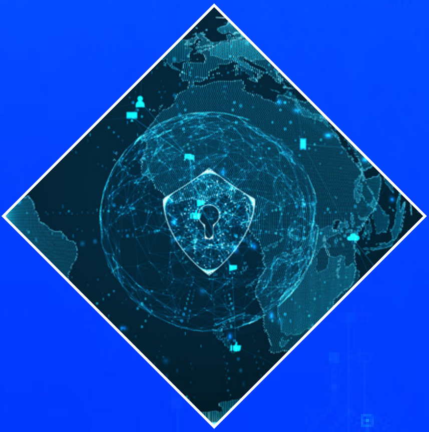
CORENEXT

TRUSTWORTHINESS

THE KEY TO EUROPE'S DIGITAL FUTURE



Funded by
the European Union

TABLE OF CONTENTS

SECTION 01

AN EXISTENTIAL MATTER FOR BOTH HUMANS AND MACHINES 4

SECTION 02

DIGITALIZATION – CHALLENGE OR OPPORTUNITY FOR EUROPE? 6

SECTION 03

ADDRESSING THE RIGHT THINGS 10

SECTION 04

ACTIONS FOR A TRUSTWORTHY FUTURE 18

1 Trustworthy Processing Cores

2 Scale-out Technologies for Disaggregation

3 Sensing and Future PHY

4 Trustworthy Future RAN

5 Call to Action

ACRONYMS & DEFINITIONS

AI	Artificial Intelligence
ASIP	Application-Specific Instruction Set Processor
B5G	Beyond 5G
BiCMOS	Bipolar CMOS
CIA	Confidentiality, Integrity, and Availability
CSP	Communications Service Provider
CRC	Cyclic Redundancy Check
DPU	Data Processing Unit
FEC	Forward Error Correction
FPGA	Field-Programmable Gate Array
Gbps	Gigabits per Second
GPU	Graphics Processing Unit
HPC	High Performance Computing
IOT	Internet of Things
ISA	Instruction Set Architecture
IT	Information Technology
LDPC	Low-Density Parity Check
M^3	Microkernel-based System for Heterogeneous Manycores
MANO	Management and Orchestration
ML	Machine Learning
MMIC	Monolithic Microwave Integrated Circuit
NIC	Network Interface Card
NSA	National Security Agency of the USA
O-RAN	Open Radio Access Network
PHY	Physical Layer Functions
PMF	Polymer Microwave Fibers
RAN	Radio Access Network
RF	Radio Frequency
RISC-V	5th RISC ISA from University of California, Berkeley
SiGe	Silicon-Germanium
SIP	System-in-Package
SmartNIC	Smart Network Interface Card
SOC	System-on-Chip
TEE	Trusted Execution Environment
VIM	Virtualised Infrastructure Manager

EDITORS

Arantxa **Echarte,** Australo
Fredrik **Tillman,** Ericsson
Michael **Roitzsch,** Barkhausen Institut
Werner **Haas,** Cyberus Technology
Zulaicha **Parastuty,** Infineon Technologies

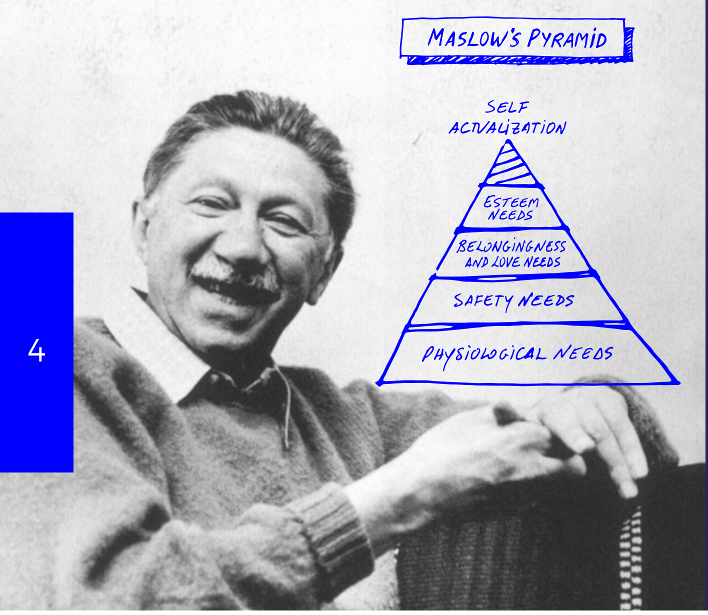
CONTRIBUTORS

Anastasia **Grebenyuk**, Ericsson
Andreas **Georgakopoulos,** WINGS ICT Solutions
Björn **Debaillie**, imec
Efstathios **Katranaras**, Sequans
Florent **Torres**, Ericsson
Frida **Strömbeck**, Chalmers University
Herbert **Zirath**, Chalmers University
Jonas **Lindstrand**, Ericsson
Julien **Lallet**, Nokia
Mamoun **Guenach**, imec
Marco **Bertuletti**, ETH Zurich
Markus **Ulbricht**, IHP
Mohand **Achouche**, Nokia
Renaud **Santoro**, Nokia
Romain **Beurdouche,** EURECOM
Ross **Staton**, Nokia
Singing **An**, Ericsson
Viktor **Razilov**, TU Dresden

SECTION 01

AN EXISTENTIAL MATTER FOR BOTH **HUMANS AND MACHINES**

Basic human needs have been studied in a social context for decades, and already back in the 1940s psychologist Abraham Maslow developed the famous 5-step ladder model.[1] The theory outlines a hierarchy of needs to be met in sequence to enable humans to reach self-fulfillment and achieve their full potential. In this pursuit, the needs gradually shift from being tangible deficiencies at the bottom, to more abstract and complex ones at the top.



