# RF Hardware Reconfigurability for Privacy-Preserving Integrated Sensing and Communication

Padmanava Sen, Prajnamaya Dass, Stefan Köpsell, Gerhard P. Fettweis

Barkhausen Institut, Dresden, Germany
{padmanava.sen|prajnamaya.dass|stefan.koepsell|gerhard.fettweis}@barkhauseninstitut.org

***Abstract*—This paper introduces a reconfigurable radio frequency (RF) front-end based management of accuracy and other sensing key performance indicators (KPIs) as means for privacy control in the context of integrated sensing and communications (ISAC). Being part of the sensing devices (especially user equipments), the reconfigurable front-end would enable the users to control dynamically the sensing KPIs of their devices. This would allow the enablement of sensing-based applications while maintaining privacy and ensuring that the sensing application only receives the minimal amount of necessary sensing data. In this work, the use of RF front-end reconfigurability is highlighted for different types of systems and an architecture to integrate the controls in privacy-preserving User Equipments (UEs) is proposed. The active KPI management with RF front-end controls can be a key factor for the deployment of joint/integrated communication and sensing systems without causing a privacy nightmare in future sixth generation (6G) networks.**

***Index Terms*—Integrated sensing and communications (ISAC), RF Hardware, radar, reconfigurable, 6G, privacy, accuracy, KPI**

## I. Introduction

In recent years, the interest and research activity in integrating communication and radio sensing systems [1] have grown multi-fold along with activities to include them in future sixth generation (6G) ecosystem [2]. Thereby, radar is considered to be one of providers of the envisioned sensing capabilities. The dual functional systems [3] may hold the key to the realization of ubiquitous radar sensing and thus enabling Radar-as-a-service (RaaS). To achieve that, Radio Frequency (RF) and physical layers for new and existing waveforms need to be co-designed and co-optimized to actively support both radar and communication services. At the same time, the system design would require an adaptive framework to enable early deployment of first generation devices with Integrated Sensing and Communication (ISAC) capabilities.

There is currently no specification for a common architecture regarding ISAC for 6G systems. Nevertheless, several (research) projects have created early architectural proposals [4]. Fig. 1 shows a consolidated and simplified overview of the proposed architectures. For this paper, one important aspect is, that the sensing devices do not only cover the currently existing base stations, e.g. Next generation Node B (gNB) but extend to the end devices i.e. User Equipment (UE). Another important aspect is, that the sensing capabilities and the processing of the sensing data are initially under full control of the Mobile Network Operator (MNO).

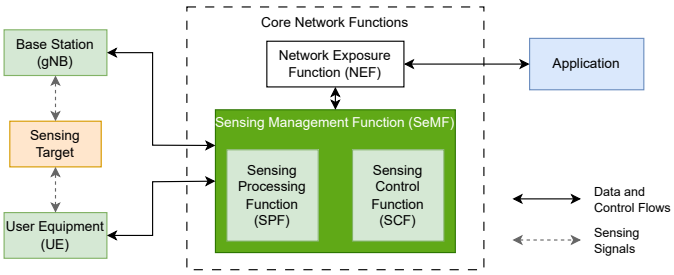


Fig. 1. Simplified architecture for integration of ISAC into 6G systems.

While integrating sensing capabilities into the 6G system will allow many new use cases [5], it also induces many challenges for data protection and privacy [6]. It was demonstrated, that radar sensing allows to derive multiple Personally Identifiable Information (PII) from human beings if they are the sensing targets [6]–[9]. This implies that data protection regulations like the European General Data Protection Regulation (GDPR) need to be considered. To align with the regulations, the overall sensing infrastructure and especially the sensing devices need to be designed in a way that gives control to the users (if the sensing devices are the UEs), reduces privacy risks, and supports privacy-respecting sensing in general.

In this paper, we concentrate on hardware-based active sensing Key Performance Indicator (KPI) management to control privacy. More specifically, we introduce a flexible hardware design that can be reconfigured based on the application needs and the required level of privacy. As a prior work, the authors have investigated thoroughly the reconfigurable architectures that can be used to tune the KPIs of ISAC receivers [10] and transceivers [11]. In the literature, research has been done to use hardware reconfigurability for cognitive sensor networks [12]. Also, software reconfigurable radar has been reported [13]. However, this paper introduces hardware and software reconfigurable active sensing KPI management for

