CORENEXT

D1.3

First 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	31-12-2023
Submission date	12-12-2023
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	Arantxa Echarte (AUS), Manuela Neyer (IFAG)

Abstract

This document connects the deliverables submitted in year one to the project objectives. It reports work performed within the work packages, summarizes achievements, and risks, and finally concludes with a statement from the project's Advisory Board.

Keywords

Deliverables, achievements, milestones, risks, advisory board report

Document Revision History

Version	Date	Description of change	Contributor(s)
v0.1	13-10-2023	Initial version and content outline	Michael Roitzsch (BI)
v0.2	15-11-2023	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	12-12-2023	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 first year of the COREnext project. It connects the deliverables submitted in year one 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. The report concludes with a statement from the project's Advisory Board, judging after we presented the progress made in year one.

Table of Contents

List of Figures

List of Tables

Acronyms and Definitions

ASIP	Application-specific instruction set processor
AXI	Advanced extensible interface
CPU	Central processing unit
DU	Distributed unit
FEC	Forward error correction
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
TRX	Transceiver
VRF	Vector register file
WP	Work package

1 Introduction

The COREnext project is motivated by the acceleration of research and development on Beyond-5G and 6G mobile networks. While these developments enable interesting new applications, they also pose risks for the European economy and society as big non-European players are pushing into the market with RAN-as-a-service offerings. In response, COREnext brings together 23 European partners, including major representatives from the telecommunications and semiconductor industry, to push against this development.

COREnext is positioned to anticipate technological developments required 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 accelerators based on RISC-V extensions and FPGAs as well as 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.

Towards these goals, we have set up a work package structure to organize the technical and strategic workflows within the project (see Figure 1). Use case and requirements analysis (WP2) will inform the technical work on an overall trustworthy architecture concept (WP3). From this architecture concept, we identify research gaps in both digital and analogue components, which the corresponding work packages (WP4 & WP5) address. Finally, validation of the developments (WP6) provides feedback of the project's achievements. Next to this technical work, a flow of strategic work takes place, starting from requirements and architecture, but resulting in a strategic roadmap (WP7) for industrial adoption of the project results.

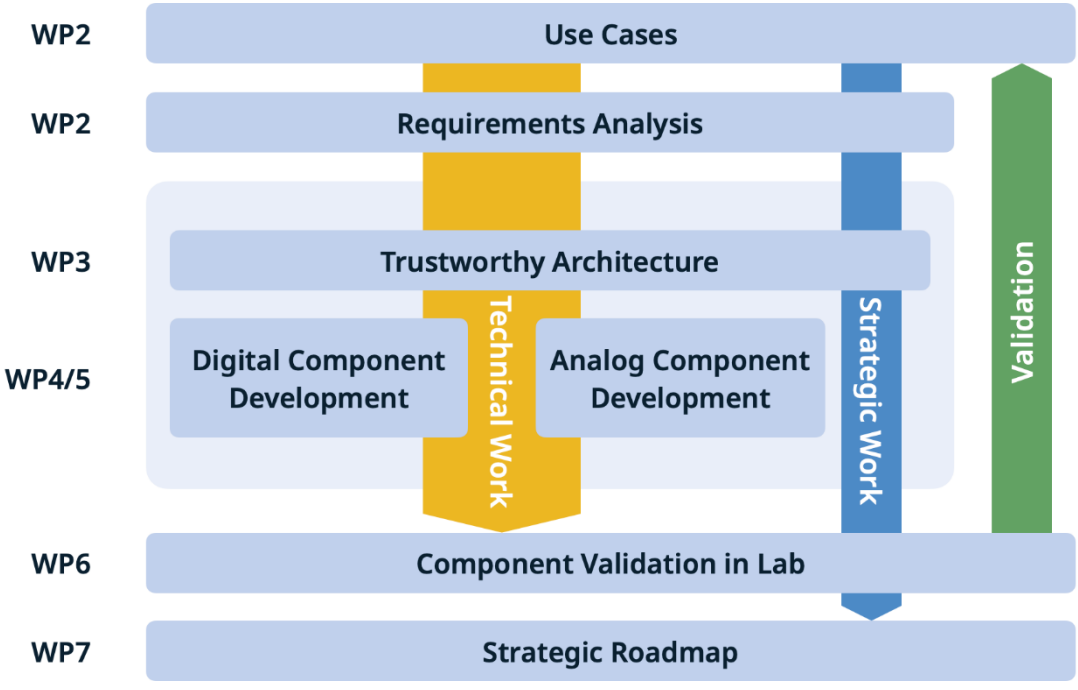


Figure 1: Work package structure

The project is facilitated by management and coordination from WP1 and exploitation and dissemination from WP8. A project handbook (D1.1) as well as a data management plan (D1.2) and impact plan (D8.1) have been created to establish the necessary support infrastructure around the technical work. Ethical aspects of the project have been studied in D9.1.

In year one, the main technical deliverable flow (see Figure 2) began with an analysis of use cases and requirements (D2.1). This led to an initial proposal for a trustworthy disaggregated computing architecture (D3.1), where we identified research gaps in the necessary building blocks. From these gaps, concrete research targets towards hardware security primitives and heterogeneous acceleration (D4.1) were derived. At the same time, the architecture concept was verified against use-case-specific attack vectors to assess the project's overall approach towards trustworthiness (D2.2).