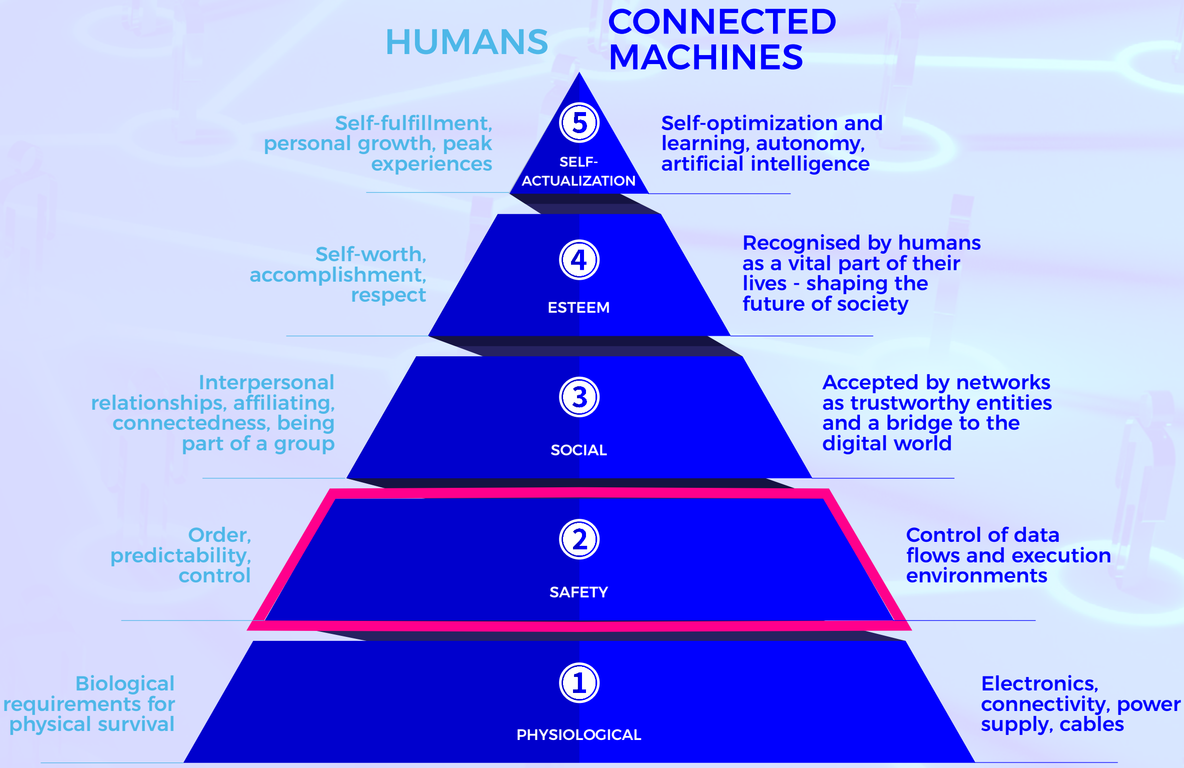
So, why should one care about this model?

The answer is simple – if any of the most important needs are unmet, it is impossible to progress and acquire higher-level aspirations.

Despite being a framework describing necessities for humans to thrive, it also represents a layer stack similar to what we find in present communication systems. At the very bottom, thus labeled fundamental, is the physical layer where the most basic needs must be functional. For humans it equals breathing, food, water, shelter, clothing, sleep etc. For communication networks it is represented by the hardware infrastructure such as electronics, wireless, cables, routers etc. - the foundation for processing and shipping bits. Climbing one level up in Maslow's model brings us to safety and security which is viewed as the second most rudimentary aspect of human survival. This is of course non-controversial and a reality for almost all living organisms on the planet. However, interestingly enough, the communication system analogy stays intact and is valid to an equal extent. Unless you can distinguish a friend from an aggressor, be part of a collaborating group with good intent, or show enough strength to withstand malicious attacks from the outside, your life expectancy is bound to be short. This is a reality shared by humans, distributed compute platforms and digital communication systems. Here the Maslow ladder model is depicted, including how a translation to the world of connected machines might look like for the upper layers. Despite the impossible nature of comparing humans and machines, it is fascinating to note the similarities and how connected machines possess incremental needs to be fulfilled in pursuit of a greater purpose. The COREnext project focuses on the second layer as highlighted in the figure. In light of increasingly connected societies, security and trust reside at the very heart of operations and must be guaranteed to add value on top. For humans, it means a journey towards self-actualisation according to Abraham Maslow – for digitalisation, a seamless merger of the physical and digital worlds in the application layer.

[1] A. Maslow, "A Theory of Human Motivation", Psychological Review, 50, 370-396, 1943. https://doi.org/10.1037/h0054346

MASLOW'S MODEL EXTENDED WITH CONNECTED MACHINES



HUMANS		CONNECTED MACHINES
Self-fulfillment, personal growth, peak experiences	5 SELF-ACTUALIZATION	Self-optimization and learning, autonomy, artificial intelligence
Self-worth, accomplishment, respect	4 ESTEEM	Recognised by humans as a vital part of their lives - shaping the future of society
Interpersonal relationships, affiliating, connectedness, being part of a group	3 SOCIAL	Accepted by networks as trustworthy entities and a bridge to the digital world
Order, predictability, control	2 SAFETY	Control of data flows and execution environments
Biological requirements for physical survival	1 PHYSIOLOGICAL	Electronics, connectivity, power supply, cables

This white paper elaborates on digitalisation from a trust and security perspective and illustrates how this societal evolution will impact Europe's current leading position in high-end consumer goods. It is clear today that the value content of products is redefined by adding connectivity and sensing capabilities to enter consumers' digital ecosystems. As outlined in section 2, this is a constant evolution that has not yet experienced major setbacks - from the early days of mobile broadband to where we stand today with the cloud surrounding us. However, this is likely to change unless more attention is paid to the pivotal question – to what extent will consumers feel secure in a digital world?

In COREnext, we believe that trust among the public can only be achieved if the system itself has native built-in security measures across all implementation layers and data flows, thus forming a trustworthy-by-design platform. Whether it guarantees safety when using self-driving cars, allowing your home to blend with the metaverse, or simply preserving privacy despite connected cameras everywhere – it does not matter. The system must earn consumer's trust. As a result, COREnext has launched a broad set of studies to capture the most promising techniques, which combined can define how such a platform may be realised and profoundly alter the trust equation – going from an end user responsibility paradigm to a trustworthy system paradigm. Some of these techniques are highlighted and elaborated on in section 3 by the active researchers.