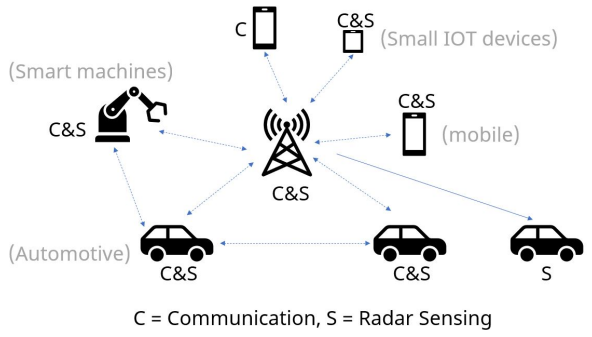


Fig. 2. Different applications in future 6G networks (IOT = internet-of-things).

the first time towards privacy-preserving ISAC, to the best of authors' knowledge.

In section II, different scenarios are considered leading to the categorization of the systems . Section III will highlight the use of hardware controllability towards privacy enhancement. Section IV and section V will delve into the privacy control mechanisms in user equipment and gNB respectively, using reconfigurable front-ends. Section VI will conclude this paper.

## II. Different Scenarios

The future networks will not only include mobile phones and base stations [5] rather several different applications with different requirements need to be integrated as shown in Fig. 2. Some devices will have both radar and communication capabilities, some only communication, and some only radar. The communication and sensing capabilities will also vary across the devices as needed. Some of these capabilities will be added as a must-have requirement e.g. communication capabilities in automotive systems to enable efficient interface management between automotive radars. Some of these capabilities will also require hardware reuse considering compact, energy and cost-efficient implementation. However, any front-end changes will add two to three years of development for newly designed systems. If these systems encounter privacy challenges during deployment, it will add another two years, thus hindering the 6G enablement/deployment. This necessitates a desperate need to rethink the capabilities of existing hardware and how they can be utilized with a fail-safe upgrade for a privacy-preserving ISAC. The higher layers e.g. digital part of Physical Layer (PHY) or Media Access Control (MAC) would also play an important role in this enablement but the control architecture for these layers is different than the analog front-ends. Being the first block receiving the information, front-ends can play a significant role in controlling the PII as well. However, the reconfigurable front-end needs to be considered in four different types of systems, broadly categorized below based on hardware reuse and data sharing:

- **Type A** - with hardware reuse for ISAC and with data sharing between systems
- **Type B** - with hardware reuse for ISAC but without data sharing between communication and radar systems
- **Type C** - no hardware reuse, i.e., separate hardware for communication and radar sensing but with data sharing between systems
- **Type D** - no hardware reuse for communication and radar sensing as well as no data sharing between systems

Type A and B systems can be considered as co-designed with different levels of integration. Type C and D systems will fall under category of co-operative and isolated systems respectively. There are instances where communication and radar systems cannot be used together due to the differences in frequency bands used, standard compliance as well as hardware KPI differences leading to performance trade-offs /sub-optimization [11], [14], [15]. However, such systems may still fall into Type C category, being controlled by the same software but working in cooperation. In terms of applications, privacy aspects of both UE and gNB based sensing are considered in later sections of this paper.

## III. Hardware Controllability towards Privacy

In this section, the use of controllability in RF hardware will be described with implications in privacy controls and the balancing act to achieve a privacy-preserving ISAC system.

### A. Hardware Controllability

Traditional communication systems are built to work under different transmission and receiver power scenarios. These capabilities are present in fifth generation (5G) [16] and are expected to be present in future systems as well. Thus, they are equipped with gain and other control measures to work under different channel conditions. Similarly, recent radars have power, linearity as well as bandwidth [17] controllability measures. There are several signal processing, front-end and antenna parameters that play a role in the overall radar performances. Among them, the usable bandwidth, transmit power, receiver gain and receiver linearity play a significant role in the detection and range resolution [18]. To analyze the implications on Type A, B, C and D systems, these four parameters will be primarily considered towards active range resolution and detection management.

A multi-purpose/reconfigurable RF front-end [11] is shown in Fig. 3 that can be key to hardware reuse and active radar KPI management. This representation includes solutions where antennas are shared or reused between transmitter and receiver. There are also possibilities of using separate receivers for communication and radar when both of these operations need to function at the same time, not covered in this representation. This front-end will consist of different reconfigurable/multi-mode blocks, for example, low noise amplifier (LNA), power amplifier (PA), analog to digital converter (ADC), digital to analog converter (DAC), mixers (frequency converters) while meeting the diverse needs of communication and radars. It will also support analog and digital radar processing needs as required by the different modes by embedding switches in the down conversion [11].