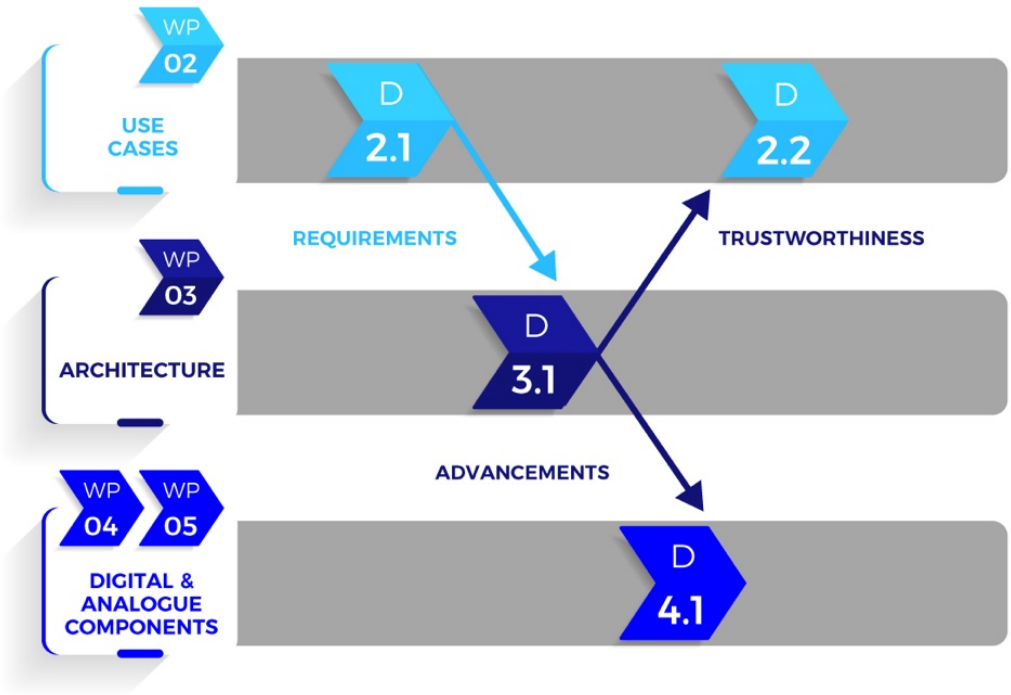


Figure 2: Main deliverable flow in year one

Additionally, the project already produced four scientific publications (see Table 1 below for details) and the consortium members attended and presented COREnext-related content in 16 events including IWPE'23, HotOS'23, EuCNC'23, and SOSP'23. The consortium plans to publish a COREnext-related white paper in January 2024.

In summary, this first-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 a report by the COREnext Advisory Board evaluating the project's progress in year one.

2 Progress Towards Project Objectives

The technical deliverable flow connects a use case and requirements analysis (D2.1) to an architecture concept (D3.1) to component needs (D4.1) and an overall trustworthiness approach (D2.2). This was flanked with additional management (D1.1, D1.2), impact (D8.1), and ethics deliverables (D9.1).

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 along the overall goals of efficiency and trustworthiness as well as digital and analogue components, we can structure the objectives as shown in Figure 3:

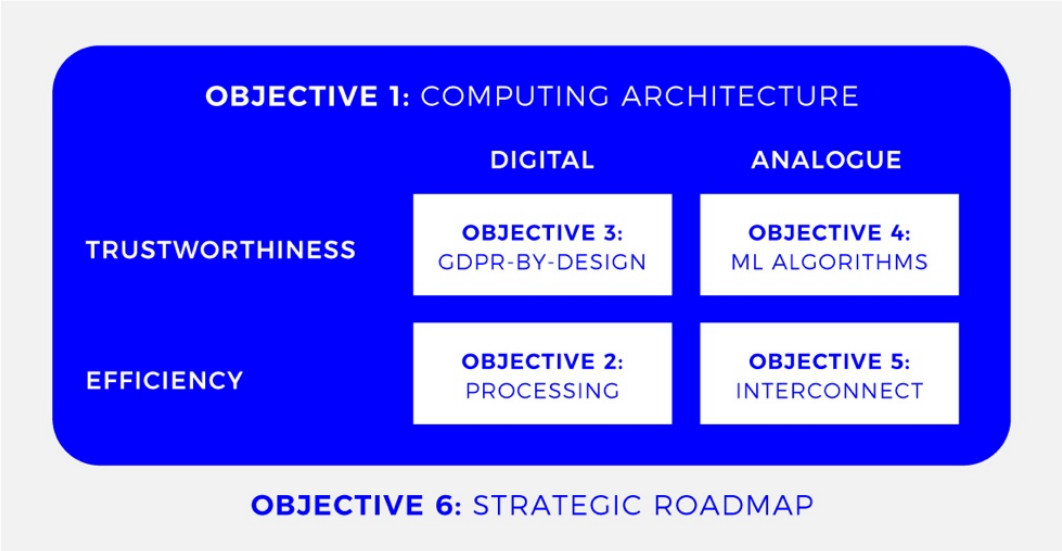


Figure 3: Structure of project objectives

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

This objective targets an open, multi-vendor, and multi-tenant RAN architecture. In D3.1, we have presented an architecture concept to this end. **In year one,** we have described components that should be part of this architecture and identified research gaps, where state-of-the-art components do not meet the needs of the proposed architecture. As end-to-end trustworthiness is an intended result of this objective, in D2.2 we assess the trustworthiness approach of the architecture. **In years two and three,** this line of work will continue with component development in WP4 and WP5 and their validation in WP6. Feedback will be given to WP3 and WP2 to refine the architecture and cross-check with the requirements.

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 based on RISC-V extensions and FPGAs are being developed with the goal of an order-of-magnitude improvement in energy efficiency compared to off-the-shelf hardware. **In year one,** a plan for the component development situated in WP4 and has been laid out in D4.1. **In years two and three,** this work will continue in WP4, with validation in WP6. Feedback will be given to WP3 as to what component properties the architecture can expect.

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 one,** we identified that a platform to withstand attack scenarios such as DMA attacks by malicious actors on the memory bus to be an essential building block of the architecture presented in D3.1. The fundamental design of a multiprocessor system-on-chip based on the M³ microkernel is explained in D4.1. **In years two and three,** work on trusted execution environments based on M³ will be conducted in WP4 and validated in WP6. The achieved security posture will influence the architecture discussion in WP3.

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 one,** WP5 has made progress on the radio sensing part, but according to the project plan has not yet reported this work as part of a deliverable. The matching signal processing needs are described in D4.1. **In years two and three,** the radio fingerprinting will be reported in D5.1 and validated in WP6. The resulting accuracy will inform the architecture in WP3.

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 one,** such a low-energy high-speed interconnect has been identified as a key building block used in the D3.1 architecture for resource disaggregation in base station hardware. WP5 partners are working on realizing the required components. In accordance with the project plan, the progress is not yet reported in a deliverable. **In years two and three,** this development will lead to D5.2, with validation following 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 one,** the corresponding work package WP7 has only started in M10. Thus, no reportable results have been produced by WP7. However, the project has already reached out to the larger community and is working on a first white paper to disseminate our ideas amongst key decision makers. **In years two and three,** such strategic publications and outreach efforts will continue, leading to an industrial roadmap document in D7.1.

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						
D1.1: Project Management Guidelines	·	·	·	·	·	·
D1.2: Data Management Plan	·	·	·	·	·	
D2.1: Use Cases and Requirements	✓					✓
D3.1: Components for Trustworthy Disaggregated Computing Architecture	✓	·	✓	·	✓	
D4.1: Concept for Hardware Security Primitives and Heterogeneous Acceleration		✓	✓	✓		
D8.1: Impact master plan	·	·	·	·	·	✓
D9.1: Ethics requirements	✓		✓	✓		
Scientific Publications						
Dual Vector Load for Improved Pipelining in Vector Processors		✓				
Towards Modular Trusted Execution Environments	✓		✓			
Software-Defined CPU Modes			✓			
Disruptive TRX design for D-band					✓	

Table 1: Deliverables and publications in relation to project objectives

3 Work Performed in Year One

This section summarizes all work performed in year one towards the project objectives and deliverables. We group outcomes by work package, with Figure 4 giving an overview of the project until now. All work packages have started and ramped up over the course of the first year.