Finally, section 4 suggests research at European level along four directions – processing cores, trustworthy radio access, distributed systems, and joint communication and sensing. These represent key technology areas which, if properly addressed, will catalyse Europe's ability to lead digitalisation while preserving the confidence and trust among users and regulators.

DIGITALIZATION
A CHALLENGE OR OPPORTUNITY FOR EUROPE?

Communication is a basic social need, thus indispensable in a digital world. To satisfy this need, one must secure the foundation underneath: the physical properties and safety, as seen in the figure in section 1. An example of how communication, and hence social needs, can be affected by security issues is how the early stages of the invasion of Ukraine spilled across borders.

Security agencies observed a range of cyber-attacks whose collateral damage had a major impact on countries far away from the war scene itself. To illustrate the consequences, a landmark incident was the attack on Viasat's KA-SAT modems. Viasat is a US company offering high-speed satellite broadband services to its customers around the world, including the Ukrainian government and military. While this could be seen as a legitimate military target, one side effect of the attack was that 5,800 Enercon wind turbines in Germany lost their remote monitoring and control capability. Consequently, the electric power generation equivalent to a handful nuclear power plants was switched to auto mode and thus out of control of power grid operators. The incident is notable for a few different aspects.

1

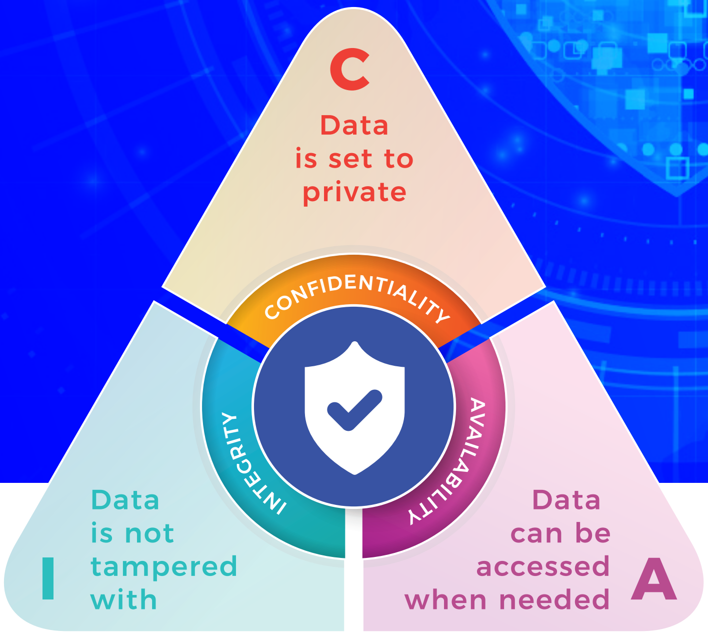
It highlights different meanings of trust and trustworthiness. As the satellite communication was attacked, the wind turbines became unreachable. This could have caused a severe problem, but thanks to the engineers designing the turbines, the system was trustworthy by embracing the concept of safety fallbacks – saving the day. In colloquial language a trusted system is one that we feel safe to use. In the field of security, however, a common definition of a trusted element is that its failure would break security policies whereas a trustworthy element simply would not fail.[2] In COREnext we believe it is necessary to investigate trustworthy components to build systems that can be trusted to fulfil integral roles in a digital future.

2

The meaning of security is expanding. Traditionally, the focus has been on confidentiality, that is on protecting data from unauthorised access. However, nowadays, to realise critical operations like autonomous driving, data exchange in the metaverse, and real time control of smart cities, three security components are strictly necessary: confidentiality, integrity, and availability (CIA). Cryptography as a prime mean for confidentiality will need to be complemented with other technologies to enable comprehensive communication security. A common trait among these is that they start at component-level and the following section will elaborate further on the actual technical details.

[2] Note that there is no universally accepted definition and alternatives differ in their point of emphasis

In COREnext we believe it is necessary to investigate trustworthy components to build systems that can be trusted to fulfil integral roles in a digital future.



3

The Viasat attack highlights the complexity of modern communication systems. The cyberattack itself started with hacking into a management centre providing network access to administrators and operators in Turin, Italy. From there, the attackers managed to access a server delivering software updates to Viasat's modems. By distributing malicious software (malware), the attackers took tens of thousands of modems offline. Although similar cyberattacks on IT infrastructure happen on a daily basis, in this case the targets were custom hardware devices as opposed to ordinary personal computers.

4

The aforementioned attack actually comprised two different vectors. Besides malware wiping out data on modems and thus rendering them inoperable, legitimate modems were abused to send carefully crafted control messages to confuse processing elements in the control plane of the network, which ultimately led to a disconnect of targeted devices. What makes this vector particularly insidious is that the attack originated from inside the network, i.e. from a trusted domain, thus bringing us back to the initial remarks about the importance of trustworthiness for system security.

So, once we become aware of the potential security issues and consequences of events such as the Viasat attack, what happens when the vehicle you are travelling in is being guided by data from an unknown source and cooperating with other vehicles to safely cross an intersection without the need for traffic lights? What is the trust level required to use robotic air taxis for transportation or to use shops and services in the metaverse whilst travelling and not being connected to your usual home network?

Our reflection on the Viasat attack shows that the existing IT solutions might not be fit to shoulder larger responsibilities stemming from continued digitalisation. A key reason lies in its construction as complex IT systems typically use standard off-the-shelf components. Commodity computer hardware on the other hand has always had security features added incrementally, thus putting enforcement of security policies predominantly in the hands of complex software.

To make matters worse, hardware itself follows the path of software and will not be an isolated monolithic building block. Technological progress has enabled complex System-on-Chip (SOC) designs and System-in-Package (SIP) devices, that integrate discrete components onto single chip or multiple chip modules. Unfortunately, this also means that we can no longer trust that all integrated sub-entities play by the rules. If we want to achieve trustworthiness at a macro level, we must start with a trustworthy architecture within the confines of a microchip.

So far, we have looked at the current situation and future trends mainly from a threat standpoint. We presented arguments for better security properties and highlighted challenges with current technology. However, before shifting attention towards the actual content of the COREnext project in the next section, we would like to elaborate on the economic aspects.