The transmission gain and power controls are partially or fully demonstrated in most communication [19] and radar

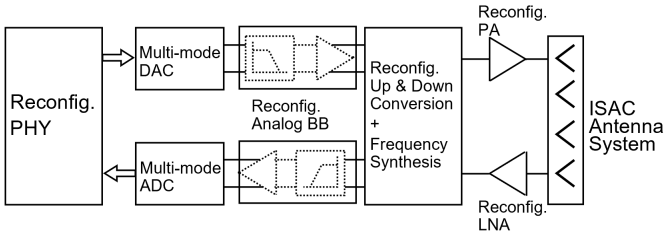


Fig. 3. A multi-purpose/reconfigurable RF front-end (PA = power amplifier, LNA = low noise amplifier, DAC = digital to analog converter, ADC = analog to digital converter, BB = baseband, Reconfig. = Reconfigurable) [11].

transmitters [20]. The gain controls [10] in receivers are already part of cellular systems today. The gain and linearity controllable receiver for ISAC is also demonstrated in [21]. The bandwidth of a receiver can be controlled either in the physical layer with a digital filter or an analog filter in the baseband. Such analog filters can also be designed with gain controls [22], [23]. The use of these controls for an ISAC system is summarized below considering the categories mentioned in section II:

- **Type A**: If we consider the RF hardware reuse architecture of Fig. 3, several control measures are available to tune the radar receiver and transmitter blocks considering the accessibility to communication chain controls. The underlying assumption is the use of traditional communication waveform, e.g. Orthogonal Frequency Division Multiplexing (OFDM) for radar processing. Even if separate signal processing methodology is used for radar in a combined front-end, different RF blocks can be shared with controllability features. However, the accuracy management controls need to be separated from the rest of the controls. Also, the sharing of power amplifiers [11] for communication and radar can be a challenge, limiting the reuse of transmission controls.
- **Type B**: Even though both Type A and B systems reuse the hardware for communication and sensing, separation of the data processing provides better privacy measures in Type B systems. However, these systems cannot use a common or reconfigurable PHY, shown in Fig. 3. Using same front-end also limits the scope of isolation and hence, additional measures need to be taken in both analog and digital domains to avoid information leakage.
- **Type C**: For such systems without RF hardware reuse, the controls for radar KPI management will be limited but some communication receiver controls can be replicated in radar transceivers with additional power consumption. The isolation of sensitive PII is easier than Type A systems for the isolation of hardware where the communication receiver has no access to the data received by the radar receiver. However, if the two separate systems have antennas nearby for cooperation at higher levels, the isolation will not be full-proof.
- **Type D**: The benefits and shortcomings of Type C will exist in Type D systems with added layers of privacy for not sharing radar data with communication systems.

The reconfigurability in the communication chain would add privacy features in a passive sensing [24] scenario as well. Apart from the software-based control, a hardware switch to completely turn off active sensing capability, gives an added layer of privacy control, described in detail in section IV.

### *B. How accuracy plays a role in privacy?*

The KPIs for ISAC systems are essential for optimizing system performance while ensuring the system can effectively provide both high-quality communication and accurate sensing. Better values for KPIs, such as range accuracy, Angle of Arrival (AoA) and Time of Arrival (ToA) accuracy, velocity accuracy, resolution, localization, and target identification accuracy, are beneficial for sensing tasks such as detecting, tracking, or identifying objects [25], [26]. However, the higher the accuracy of these sensing KPIs, the more detailed and precise the information that can be deduced about objects in the sensing area, leading to various privacy issues [27]. Moreover, as sensing accuracy improves, the risk of exposing PII, such as location and movement patterns, increases significantly. For instance, as specified in Table I (3GPP use case KPIs [5]), the positioning accuracy needed for hand gesture recognition is not as stringent as that required for human or UAV detection. However, when the same hardware is used for both use cases, the sensing data collected for human detection can also capture additional details, such as human gestures and movements. In ISAC use cases for health and sleep monitoring, the biometric data can reveal even more sensitive personal details. The privacy risks raise concerns around linkability, identifiability, and observability threats.

Although the KPIs used for communication are primarily focused on evaluating the accuracy and quality of data transmission in ISAC systems, they can inadvertently expose privacy-sensitive information related to sensing targets. Communication KPIs like low Bit Error Rate (BER), high throughput, low latency, and high Signal-to-Noise Ratio (SNR) can reveal detailed information about sensing targets [28]. These KPIs enable precise and detailed data transmission, allowing high-resolution sensing data, such as environmental maps, movement patterns, or biometric information to be communicated without degradation. Real-time transmission and large-scale data collection increase the risk of surveillance, tracking, or profiling, raising privacy concerns if the sensing data is not properly anonymized or secured.