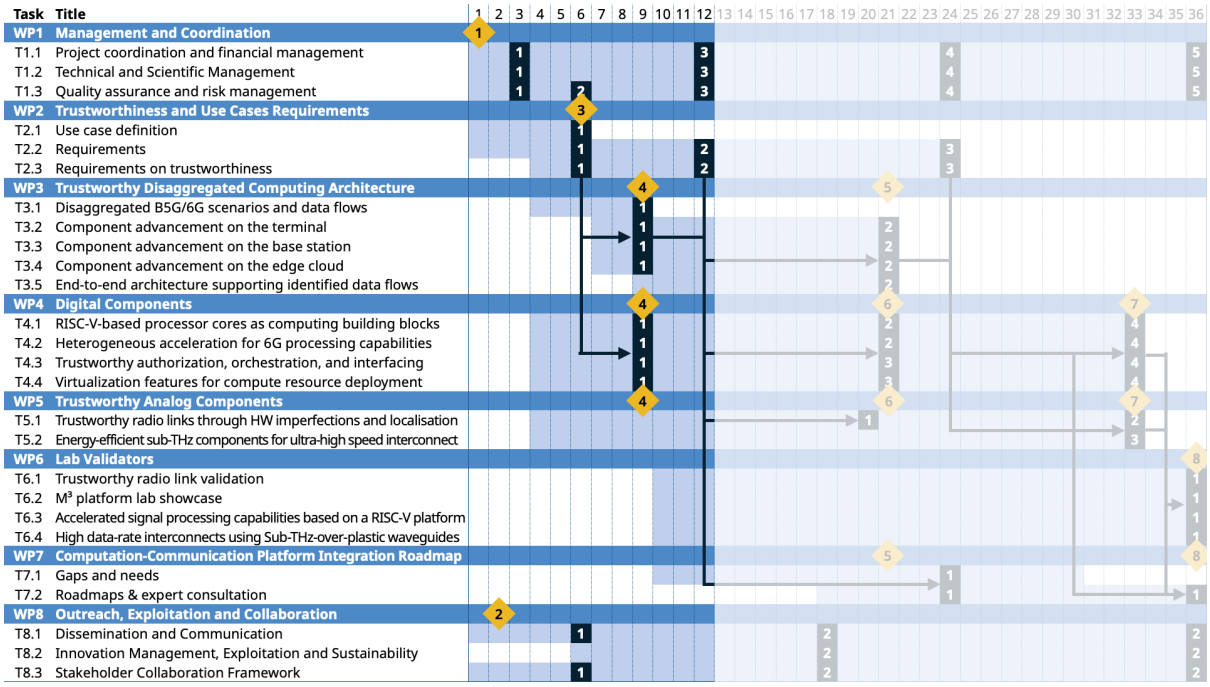
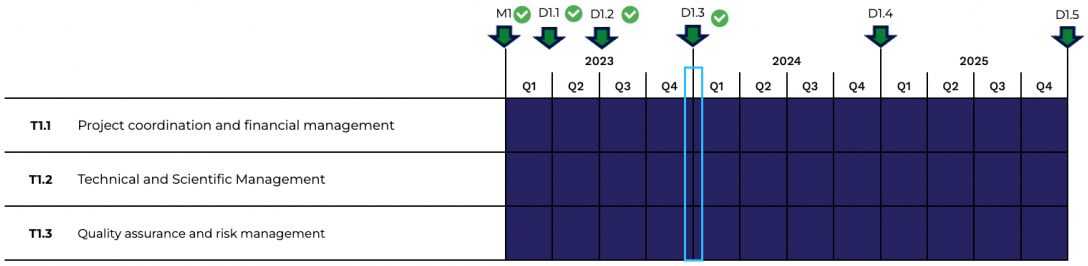


Figure 4: Project timeline

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 maintains efficient operation between project bodies and manages the reporting to the European Commission. Supported by the other work package leaders, the project is led by a core team consisting of:

- the **Project Coordinator** Michael Roitzsch from Barkhausen Institut,
- the **Technical Manager** Fredrik Tillman from Ericsson AB,
- the **Innovation Manager** Patrick Pype from NXP Semiconductors, and
- the **Data Manager** Panagiotis Demestichas from WINGS ICT Solutions.

Together, this team oversees all technical work and supervises the submission of project deliverables as well as financial and technical reports. A regular online meeting structure has been established to consult key issues between core team and work package leaders. Within the work packages, the work package leaders organize individual meeting schedules to consult with the respective partners. In addition, the project partners met twice in person during the first year:

- for the kick-off in January 2023 in Dresden and
- for technical discussions in July 2023 in Munich.

Achieved Outcomes

In the beginning of the first year, the project's administrative structures were set up in the form of shared storage and regular online meetings. As a reference for existing project members and to onboard new members, **Deliverable D1.1** was created as a project handbook. In month six, the data management plan was finalized in **Deliverable D1.2.**

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 one were achieved on time:

- Month 1: Kick-off meeting
- Month 2: Website & social media
- Month 6: Definition of use cases and initial requirements
- Month 9: Breakdown of requirements into component advancements

To solicit feedback from outside experts on the direction and progress of the project, the partners have agreed on an **Advisory Board,** to which we have presented the project state looking back at year one during a two-hour online meeting on October 9, 2023. The report of this meeting is part of this deliverable.

Risk Assessment

Several risks were foreseen in the project proposal, like underperforming partners or delayed milestones or deliverables. None of these have manifested. No changes to the consortium were necessary and restrictions due to COVID were no longer an issue since the start of the project.

A challenge is posed by the fact that the project partners so far have not signed a consortium agreement. Legal negotiations have been extremely demanding, which delayed this process extensively, but also shows the overall interest and weight that partners attribute to this project. So far, communication on a work level has not been negatively impacted by this as inter-partner collaborations are still forming. The agreement is now being signed, so we are confident to resolve the situation very soon and are looking forward to then make all deliverables marked for public dissemination available on the project website and on Zenodo.