Security concerns about telecommunications equipment received public attention given the ban of Huawei and ZTE, huge Chinese market players, from 5G networks in western countries. The risk of having trusted, yet not trustworthy elements in critical infrastructure outweighed pure financial considerations. Different studies estimate the economic impact in the range of billions of Euros.

However, the situation is not as simple as East vs. West. The famous whistle-blower Edward Snowden leaked information about the NSA intercepting devices shipped to international customers of US companies like Cisco and implanting backdoor surveillance tools. So, the end user is in principle left with a vote of confidence, namely which camp to trust the most. This is an opportunity for Europe as a neutral player to take the lead and drive the development of devices requiring lower levels of trust to meet security objectives. While it is probably unrealistic to expect formal guarantees, see for example renowned security expert Ross Anderson's paper 'If it's Provably Secure, It Probably Isn't'.[3] COREnext aims at raising trustworthiness-by-design in digital systems to a new level.

This would also have effects beyond mobile communications, which is the origin and main focus of the project. Leadership in the telecommunication infrastructure has the potential of transcending into other markets and fuel new verticals, one example being connected homes. A recent survey[4] shows safety and privacy aspects are key to many people across the world when it comes to smart home technologies. At least one third of the respondents listed safety as especially important which requires a strong foundation in the CIA security pillars. The smart home market, for example, is projected at roughly 75 billion Euro in 2023 and expected to grow on average by more than 20% over the next decade, reaching more than 500 billion Euro by 2032.[5]

The trustworthy-by-design platform that COREnext proposes is a solution that would increase networks' resilience against attacks. By preventing threats, detecting and mitigating assaults, protecting data, establishing resilient communication channels, ensuring redundancy, and enabling rapid recovery, the platform architecture will help end users to stay safe. In COREnext we view the accelerating security challenge as a great opportunity for Europe to regain momentum in SOC and SIP technology development that has been lost over the last decades.

In COREnext we view the accelerating security challenge as a great opportunity for Europe to regain momentum in SOC and SIP technology development that has been lost over the last decades.

[3] Anderson, R. and Boucher, N. 'If it's Provably Secure, It Probably Isn't: Why Learning from Proof Failure is Hard' (2023). https://arxiv.org/abs/2305.04755

[4] See https://www.statista.com/forecasts/1227824/smart-home-security-safety-vs-privacy-concerns

[5] See https://www.precedenceresearch.com/smart-home-market

SECTION
03

ADDRESSING THE RIGHT THINGS

For anyone with ambition to lead in 6G, digital capabilities to ensure trustworthiness and security will be an absolute must. In this regard, COREnext has identified two distinct technology gaps that represent key opportunities for Europe to take the lead and to maintain its thriving communication technology ecosystem.

First, the breadth and depth of 6G applications impose challenging demands on mobile network hardware.
To process the expected signal workload, computations occurring on terminals, base stations, and in the mobile edge cloud must meet increasing performance goals in terms of throughput and latency. At the same time, this enormous compute capacity must be operated efficiently, requiring virtualisation mechanisms and disaggregation to improve resource utilisation. Network functions and services, formerly tied to specialised hardware, will be unbundled into dynamically managed software components. In addition, virtualisation and disaggregation are bound to increase operational flexibility by allowing migration of compute workloads to follow the demand for connectivity. For cloud hyperscalers and processor vendors, virtualisation and massive workload scaling are established technologies. However, their approach to 6G is based on off-the-shelf digital components, whose raw compute power is not purpose-built for RAN applications and thus cannot meet efficiency and sustainability targets mandated by regulations.

The second gap is the limited attention to trustworthiness.
Especially when hardware from multiple vendors is integrated in one system, current architectures require the trust of each supplier to trust the entire system. Given the expected deployment of multi-vendor hardware in critical and privacy sensitive infrastructure, trust validation of multiple component vendors is neither scalable nor acceptable. COREnext will change this trust equation by embedding hardware-based trust anchors within the architecture itself, enabling the integration of potentially adversarial software and hardware components into systems without the need to trust them. The project will address trustworthiness end-to-end, from the communication and sensing capabilities of the analogue radio interface to the digital processing.

The aforementioned gaps require both analogue and digital domain innovation and efficient interplay. COREnext has identified four key technology areas to be addressed:

1. Virtualisable accelerator hardware for 6G signal processing
2. Connectivity for disaggregated architectures
3. High-speed low-power chip-to-chip interconnect to support system integration
4. Trustworthy access and sensing enabled by radio hardware

COREnext MISSION #1

Develop efficient, scalable and virtualisable accelerators based on RISC-V extensions and FPGAs to drastically enhance European capabilities in hardware, computing, and signal processing technologies for B5G/6G infrastructures.

COREnext MISSION #2

Develop a trustworthy-by-design platform to secure European leadership in B5G/6G compute architectures. Enable efficient and trusted integration of third-party accelerators capable to support B5G/6G processes in cloud servers, radio base stations, and client-side devices.

Starting on the digital side, COREnext investigates trustworthiness of fundamental components, including compute platforms and accelerators. Each of these components must enable sufficient data protection and resilience to potential attackers and threats. Accelerators should always propel trusted and authenticated computing and avoid information leakage, no matter if they handle baseband processing, packet routing or AI decision making. Similarly, trustworthy computing platforms must guarantee isolation as they reside on top and manage accelerators and interconnects.

By embedding machine learning (ML) capabilities in such platforms, algorithms can be trained to identify and verify the authenticity of transmitting entities. ML techniques can, for instance, leverage unique imperfections and manufacturing discrepancies in the hardware. As a result, every transmitting device has unique signal characteristics - akin to a human fingerprint. These unique elements, which persist over time and cannot be easily altered or cloned, provide an additional layer of security in wireless networks by enabling detection of unauthorised or spoofing devices. Deep learning algorithms have demonstrated high stability and accuracy in such identification, making hardware detection an interesting technique for further exploration. By continuously learning from vast amounts of data, these models will in addition adapt to new threats over time. In the dynamic and evolving landscape of digital communications, the innovative use of ML in COREnext is bound to be an important step towards communication system security.

