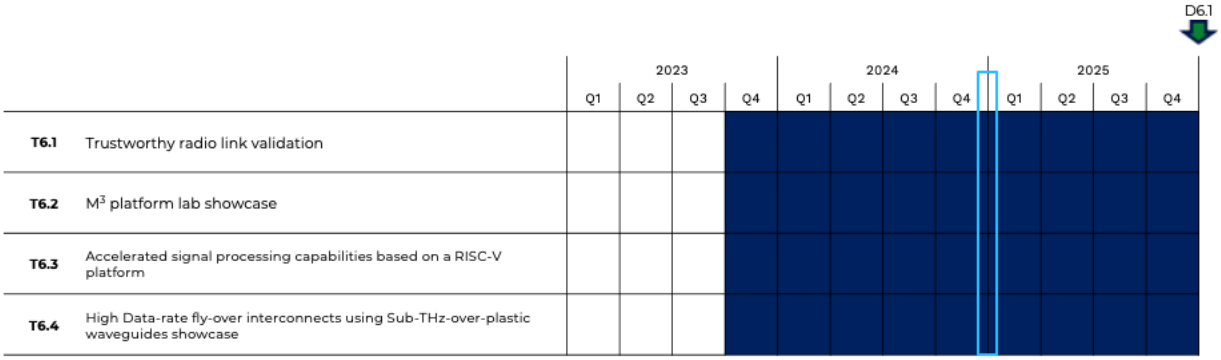
Risk Assessment

The following risks have been foreseen:

- The 140GHz testbed used for fingerprint evaluation may not be ready for use or not fully functional.
- Design and manufacturing of H-band waveguide may be too slow.
- Limited performance for H-band transceivers.

So far, these risks did not manifest. We will continue to monitor during the execution of WP5 to take fast action in case they become reality.

3.6 WP6: Component Validation in Lab



WP6 was kicked-off in month 10 (November 2023) in a virtual meeting with the objective to demonstrate the results from WP4 and WP5 to validate versus the use case requirements from WP2 and the computing architectures defined in WP3. The WP6 team continued with monthly meetings and met physically in Athens on January 24. During early 2024, Giuseppe De Astis (IFAT) took over WP6 lead. The focus of WP6 in year two was on collecting the inputs from WP2 to WP5 and strategically drive the planning for lab validation. In February '24 the WP3 team and TIM were included into WP6 meetings; WP6 team still is continuously extending to include relevant partners and experts to execute the planned validations. Since November '24, the WP6 team is supporting deliverable writing for D2.3 (Final report on requirements and trustworthiness) and is also following up inputs for the upcoming validations, such as D5.1 in M20 (input for Task 6.1), D4.2/D4.3 in M21 (inputs for Tasks 6.1, 6.2, and 6.3), and D4.4/D5.2/D5.3 in M33 (inputs for tasks 6.1, 6.2, 6.3, and 6.4).

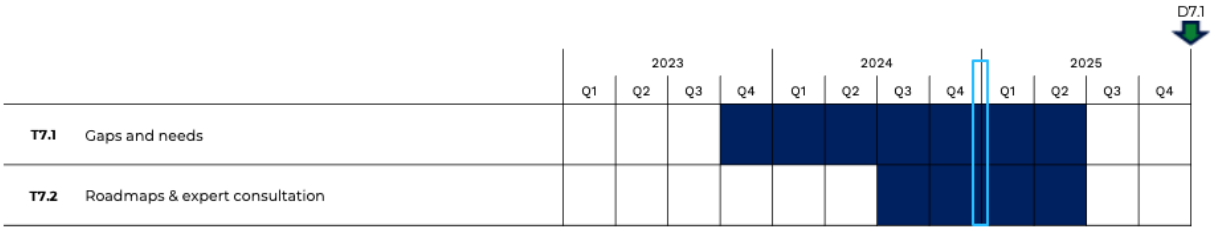
Specific tasks in WP6 are the development of four technology validators:

- Task 6.1: Trustworthy radio link validation,
- Task 6.2: M³ platform lab showcase,
- Task 6.3: Accelerated signal processing capabilities based on RISC-V platform, and
- Task 6.4: High data-rate interconnects using Sub-THz-over-plastic waveguides showcase.

Risk Assessment

Within WP6 monthly meeting we are constantly monitoring the progress of concepts for the validators and their realisation. Currently there is no indication for significant delays or other risks.

3.7 WP7: Computation-Communication Platform Integration Roadmap



WP7 consists of two main tasks, which will run in parallel with the goal to create an integrated computing-communication-sensing platform roadmap, to be signed-off by all relevant stakeholders in the field. During year two, the focus was on project-internal interaction, especially with WP2 (baseline requirements for roadmap), WP3 (architecture proposals), WP6 (validation results) and WP8 (dissemination).