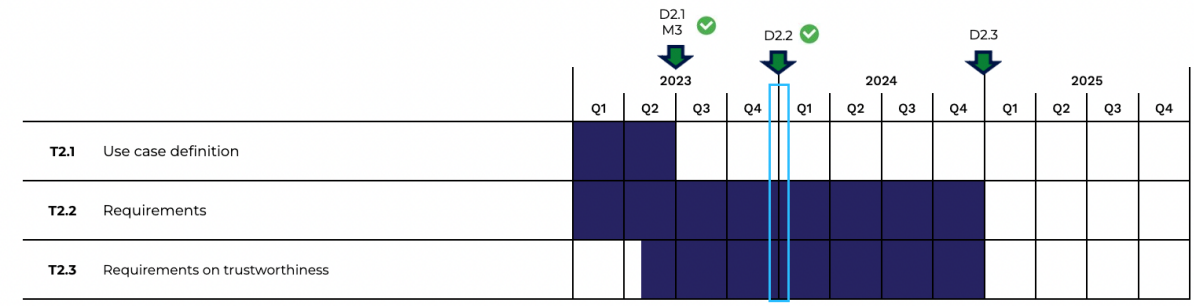
Deviations From Project Proposal

During the first year, the partner originally labelled 'Alcatel-Lucent International SA' (ALU) renamed itself to 'Nokia Network France' (NNF). We are using the new name in all project reporting.

The partner TIM enacted a cost-neutral change in person months by deducting 10PM from work package 2 and adding 6PM to work package 3 and 4PM to work package 6. This change was agreed

upon by all partners and allowed TIM to bring their network operator expertise also to the work on project architecture and lab validation.

3.2 WP2: Trustworthiness and Use Cases Requirements



In the first year, WP2 activity focused on the following work package objectives:

- Definition of meaningful use cases which will drive validations in WP6.
- Definition of the requirements which the project's technical components (in technical work packages) and lab validators will satisfy.
- Introduction of trustworthiness aspects for enabling the delivery of end-to-end-trusted services.

Framed in this context, WP2 progressed well in all three tasks defined for the work package, namely:

- Task 2.1: Use case definition
- Task 2.2: Requirements
- Task 2.3: Requirements on trustworthiness

WP2 achieved milestone 3, **Definition of use cases and initial requirements,** by month 6, and submitted **Deliverable 2.1: Use cases and requirements** in June 2023, as well as **Deliverable 2.2: Definition and impact of trustworthiness** in December 2023 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 to WP5 for feedback to digital and analogue enablers respectively.

WP2 holds bi-weekly 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 first COREnext White Paper

Achieved Outcomes

WP2 submitted Deliverable 2.1 in month 6 and Deliverable 2.2 in month 12. The first deliverable (D2.1) presented a comprehensive overview of the COREnext scope and a description of the case scenarios selected to show the goals of the project. The use cases outlined in this document showcase the potential of the proposed by trustworthy-by-design platform for signal processing and hardware acceleration addressing various industry verticals and societal challenges. The project focuses on leveraging a disaggregated computing architecture, where computing resources are distributed across different network locations, to enable efficient and flexible resource allocation, dynamic scaling, and improved network performance. By providing a comprehensive overview of the use case scenarios, this document served as a starting point to identify the main requirements for evaluating the project's components which will be developed in the technical work packages.

The second deliverable (D2.2) elaborated on the definition and description of the impact of trustworthiness in accordance with the various use cases proposed in D2.1. It defined the project's notion of trustworthiness by using the concept of a Trusted Computing Base and reducing the attack surface. Moreover, the deliverable elaborated on the description of attacker models regarding trustworthiness for the use cases we selected and showed how our architecture and enablers address these attacks.

Regarding **Task 2.1: Use case definition** we have focused on the definition and prioritization of the use cases. A set of use cases has already been identified to show how we can exploit the project's developed components. As a task outcome, detailed use cases which inform T2.2 and T2.3 were provided. These are taken also into account in the technical work packages for the components' development, testing, and validation (WP3–WP6).

With respect to **Task 2.2: Requirements** we have focused 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.

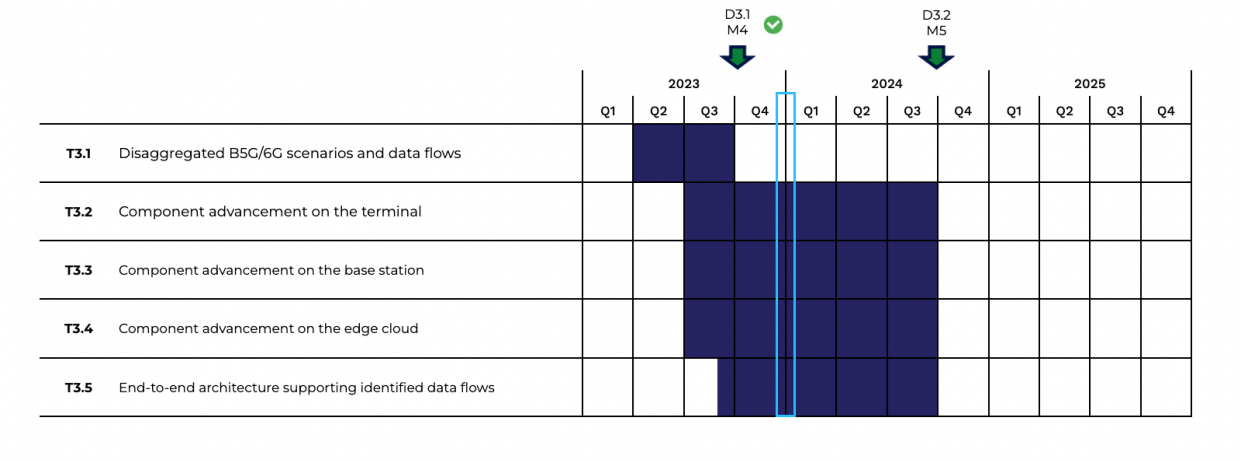
Finally, regarding **Task 2.3: Requirements on trustworthiness** we explicitly focus on trustworthiness aspects to enable service providers to combine equipment from different vendors and to enable hardware and system providers to deliver and integrate components of a system that provides trustworthiness for a society based on European values of privacy and data protection. After consulting with WP3 on the project architecture (D3.1), Deliverable D2.2 was produced to report an assessment of the trustworthiness aspects of this architecture and the resulting component developments.

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 since both aspects were

already analysed in D2.1 and D2.2. 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 first year, WP3 activity focused on the following work package objectives:

- Define disaggregation dimensions, data flows, and attacker models from requirements.
- Identify necessary component innovation to advance processing capability and trustworthiness.