As for the innovation targeting digital components, it falls into two categories. The first one is about implementing power-efficient base band processing fitting the requirements of the COREnext architecture, including the use of RISC-V. The other one is about setting up a heterogeneous compute platform with trusted execution environments.

ISSUE 1

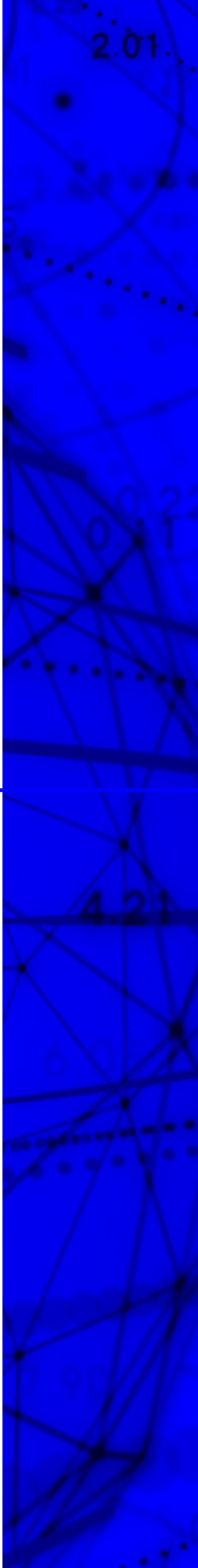
Challenging demands on mobile network hardware and enormous compute capacity must be operated efficiently

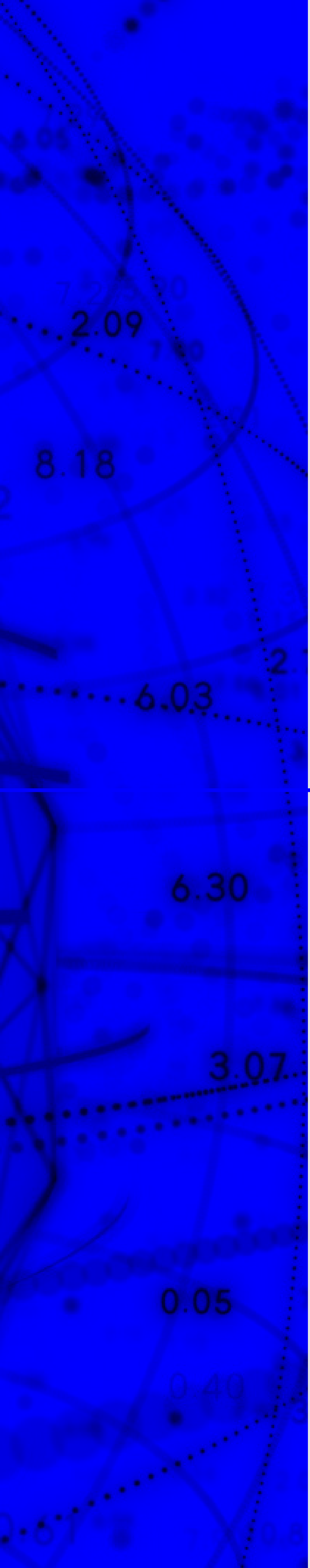
ISSUE 2

Limited attention to hardware trustworthiness

It is given that virtualisation leads to more centralised processing in the edge cloud, thus growing the importance of chip interconnect aspects. In COREnext we address this challenge by studying ultra-high speed data links over short distances. Conventional electrical and optical high-speed links struggle with functionality, economics, energy efficiency, and trustworthiness. Copper-based electrical links are bandwidth-limited due to skin losses, in addition to complex circuits for equalisation and coding. For short distance optical links (less than a few meters), the complexity and cost of electronic/optical conversion devices as well as chip-to-fiber assembly are challenging. In this context, radio transmission over polymer microwave fibers (PMF) is an interesting alternative as it represents a cost-effective solution with enhanced robustness. Thanks to the larger wavelengths, the fiber alignment is easier and more mechanically stable compared to optics. PMFs are also less sensitive to temperature changes, making the technology suitable for harsh environments such as autonomous vehicles.

To guarantee end-to-end security and trustworthiness in communication networks, analogue-based solutions that exploit the uniqueness of radio frequency (RF) hardware signatures are gaining more momentum. As previously mentioned, we target to limit the radio links vulnerability to impersonation attacks by developing fingerprint techniques using ML algorithms. In this type of attacks, a hacker device impersonates a legitimate device to gain unauthorised access to the network for malicious intents such as degrading network performances, denying access to legitimate users, identity fraud, or extracting sensitive information.





COREnext TECHNOLOGICAL ADVANCEMENTS

Power efficient baseband processing

Many-Core accelerators

Vector processing accelerator

Forward error correction (FEC) accelerator

MAC scheduling accelerator

High-speed interconnect ambitions

Advanced SiGe BiCMOS semiconductor technology (600 GHz fmax) and monolithic microwave integrated circuits (MMICs)

Stable and cost-efficient ways to connect chip and fiber

Antenna-in-package solutions

Radio fingerprinting

Analog/RF device hardware and RF fingerprinting

Heterogeneous computing

Field-programmable gate array (FPGA) multi-tenancy

A microkernel-based system for heterogeneous multicores

IoT management

For this purpose, we explore the RF hardware fingerprint concept as a first line of defense to identify radio transmitters based on their unique hardware signatures – thus difficult to replicate by an attacker. From a network security perspective, it is an additional security mechanism complementing existing methods at the physical layer.

In the long-term perspective beyond the first phase of 6G, sub-THz wireless communication systems must ultimately be studied. Finding methods to mitigate attacks and eavesdropping will be essential. In COREnext we envisage that accurate modelling and control of RF hardware impairments enable advanced beamforming as a complement to RF fingerprinting concepts. This will enhance both the physical layer performance and security aspects. This also allows fast counter-attack measures to relax the need for security protocols suffering from high latency. In this context, it is important to detect security threats using hardware-based identification (such as RF fingerprinting) and localisation/sensing techniques to actively jam eavesdroppers, thus preventing decoding of malicious data.

The merit of early physical layer counter-attack measures is tightly linked to transceiver architectures and RF hardware impairments. As a result, the underlying semiconductor technology options must be studied carefully. Proper characterisation and control of hardware impairments will turn them into a companion – not an unwanted artifact.