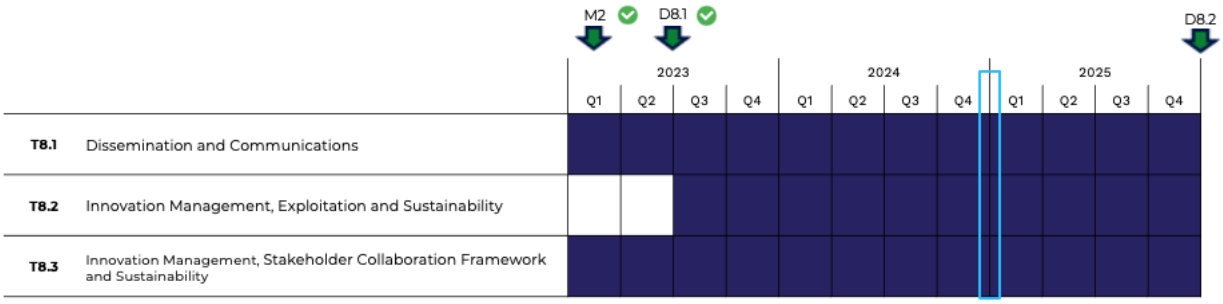
These internal discussions led to WP7 contributing to the COREnext whitepaper with an outlook on future research needs. This work will also contribute to the initial version of **D7.1: Computing-communication-sensing platform integration roadmap,** due for publication by the end of 2024 as a first progress report of WP7.

Further work in year three will extend to incorporate viewpoints and have discussions with external experts. These expert consultations will then help us shape the final version of D7.1, due for publication by the end of the project.

Risk Assessment

No risks have been identified for WP7 so far. The critical element will be the collection of information and data from external stakeholders, especially from the point of view of confidentiality versus publicly available information. This will be continuously monitored during the execution phase of WP7.

3.8 WP8: Outreach, Exploitation and Collaboration



WP8 made good progress in all three tasks defined for the work package.

- Task 8.1: Dissemination and Communication
- Task 8.2: Innovation Management, Exploitation and Sustainability
- Task 8.3: Stakeholder Collaboration Framework

In year two, WP8 submitted **Deliverable 8.2: COREnext Interim Impact Report** in June 2024, complying with all reporting obligations related to the work package for this period.

Apart from the specific WP8 contributions, this work-package contributed to WP7 by attending monthly meetings and contributing to **Deliverable 7.1a,** the CCS Platform Integration Roadmap. This involvement included identifying gaps and needs with consortium members and providing relevant content to address them in D7.1a. WP8 also contributed to all other WPs with branding and design support.

WP8 holds monthly meetings, and in year two all partners contributed to this work package by:

- Attending monthly meetings
- Reviewing C&D material (i.e., website, slide deck and pitch deck, deliverable template, etc.)
- Reviewing non-scientific publications
- Supporting online activity by engaging and sharing with social media posts
- Contributing and disseminating the Newsletters
- Sharing information about COREnext related events and publications they attended and produced to be used for C&D activity
- Contributing to stakeholders' engagement and stakeholder management strategy
- Helping to identify relevant EU projects to liaise and collaborate with
- Producing a white paper with title 'Trustworthiness: The Key to Europe's Digital Future'
- Producing 11 new scientific publications (added to the 8 scientific publications in 2023)
- Attending more than 9 new events to actively support the dissemination of COREnext initiatives across diverse stakeholders, including industry professionals, academic institutions, and other relevant sectors.

Achieved Outcomes

WP8 submitted **Deliverable 8.2** in month 18. The purpose of this Interim Impact Report was to provide an update on the progress and effectiveness of the impact of the communication, dissemination, exploitation and standardisation activities undertaken as part of the project in the first 18 months. It served as a mid-point evaluation to assess whether our efforts were on track to achieve the desired outcomes and objectives outlined in D8.1 Impact Master Plan.

Key indicators of our communication and dissemination efforts include substantial traffic to the COREnext website, which, by the end of year 2, has received over 5,494 views from more than 1,351 unique visitors. Moreover, COREnext has published 919 social media posts, reaching over 1,603 followers and COREnext social media received more than 90K impressions. The website features 29 awareness publications, 1 white paper, 11 deliverables, and 14 scientific publications, all of which are crucial for maximizing the project's impact.

Attending events allows consortium members to disseminate results, network, exchange knowledge, influence policy, and foster collaborations across sectors. Events attended, in year 2, include HiPEAC 2024, FGBS Spring 2024, EuCNC 2024, INF 2024, CICC 2024, ASPLOS 2024, RTAS 2024, IP-SOC 2024 and IEEE IMS 2024.

Regarding **Task 8.1: Communication and Dissemination outputs**, by the end of year **2,** we have further strengthened the COREnext project brand through the development of new visual elements. Additionally, we have expanded COREnext's presence across various media platforms and newsletters, publishing several press releases to enhance visibility. Our online presence has grown with the launch of new social media channels, such as Bluesky and YouTube.

To support engagement, we have initiated project-related campaigns like COREnext in the Spotlight, conducted interviews, published newsletters and awareness articles, and produced a range of promotional materials, including videos showcasing key COREnext concepts and outcomes.

With these C&D outputs we aim to enhance general awareness and interest in the project by, for example, clearly conveying technical and scientific results, while also increasing awareness.