The third objective (Analyse and balance the trade-off between trustworthiness and efficiency) was not addressed in year one as it requires further research on the innovations happening in WP4 and WP5. We also made good progress on all tasks defined for WP3:

- Task 3.1: Disaggregated B5G/6G scenarios and data flows
- 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

In year one, WP3 achieved milestone 2 in month 9 by submitting **D3.1: Components for trustworthy disaggregated computing architecture.** Apart from the specific WP3 contributions, this work package also contributed to the use case and requirements discussions in WP2 and provided input to the component advancements performed in WP4 and WP5.

WP3 has bi-weekly meetings where all partners actively participate to bring the discussions forward. During the first months, each partner presented their technical contribution to the project, which we used as a foundation to design the overall architecture for COREnext.

Achieved Outcomes

We submitted **Deliverable 3.1** in month 9, which takes the use cases and requirements from D2.1 and proposes an architecture with focus on trustworthiness that covers an end-to-end technology

stack from the device in the user's control up to edge cloud processing of user data. 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. Within the architecture, we identified multiple spots that require key innovations to combine trustworthiness with efficiency. For example, novel signal processing accelerators are required to achieve the desired energy efficiency, which at the same time need to be integrated securely into the hardware platform to achieve the desired trustworthiness. The architecture also considers the importance of existing standards like O-RAN and therefore describes its relation to COREnext.

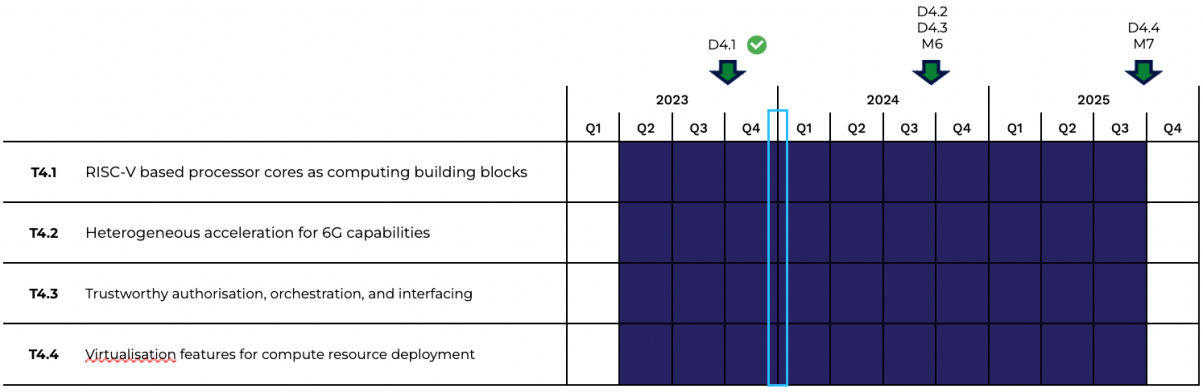
The disaggregated B5G/6G scenarios and data flows (**Task 3.1**) were obtained within WP2 and used as an input to WP3 and the first deliverable D3.1. The architecture presented in D3.1 and the key innovations within the architecture were selected to cover the identified scenarios and to deliver the required efficiency and trustworthiness.

Furthermore, the discussions and overall architecture set the foundation for the component advancements in the three considered device types: terminals (**Task 3.2**), base stations (**Task 3.3**), and edge clouds (**Task 3.4**). And vice versa, the specific requirements for these device types also drove the design of the architecture. For example, the COREnext hardware platform considers both energy-constrained terminal devices as well as the disaggregation as found and desired in base stations. The work on and end-to-end architecture supporting identified data flows (**Task 3.5**) has started with the first version of the architecture as part of D3.1 and will be continued in the following months.

Risk Assessment

None of the generic risks were identified for WP3, i.e., underperforming partners, partners leaving and restrictions due to COVID. 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. However, as we are quite early in the project, more research and advancements in other work packages is required to finally determine whether these risks manifest.

3.4 WP4: Digital Components



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

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

Within this context, 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

In year one, WP4 supported the achievement of milestone 4 in month 9 by contributing to D3.1: Components for trustworthy disaggregated computing architecture. In the same month WP4 successfully delivered **D4.1: Concept for hardware security primitives and heterogeneous acceleration,** where we derived the digital components to build the architecture and its component clusters outlined in D3.1. Additionally, this work package contributed to the use case and requirements discussions in WP2 and provided input to the component advancements performed in WP5.

WP4 has bi-weekly meetings where all partners actively participate to bring the discussions forward. During the first months, each partner presented their technical contribution to the project, which we used as a foundation to design the overall architecture for COREnext.

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

For **Task 4.1: RISC-V based processor cores as computing building blocks** we have explored the potential of the Snitch RISC-V cores as part of a Many-Core architecture for 5G/6G processing. From our analysis, we see the potential for ISA extensions to accelerate the FFT and the Beamforming (e.g. complex multiplication support, vector extensions for energy-efficient matrix multiplication). We plan to further extend the basic ISA supported by the Snitch on MemPool and TeraPool, introducing floating-point operations.

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. Furthermore, TUD has proposed dual load instructions as an optimization inspired by digital signal processors (DSP). The feature was analysed theoretically and practically, and it was determined that dual load is beneficial for compute-bound and some memory-bound programs. The highest possible speedup is 33 % and we demonstrated a speedup of 21 % in an implementation with about 2 % area overhead. The result was disseminated at a major conference on power-efficient chip designs. As a next research

focus, we have identified the vector register file (VRF) as a bottleneck in contemporary vector processors.

As part of **Task 4.2,** a refinement of the Kalray PE ISA (instruction set architecture) and its toolchain (compiler, assembler, linker, simulator, debugger) was started so it can meet the computational requirements of Layer 1 High-PHY processing of the O-RAN Distributed Unit (DU).

Also, as part of **Task 4.2,** progress has been made in choosing LDPC as the preferred FEC algorithm due to its evident benefits. Extensive research has been conducted on various code-rates for the LDPC encoder/decoder, analysing their performance across diverse bit error rates. Additionally, we've chosen a decoding algorithm and a parity matrix that align with our performance parameters. Subsequently, a preliminary version of the encoding and decoding process was implemented in MATLAB to thoroughly assess its error-correction capabilities.

Furthermore, in **Task 4.1 and 4.2,** we are delving into AI accelerators as an energy-efficient solution for MAC schedulers. 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.

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,** an architecture relying on virtualization and disaggregation was chosen for complying with project requirements as well as for aiming the highest efficiency possible (WPO 4.2, Tasks 3.4, 3.5, 4.2, 4.3, 4.4). Virtualization, if it is well managed, is also a way to reconcile trustworthiness and efficiency (WPO 3.3, Tasks 3.5, 4.3). Experimental and validations setups had to be planned throughout the year in the prospective of WP6 start and for the purpose of assessing the architecture. The experimental infrastructure will consist of a complete base station at commercial scale and featuring multiple architecture options thanks to virtualization. The other key purpose of such an infrastructure is to demonstrate that COREnext components and architecture could be reused for commercial networks.