COREnext STUDIES ON POWER EFFICIENT BASEBAND PROCESSING

MANY-CORE ACCELERATOR

COREnext will develop a many-core accelerator for parallel processing of data streams at the PHY layer of B5G and 6G systems, that is the lowest layer in a network stack. The accelerator architecture consists of a cluster with 100s of processing elements tightly coupled to a shared low-latency and high-bandwidth memory. Each processing elements support the open RISC-V instruction set architecture (ISA), in addition to the domain specific extensions. This allows the use of standard languages and tools for fully programmable signal processing acceleration.

VECTOR PROCESSING ACCELERATOR

Fixed-function accelerators provide excellent efficiency but have limited functionality and modifications options. Furthermore, custom chip-development and production are not feasible for every application. It is therefore desirable to study and develop efficient programmable accelerators that lie between general-purpose processors and fixed-function accelerators on the performance-flexibility trade-off curve.

FORWARD ERROR CORRECTION (FEC) ACCELERATOR

The PHY handles transport block segmentation, cyclic redundancy check (CRC) generation, FEC via e. g. low-density parity check (LDPC), rate matching, scrambling, modulation, and many more tasks. In COREnext, the acceleration of CRC and FEC will be tested in particular.

MAC SCHEDULING ACCELERATOR

COREnext will investigate this research area in detail to find a suitable accelerator implementation that can be tightly coupled to a RISC-V processor via an ISA extension.

ARTIFICIAL INTELLIGENCE (AI) INFERENCE FOR RADIO LINK AUTHENTICATION:

COREnext plans to explore the use of ML techniques for RF fingerprinting.

CORENext STUDIES ON HIGH-SPEED INTERCONNECT

To facilitate the disaggregated and distributed data processing expected in next generation mobile communications, highly efficient rack-scale links for up to a few meters distance are required. COREnext aims at providing transfer rates beyond 100 Gbps over a single lane using Polymer Microwave Fibers (PMF), that is cheap plastic, as transmission medium. With less than 1 pJ/bit energy consumption, the technology is orders of magnitude more energy efficient than conventional electrical cables. It is on par with optical links yet promises more cost-efficient assembly and usage of well-established SiGe BiCMOS semiconductor technology. COREnext will also address manufacturing-related aspects such as integration of monolithic microwave integrated circuits (MMICs) with antennas and other passive microwave components in a single chip package. The trustworthiness of the interconnect must also be addressed, primarily to mitigate eavesdropping. Attackers could, for example, manipulate the fiber or exchange components in order to sniff data traffic.

CORENext STUDIES ON RADIO FINGERPRINTING

The focus is to analyse physical properties of analogue/ RF device hardware to understand the underlying mechanisms of RF fingerprinting and define hardware non-idealities that should be tracked/acquired. In the design and manufacturing of radio hardware, all non-idealities are within a specification, however, the distribution/spread of these non-idealities makes each radio hardware unique and this is the key mechanism to exploit. We are also developing RF fingerprint-based concepts and methods to increase the trustworthiness of radio links by establishing trustworthy device authentication. These concepts could also help verifying the authenticity of embedded hardware elements in infrastructure equipment. This would limit the vulnerability to hardware enabled backdoors.

CORENext STUDIES ON HETEROGENOUS COMPUTING

FIELD-PROGRAMMABLE GATE ARRAY (FPGA) MULTI-TENANCY

Cloud providers offer data processing in FPGAs. Currently available commercial solutions suffer from a lack of security and integrity for both the data processed and the intellectual property of the algorithm. COREnext is researching a deployment framework comprising HW and SW components in order to fill this gap. By signing and encrypting all data exchange between the parties involved we provide data and IP privacy and thus enable the use of Cloud FPGAs.

ACCELERATOR VIRTUALISATION

In contrast to typical Cloud deployments, the mobile communication use case features a computing infrastructure that is not only virtualised but also distributed. Thus, it is needed to ensure that the management of the infrastructure is compatible with the use of heterogeneous acceleration. Experiments will help to find potential limitations of state-of-the-art distributed infrastructure management. This will allow subsequent design of improvements and features to fully enable virtualisation and distribution in the COREnext architecture.

A MICROKERNEL-BASED SYSTEM FOR HETEROGENEOUS MULTICORES

Solutions to integrate TEEs on accelerators with TEEs on processors are currently tied to the concrete combination of TEE technologies. With M³, a major development goal within COREnext is to offer a general solution for TEE interaction, independent of the concrete accelerators, strengthening the position of M³ as an integrative system-level solution for trustworthiness.

IOT MANAGEMENT[6]

With IoT devices becoming increasingly integrated into critical systems and exposed to sensitive data, their trustworthiness has a direct impact on user safety, data security, and overall system integrity. In COREnext various management mechanisms are investigated to ensure security and trustworthiness of IoT devices.