Additionally, all WP8 efforts are geared towards creating impact beyond the boundaries of the project.

In terms of **Task 8.2: Innovation Management, Exploitation and Sustainability,** the main purpose of the task is to design and execute the overall exploitation roadmap for COREnext, with the ambition to foster the use, consolidate the uptake and seek the sustainability of the Key Exploitable Results (KERs) across the value chain. In the second year, the task continued the work on the COREnext exploitation roadmap and identified three Key Exploitable Results (KERs) and four innovations. It also proposed a conceptual business model. Additionally, the task worked on the COREnext IP strategy and identified relevant project-related standardization activities.

For the next period, updates on these matters will be reported to show how COREnext can further exploit its key innovations in line with the project's **Objective 6:** Strategic roadmap for disaggregated communication-computing platform involving European microelectronics and telecommunications players.

Lastly, with regards to the **Task 8.3: Stakeholder collaboration framework,** COREnext impact has been identified and evaluated across a wide spectrum of entities, encompassing the B5G/6G ecosystem, application sector, microelectronics ecosystem, relevant partnerships and networks, policy makers and society.

In year 2, we have actively collaborated with projects like Hexa-X-II and CENTRIC to support mutual communication and dissemination efforts, while exploring potential synergies between our initiatives. Additionally, we have engaged with initiatives such as SNS JU and CHIPS JU, and we are currently reaching out to other initiatives, including 6G-IA, 6G4Society, and THALES, to propose a joint workshop about Trustworthiness at EuCNC 2025. We are confident that stakeholder engagement activities will intensify in year 3, as we will have the opportunity to present and discuss the project's findings and technological advancements in greater detail.

Risk Assessment

None of the generic risks were identified for WP8, i.e., underperforming partners, partners leaving and restrictions due to COVID. As the collaboration agreement was signed in 2024, we only identify one relevant risk that could have an impact on the performance of this work package.

Risk 1: low engagement and reporting from members (severity: low/medium). To mitigate this risk, we keep constant communication with members and send reminders about reporting resources in place.

4 Feedback from Mid-Term Review

In the First Year Management Report (D1.3), this last section reported on the advisory board meeting of the project. This year, we did not conduct such a meeting for two reasons: first, the late signing of the consortium agreement led to delays in the NDA signature process with the board members. This pushed a potential board meeting date until after the mid-term review. At this point however, we already received feedback on the project progress from the external experts as part of the mid-term review. We thus opted to digest this feedback first and plan how to address it, then present this plan at an advisory board meeting early 2025 to discuss our approach with the board members. The rest of this section thus presents our initial comments to the feedback gained during the mid-term review. Overall, the project's progress was well-received, with the first recommendation being to continue along this path. We did however identify four main groups of project-wide recommendations, which we comment in individual subsections below. Individual work package feedback will be handled by those work packages directly.

4.1 Monitor Top-down and Bottom-up Convergence

COREnext was designed to cover a broad range of topics from digital to analogue and across various layers of the technology stack from semiconductors over hardware design up to operating systems. To use the three project years effectively, we decided to combine a top-down approach by iterating from use case analysis to architectural requirements to component needs, with a bottom-up approach by looking at existing research and industry trends and developing components towards previously identified needs. This method allowed us to ramp up technical development on the components early but bears the risk of designing something that in the end does not fit the overall project architecture and project objectives.

The reviewers thus recommended to monitor this convergence. We address this recommendation already in Deliverables 3.2, where the project architecture is refined given the component prototypes. Furthermore, Deliverable 2.3 brings use cases and trustworthiness aspects together and matches them to the conducted developments. An output of this process are validation criteria that are derived from project objectives and that will help WP6 to measure the success of the developed components.

4.2 Increase Engagement with Relevant Stakeholders in Standardization and Regulation

Reviewers mentioned stakeholder groups such pre-standardisation and standardisation groups, industrial consortia, alliances in the 6G area, as well as regulatory bodies. Further, the project was asked to increase activities to identify and explore opportunities for industrial exploitation.

With component prototypes only being available at the month 21 milestone, many activities related to the above stakeholder groups were deliberately withheld until year three of the project. In year three, we certainly intend to ramp up such activities and showcase our results to those groups as well as at relevant exhibitions. Demonstrators are being built for evaluation in WP6, and these will be repurposed also for such outreach activities to stakeholder groups. With many major

industry players already part of the consortium, industrial exploitation will be concretized and discussed internally and with external parties towards the final WP7 deliverable of the computing-communication-sensing platform roadmap.

4.3 Assessment of Trustworthiness Architecture

Finally, the reviewers commented that the trustworthiness use cases, requirements, and the proposed architecture should be compared against the perspectives in other 6G-related EU projects as well as views outside the EU. We conducted a first trustworthiness evaluation of the COREnext platform in Deliverable 2.3. However, this evaluation compares against a research perspective. A comparison against other 6G EU projects' viewpoints as well as non-EU viewpoints is missing. We will conduct a corresponding study in year three and provide such a comparison as part of Deliverable 7.1 at the end of the project.