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). To that end, BI has begun to develop an initial concept

and design for M³-based TEEs and published these initial ideas as a scientific publication on the international Workshop on System Software for Trusted Execution (SysTEX).

In **Task 4.3,** we have explored machine learning (ML) for radio hardware fingerprinting to establish trustworthy device identity to authorize any data exchange over a radio link task. We built a framework which performs ML training and validation on simulated radio frequency (RF) fingerprints data. The data is four different transmitter configurations, featuring four different power amplifier models based on measurements and/or post-layout simulations. We explored different ML architectures and observed very good classification accuracy for the provided dataset.

The result shows that we have a well-controlled framework, which can process the data and perform device identification with different types of ML architectures. The data, representing hardware impairments, has been generated by contributors from WP5 and continues to be produced, showing effective collaboration between different WPs. Current results prepare more detailed studies on ML architectures, as well as exploring different transmitter hardware impairments sources and its impact on the ML performance.

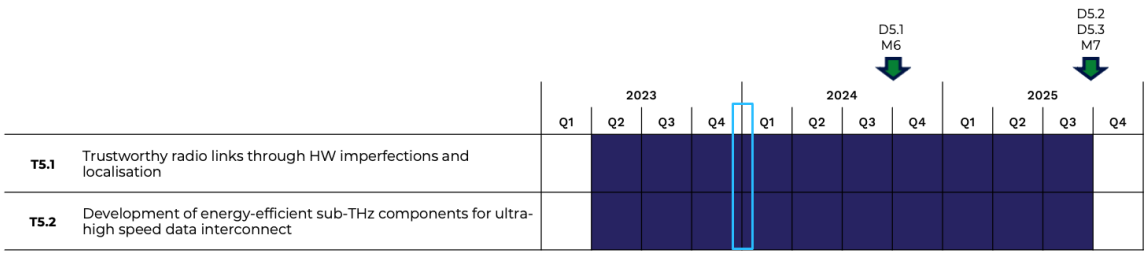
Risk Assessment

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.

Other potential risks to achieving WP goals are staff related. Our experts working on the different topics are crucial for achieving the technical goals and might be hard to replace if they decide to leave our institutions. Additionally, a potential problem for achieving the targeted goals is getting additional person power.

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 have taken place online. On July 4-5, a physical meeting took place in Munich.

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

- Fingerprinting: building models, ML-algorithms (cooperation with T4.3)
- Modelling and simulation of (sub-THz) wireless communication
- D-band RF transceiver characterization through the proper modelling and controlling the RF impairments
- Testbed for trustworthy communication and robustness
- Intelligent beamforming

Task 5.2 works in two tracks, targeting different frequency bands.

For the H-band track, the activities can be summarized as follows:

- The H-band track is working on circuit design. EAB and IFAT/IFAG are waiting for CHAL to measure the circuits and decide the circuit candidates. After that, IFAT/IFAG and EAB will do interconnect design.
- CHAL has done integrated transmitter and receiver (RXTX) design in both B11HFC and B12HFC SiGe BiCMOS technologies from Infineon. Infineon offers the B11HFC process in COREnext as a backup to B12HFC since B11HFC is a more mature process with well-established models.
- Characterization and relevant measurements on RXTX circuits including full ICs and break-out circuits like amplifiers, mixers, PAM-4 modulator, IF amplifier, frequency multipliers etc. are being carried out.
- Initial PMF link measurement based on B11 circuits in Y-band (170-260 GHz) is ongoing.

For the D-band track, the activities can be summarized as follows:

- Setting-up the D-band validation platform comprising a baseband-to-baseband testbed that can include a D-band TX and RX point-to-point link.
- Developing a 'digital twin' of the link including RF nonidealities modelling (carrier frequency offset, I/Q mismatch, non-linearities, phase-noise and spurs, channel-to-channel interferences, etc.)
- Currently, D-band TX and RX ICs are based on a multichannel architecture with a total RF bandwidth at D-band of 17 GHz (integrating 8x2.16 GHz baseband channels). This circuits allow to send up to 60 Gb/s data-rate using 16-QAM modulation. CEA is working in the next generation circuits with a total RF bandwidth at D-band of 34 GHz (integrating 16x2.16 GHz

baseband channels), that would be able to provide 120 Gb/s with 16-QAM and potentially 180 Gb/s with 64-QAM modulation.
- The footprint of the ICs has been shared with IMS Bordeaux and Radial to start the investigation and design of the IC to fibre couplers.

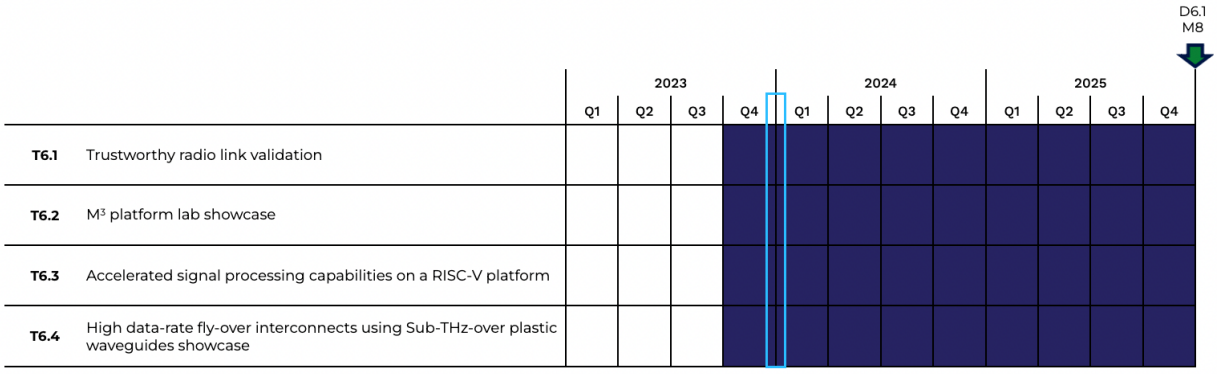
Risk Assessment

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



According to the project work plan WP6 started in M10 (October 2023). WP6 is closely connected to WP4 (Digital Components) and WP5 (Trustworthy Analog Components) and the WP6 leader (IFAG) is attending WP4 and WP5 meetings for alignment.