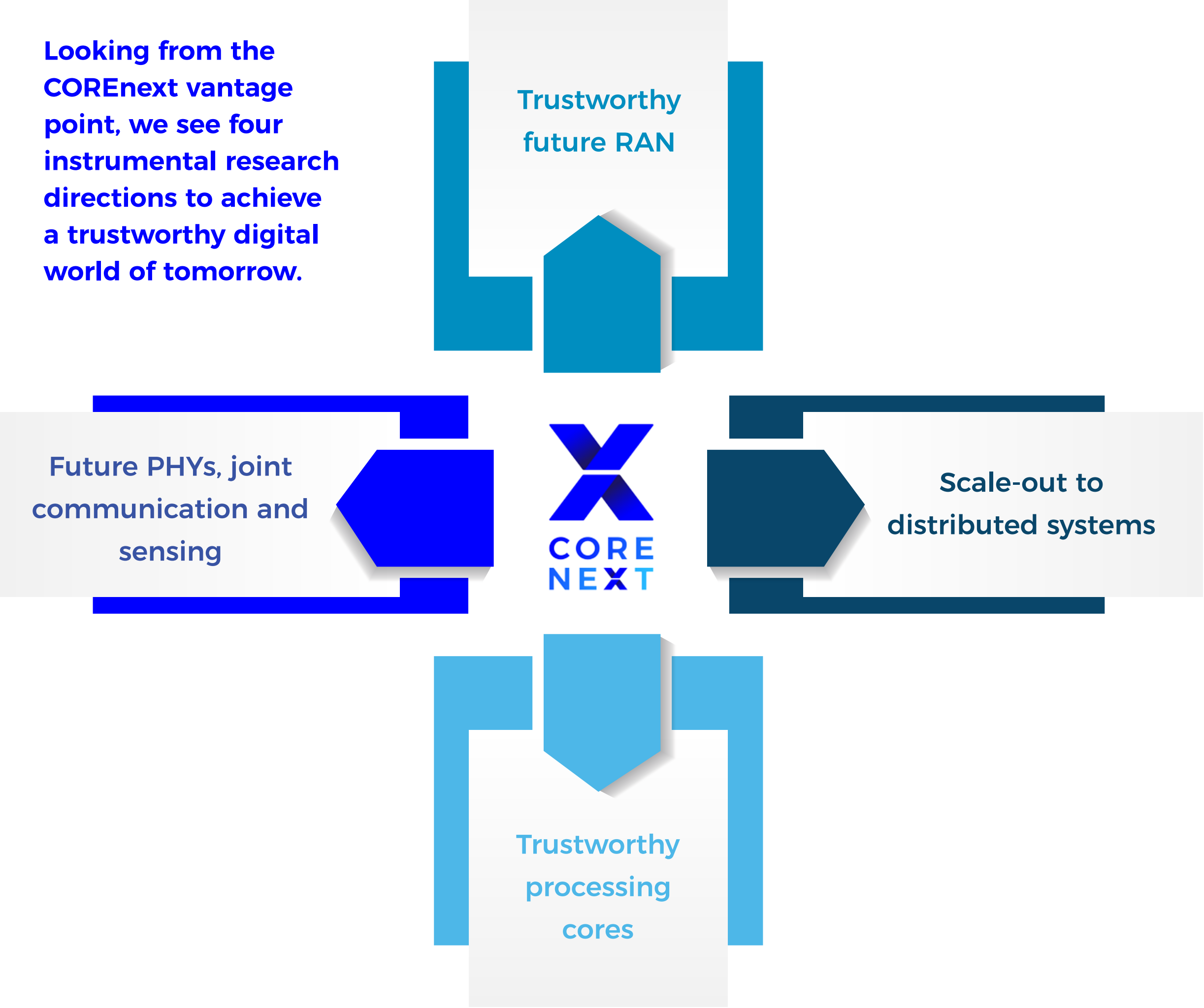
[6] See https://sequans.com/addressing-security-in-cellular-iot-modems-lp/

ACTIONS FOR A TRUSTWORTHY FUTURE

The fifth and final level in Maslow's hierarchy of needs is self-actualisation, which for connected machines equals autonomy, learning, self-optimisation etc. In the light of this pursuit, the European Union has funded numerous research projects over the years and involved both the private and public sectors to shape a European digitalisation agenda.

One example is the COREnect project (2020–2022) that gathered knowledge of experts and solidified it into distinct research missions – one being trustworthiness of communication infrastructure currently addressed by COREnext (2023-2026). But what are the missing pieces? What topics do we already identify now as key for Europe to address towards 6G and beyond?

Looking from the COREnext vantage point, we see four instrumental research directions to achieve a trustworthy digital world of tomorrow.


Trustworthy future RAN
Future PHYs, joint communication and sensing
CORE NEXT
Scale-out to distributed systems
Trustworthy processing cores

1 TRUSTWORTHY PROCESSING CORES

In a world defined by software, controlling the foundation on which all computation rests is critical. When software is running on a digital platform, every computation is ultimately performed by a silicon manifestation of a processor design. No matter what security mechanisms are implemented in the upper layers of the technology stack, the processor itself is the final arbiter to either bolster or compromise system security. In COREnext, we develop Trusted Execution Environments (TEEs) as a mechanism to strengthen code execution against outside influence. But we still have to rely on the individual processor cores to correctly execute the code we intend it to execute. Two trends show this to be a shaky assumption: growing processor complexity and supply-chain attacks.

Because the scaling of silicon chips is reaching its physical limits, the primary way to make general-purpose processor designs faster is to enlarge their designs, for example with wider instruction issue, more specialised functional units, and more sophisticated execution speculation. These innovations however all increase the overall processor complexity. With increased complexity comes a higher risk for unintended interactions between parts of the processor, leading to security compromises.

We have seen exactly this tragedy play out with the Spectre and Meltdown vulnerabilities in 2018, where from one day to the next millions of deployed processors became exploitable due to a design error being discovered. In addition to such unintended errors, actors with malicious intent can insert backdoors into processors during design, manufacturing, or packaging.

However, we are not powerless to these problems. Openness and an architectural rethinking are part of our arsenal. RISC-V is an emerging processor technology and a strategic asset in the development of fully European processing capabilities. Its open-source nature allows European platforms to break free from the captivity of proprietary designs. The resulting transparency reduces the chance of hidden mechanisms that can threaten security. Beyond RISC-V, Europe should develop processor technologies that address fundamental security flaws of contemporary processor architectures. CHERI is an example of such a redesign. Re-envisioning the role of processors without the burden of backwards compatibility can strengthen overall security.

2 SCALE-OUT TECHNOLOGIES FOR DISAGGREGATION

In the age of AI and other large-scale computational workloads, a single processor alone is no longer sufficient. We need ways to join the forces of many distributed processors and purpose-built accelerators. Resource disaggregation is an architecture, where physically separate computing resources are combined dynamically over fast interconnects to meet the needs of applications. Such an architecture requires high-throughput chip-to-chip communication that is also energy-efficient.

Very efficient multi-100-Gbps datalinks can be realised utilising Polymer Microwave Fibers (PMF) as a transmission media over distances up to a couple of meters. During COREnext, initial ultra-wideband transmit and receive hardware will be designed and evaluated.

While it shows a lot of promise in reaching new energy-per-bit efficiency levels, the technology still has challenges to overcome. Further research should be performed on waveform generation, chip-level integration of PMF transceivers, and eavesdropping on the PMF link. Impurities in the fibers can be detected or even actively implanted to ensure link authenticity.