Specific tasks in WP6 are the development of four technology validators based on inputs from WP2, WP3, WP4 and WP5. In detail, these are:

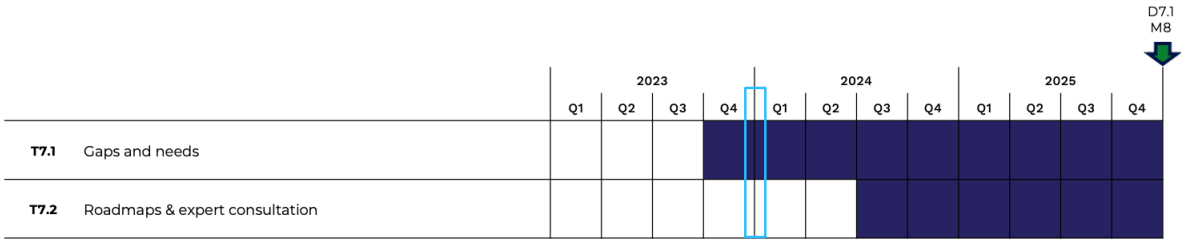
- Task 6.1: Trustworthy radio link validation,
- Task 6.2: M³ platform lab showcase,
- Task 6.3: Accelerated signal processing capabilities based on RISC-V platform (), and
- Task 6.4: High data-rate interconnects using Sub-THz-over-plastic waveguides showcase ().

In the WP6 Kick-off meeting on November 7, 2023, the main agenda topic was to discuss the relevant inputs for WP6 from other WPs. Overall, these include D4.1 (input for tasks 6.1 and 6.2), 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).

Risk Assessment

In the Kick-off meeting there was also a discussion about potential risks in terms of delays of WP6 relevant deliverables. In this regard it was concluded that the progress at WP and task level is constantly monitored. There is no indication yet for any delays.

3.7 WP7: Computation-Communication Platform Integration Roadmap



According to the project work plan WP7 started in October 2023. 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. A close interaction will take place with WP2 (baseline requirements for roadmap), WP3 (architecture proposals), WP6 (validation results) and WP8 (dissemination).

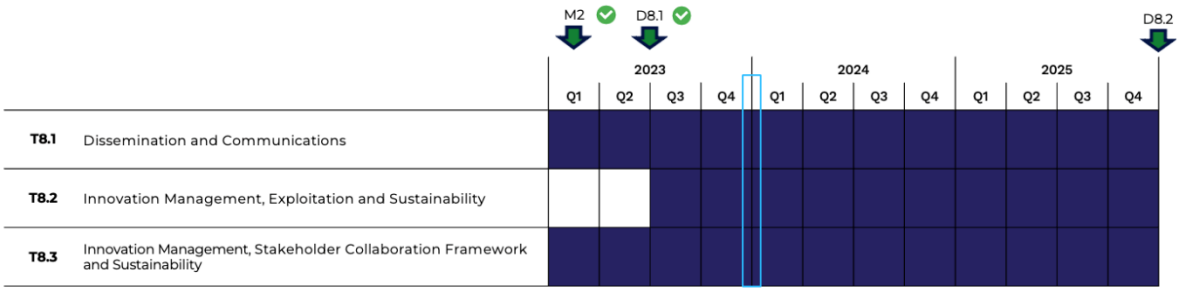
In October, several bilateral discussions took place with some of the key contributors to this WP. Main topics of discussions were how to collect the relevant information, and which stakeholders (internal & external) to involve. Partners from COREnext have also participated in an SNS-KDT workshop, organized by the European Commission on future priority topics in the field of interest of COREnext and beyond.

A formal kick-off meeting of WP7 is scheduled for December 5, 2023. The goal is to come to concrete actions and finalize planning on how to proceed, based on the first informal discussions. A table-of-contents for D7.1 will be defined to get a structure on how to collect future information via partners, via email, via existing reports, and via internal as well as external workshops and meetings.

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



During year one WP8 activity focused mainly on two of the four work package objectives:

- designing and executing dissemination and communications strategies to efficiently raise awareness about the project's outcomes, promoting the activities and results among a critical mass, and
- operating a collaboration framework that will identify and build synergies with a range of target groups.

However, even if the other two objectives of the WP were not actively addressed, 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 one, WP8 achieved **Milestone 2: Website & social media**, by month 2, and submitted **Deliverable 8.1: COREnext Impact Master Plan** in June 2023, complying with all reporting obligations related to the work package.

Apart from the specific WP8 contributions, this work-package contributed to WP2 by attending two-weekly meetings, and contributing to Deliverable 2.1 section 3, and Deliverable 2.2 section 6. WP8 also contributed to all other WPs with branding and design support.

WP8 holds monthly meetings, and all partners contribute 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 first Newsletter
- Sharing information about COREnext related events and publications they attended and produced to be used for C&D activity
- Contributing to stakeholders mapping and stakeholder management strategy
- Helping to identify relevant EU projects to liaise and collaborate with
- Contributing to initial discussions about a COREnext White Paper

Achieved Outcomes

WP8 submitted **Deliverable 8.1** in month 6. This deliverable served as a preliminary roadmap for COREnext communication, dissemination, and exploitation activities, and it also presented the work done in WP8 in the first six months of the project. Through the frameworks established by this deliverable, we will be able to assess the outreach footprint of the project through KPIs, develop an effective framework for IPR management, and contribute to relevant standardisation bodies and committees.

Regarding **Task 8.1: Communication and Dissemination outputs** we have established, among others, the project brand (e.g., logos, colour palette, etc) and brand guidelines; the press release; the website; the social media channels (Twitter/X and LinkedIn); project related campaigns (e.g. Women in Science); interviews; newsletters; awareness articles; the slide deck and pitch deck, and other promotional materials (e.g. one-page flyer). Additionally, we created several monitoring tools, including the one that helps us keep track of member's publications and event attendance. In the future we will expand on the above with, for example, training, and more technical publications.

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.

Some of the so far achieved figures towards WP8 KPIs are: website average unique visits per month views: 73 (KPI: 300); social media followers: 1067 (KPI: 2.5K); impressions on social media: 53K (KPI: 150K); peer-reviewed Scientific Publications in journals and conferences: 1/4 (KPI: 10/20); events attended: 5 (KPI 30) and non-scientific publications: 14 (KPI: 50). These are all above average results regarding the stage of the project.

In terms of **T8.2: Innovation Management, Exploitation and Sustainability,** the main purpose of the task is to design and execute the overall exploitation roadmap for COREnext, with

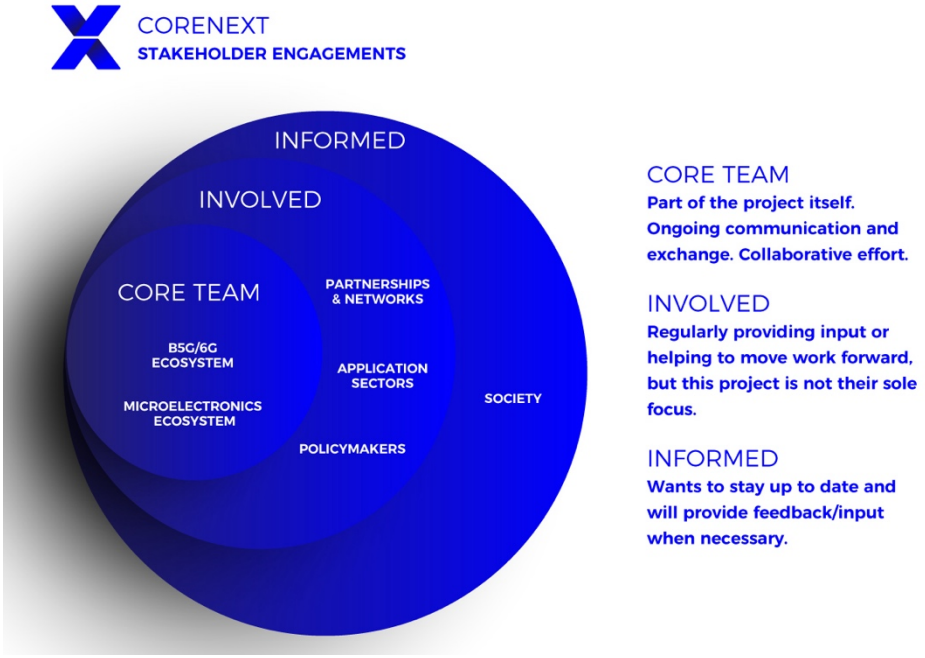
the ambition to foster the use, consolidate the uptake and seek the sustainability of the Key Exploitable Results (KERs) across the value chain. Since month 6, WP8 established the project KERs:

- KER #1: Trustworthy Disaggregated Computing Architecture,
- KER #2: Trustworthy Digital and Analogue Components in Base Station, Terminal, Edge Cloud,
- KER #3: Trustworthy IoT and Vertical Services and Applications.

And analysed the project exploitation strategy, market aspects and IPR management strategy.

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. The aim is to understand the ecosystem of actors which might be interested in the project findings, to develop a specific value proposition for each category. Following a stakeholder mapping exercise with all members, the figure below shows the proposed stakeholder engagement plan.



Assessment of partnerships and networks already started within this quarter, and we will expand on those in due reports.

Risk Assessment

None of the generic risks were identified for WP8, i.e., underperforming partners, partners leaving and restrictions due to COVID. However, we identified two risks 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.

Risk 2: lack of signed collaboration agreement (severity: medium). To mitigate this risk, we create C&D material that does not mention any of the partners but still presents the project in an effective manner.

4 Advisory Board Report

The COREnext project consulted with the project's Advisory Board in an online meeting on October 9, 2023, reviewing the past nine months of achieved project output. The Advisory Board was present in full, COREnext was represented by the core team and the respective deliverable editors. Specifically, the board consists of:

- **Prof. Gustavo Alonso**
  Professor of the Systems Group, ETH Zürich
- **Didier Belot**
  Wireless Strategic Innovation Head in Technology Design Platform Division, ST Microelectronics
- **Prof. Dr. Dirk Elias**
  Senior Vice President Corporate Research Advanced Digital, Robert Bosch GmbH
- **Heiner Grottendieck**
  German Federal Office for Information Security (BSI)
- **Nikos Kalogeropoulos**
  Hellenic Telecommunications and Post Commission (EETT)
- **Dr. Sara Wilford**
  Ethics expert, De Montfort University, Leicester, UK

The following subsections summarize the board's opinion on the presented deliverables and publications.

D2.1: Use Cases and Requirements

The board acknowledges that the project selected use cases with industrial relevance: extended reality, automotive infrastructure, intelligent management in smart city. These use cases cover a spectrum of interesting trustworthiness and architecture challenges. A suggestion was made to widen the scope to use cases of personal robotics and assistive devices, considering their unique privacy and reliability challenges.

The project was reminded to engage with stakeholders early in the development process to gauge their views on the selected use cases and their privacy and ethical challenges. Furthermore, the project needs to ensure, the selected use cases carry through to the validation work package by selecting meaningful performance indicators to evaluate.

D9.1: Ethics Requirements

The board acknowledges that COREnext has outlined the societal impact of its work, especially regarding privacy of personal data. The technical results of the project contribute meaningfully to ensure the European standards for privacy protection. In addition, the self-reflection and monitoring efforts are well-suited to the scope of the project. The project should make a continued effort to monitor and analyse its ethical impact and engage with relevant stakeholders.

D8.1: Impact Master Plan

The board considers the master plan to be ambitious and covering all relevant aspects of project outreach. The presented KPIs are valuable to gauge the project's dissemination impact. The current trajectory of these KPIs is very promising given the early state the project is in. Once the project has started to develop an industry roadmap, the dissemination activities should highlight this roadmap as a key outcome of COREnext.

D3.1: Trustworthy Disaggregated Computing Architecture

The discussed architecture bridges the gap between use cases and trustworthiness analysis which leads to a clear need for technical development beyond the state of the art. The presented architecture fits the application area of future 6G networks, and the board considers the identified research gaps to be relevant and their development to have high impact. It was suggested to conceptually look beyond the scope of 6G base stations and consider the applicability of the concept to the core network and cloud platforms. Furthermore, the project should ensure that validations are tied to this architecture proposal to show that the component needs have been satisfied.

D4.1: Hardware Security Primitives and Heterogeneous Acceleration

The component contributions are clearly scoped and are well-fitting building blocks for the presented architecture. The research projects are ambitious and relevant to extend the state of the art. Component development should be continuously monitored for their fit to the architecture and validations should be planned accordingly. The project should also consider the risk of research ideas failing by identifying which components are most critical for the success of the project.

WP5 Update: Analogue Components

Work package 5 had no deliverable in the reporting period, but a short overview was presented. The board acknowledges that work package 5 is ramping up in the topics of efficiency and trustworthiness, matching the project's goals and proposed architecture.

Summary

Overall, the board considers the trajectory of the project to match with the stated objective of improving trustworthiness in future 6G networks. The progress is in-line with expectations for a project that has been running for less than a year. The output of four scientific publications is a good achievement and the publications topically fit to the project's research goals.