Such high-speed interconnects are a key ingredient to novel base station processing paradigms. With emerging use cases like augmented or extended reality, the network edge will see a significant increase in computation demand. Efficiently combining a diverse set of processors and accelerators requires new interconnect concepts like PMF.

3 SENSING AND FUTURE PHY

The radio interface is a key part of any mobile communication network. Here, we see two needs for innovation: increasing the energy efficiency and enabling new sensing applications in a trustworthy way. The physical layer (PHY) hardware is involved in both aspects. On the transmit path, this piece of hardware forms the last signal processing step before the radio waves are emitted via an antenna. On the receive path it is the opposite: the physical layer hardware is the first to transform the signal. Currently, this hardware part operates in the same basic manner independent of network utilisation. However, this is not ideal from the standpoint of saving energy. The energy-optimal method of signal processing is different for a lightly loaded radio cell compared to a heavily loaded one. Thus, future PHYs should be made adaptive to significantly cut down the energy usage of networks while continuing to increase data rates. A densification of the network grid in populated areas will allow for more bandwidth beyond mm-Wave frequencies, but also require power and cost efficient PHYs.

Joint communication and sensing is a new functionality expected to be added to networks. It allows the radio system to be used to sense the environment in a radar-like fashion and simultaneously transmit communication signals. While further research is also needed to realise this idea on the functional level, another important area to consider is privacy. Base stations and mobile phones being able to continuously sense their physical surroundings enables a new quality of pervasive surveillance. Enabling the desired use cases while protecting citizens' privacy must happen deeply within the radio infrastructure, not as an afterthought placed at software-level.

Finally, we must not forget that the radio interface itself is the most exposed interface in the network. Security in its design is therefore paramount. COREnext is researching novel AI-assisted ways of determining device authenticity by way of radio fingerprinting. This is one example of new security measures that must be employed to protect our infrastructure right at the signal ingress point. Physical-layer security is therefore another key research area when developing future PHYs.

4 TRUSTWORTHY FUTURE RAN

Processing, disaggregation, physical layer – the Radio Access Network (RAN) is the management layer on top of all these building blocks. The RAN assigns resources to workloads, distributes tasks and makes use of accelerators like GPUs and FPGAs. To fulfil this diverse task securely, the RAN itself needs to be constructed with trustworthiness in mind.

Nowadays, cloud compute infrastructure is mostly dominated by non-European vendors. To maintain our high standards of privacy and information security, we must develop a European counterpart.

Modern clouds run on programmable network infrastructure like smart network interface cards (SmartNICs) or data processing units (DPUs), which organise communication between hardware components and thus establish the fundamental security primitives of the platform. We believe, European research should target these network infrastructure components. Europe should not be reduced to a provider of individual puzzle pieces but must be able to apply its own technology to determine what the final picture looks like.

5 CALL TO ACTION

Trustworthiness as a goal has a marketing problem: other than flashy new features, measures to improve trustworthiness are invisible. Just like our basic human needs in Maslow's pyramid, they fade to the background when they are satisfied. This is a problem, because both the foundations of our human society and the foundations of our digital infrastructure need constant care and attention, otherwise they become corrupted. Thus, we need to make sure trustworthiness becomes a desired and requested item.

In fact, trustworthiness should be so deeply engrained into system design that users can take it for granted. But to get there, much more work on fundamental trustworthiness of digital infrastructure is needed. We believe, European ingenuity is already being applied to many relevant pieces for a trustworthy communication infrastructure. We have outlined our thoughts for four research directions, which, taken together, can form a cohesive whole. Let's act now and move forward to build the trustworthy network of the future.

ACTION #1

Trustworthy Processing Cores
All digital code execution uses processors. They are the foundation all other trustworthiness mechanisms build upon. Openness and architectural rethinking are needed to make processors themselves trustworthy.

ACTION #2

Scale-out Technologies for Disaggregation
Disaggregation physically separates resources, which is a key tool for trustworthy system integration of accelerators. However, high-speed and low-latency interconnects are needed to render such systems efficient.

ACTION #3

Sensing and Future PHY
Joint communication and sensing enables exciting new use cases, but also opens new privacy risks. A trustworthy architecture should fundamentally protect user privacy within the radio infrastructure - not as an afterthought placed at software-level.

ACTION #4

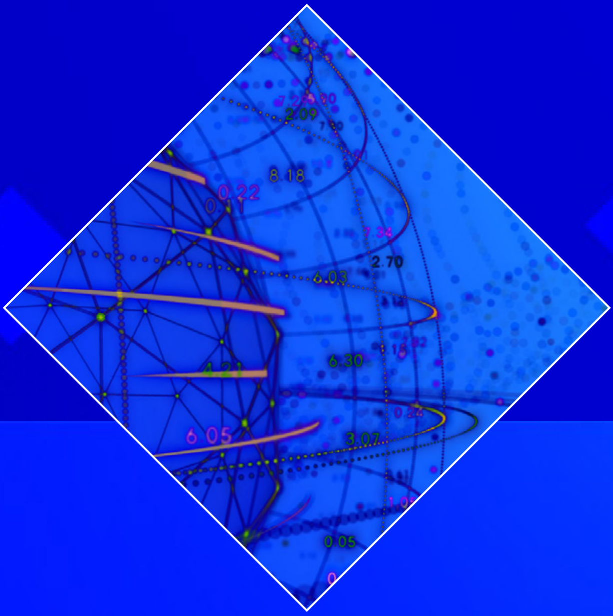
Trustworthy Future RAN
Cloud compute infrastructure consists of a programmable network infrastructure to organise communication and a software layer managing workloads and resources. Europe should develop its own technology stack to improve digital sovereignty.

FOLLOW

CORENEXT

WWW.CORENEXT.EU

INFO@CORENEXT.EU



DISCLAIMER

The information, documentation and figures available in this publication 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.

This document does not reflect the opinion of any single COREnext partner or any of the organizations with which the experts are affiliated. The COREnext project and its consortium partners are not liable for any consequence stemming from the reuse of this publication.

Funded by
the European Union