### *C. Is there a middle ground? — privacy KPIs versus Hardware KPIs*

To address privacy concerns in ISAC systems, certain accuracy KPIs such as range, localization, and target identification can be traded off by hardware design to protect user privacy, while still maintaining system functionality. For instance, by controlling the accuracy of hardware KPIs for human object detection use case in Table I, the sensitive human movement and gestures could be protected. By mapping ISAC KPIs to privacy KPIs such as data minimization, location privacy,

TABLE I
KPI REQUIREMENTS FOR SOME OF THE ISAC USE CASES IN 3GPP [5]

| Sensing service area | Accuracy of positioning estimate by sensing | | Accuracy of velocity estimate by sensing | | Sensing resolution | | Max sensing service latency [ms] | Refresh rate [s] | Missed detection [%] | False alarm [%] |
|---|---|---|---|---|---|---|---|---|---|---|
| | Horizontal [m] | Vertical [m] | Horizontal [m/s] | Vertical [m/s] | Range resolution [m] | Velocity resolution [m/s x m/s] | | | | |
| Object to be detected: Human (indoor), UAV (outdoor) | 10 | 10 | N/A | N/A | 10 (NOTE 1) | 5 (NOTE 2) | 1000 | 1 | 5 | 2 |
| Object to be detected: Vehicle in ADAS | SRR: 2.6 LRR:1.3 | 0.5 | 0.12 | N/A | 0.4 | 0.6 | SRR: 20 LRR:50 | SRR:0.05 LRR:0.2 | 10 | 1 |
| Indoor human motion-sleep monitoring (NOTE 3), sports monitoring (NOTE 4) | N/A | N/A | N/A | N/A | N/A | N/A | 60000 | 60 | 5 | 5 |
| Hand gesture recognition | 0.2 | 0.2 | 0.1 | 0.1 | 0.375 | 0.3 | 5 to 50 | 0.1 | 5 | 5 |
| SRR: short-range radar; LRR: long-range radar; NOTE 1: To detect the Unmanned Aerial Vehicle (UAV) existence (e.g., for intrusion detection), the sensing resolution of distance is 10m; NOTE 2: To detect the UAV existence, the sensing resolution of velocity is 10m/s; NOTE 3: Additional KPI on human motion rate accuracy of 2 times/min (0.033 Hz); NOTE 4: Additional KPI on human motion rate accuracy of 3 times/min (0.05Hz) and 4 times/min (0.07 Hz). | | | | | | | | | | |

and anonymization, with dynamic hardware design principles, network operators and device manufacturers can implement privacy-preserving controls like obfuscation, consent mechanisms, and data encryption to mitigate the risk of privacy violations.

In addition to these considerations, antenna gain and multi-antenna configurations enhance both communication throughput and sensing accuracy, while low noise amplifiers and advanced signal processing improve SNR, essential for clear detection and reliable data transmission. Bandwidth selection determines resolution and data rates, balancing sensing precision with communication demands. The bandwidth tuning as mentioned in subsection IIIA can also limit sensing KPI - range resolution. Synchronization accuracy between different hardware components is vital for coherent data fusion and time-sensitive operations, especially in real-time applications like autonomous vehicles or smart environments. Thus, optimizing these hardware factors is key to achieving a robust and privacy-conscious ISAC system that can meet the dual demands of communication and sensing.

## IV. RECONFIGURABLE FRONT-END AS PRIVACY CONTROL IN USER EQUIPMENT

In this section, we will sketch how the reconfigurable front-end can be utilized as one privacy control in an overall privacy architecture for UE. There are at least the following two approaches, which should be combined:

A) A hardware switch to turn on/off the sensing capabilities.
B) Software-based control, allowing for adjustment of the sensing capabilities/KPIs according to the needs of the use case and the privacy policy of the user.

Note that in both cases the status of the sensing capabilities should be signaled to the user in a trustworthy way.

### A. Hardware switch for controlling the sensing capabilities

The idea of a hardware switch is comparable to similar existing approaches for other sensors like camera (slidable camera covers) or microphone (hardware based on/off switches). Note that in the case of radar sensing, we need the reconfigurable front-end because simply disconnecting e.g. the antenna, would also prevent communication.

Obviously one needs to trust the device (UE) manufacturer to correctly wire the hardware switch to the reconfigurable front-end so that the switch is indeed effective. To a certain extent, this implies less control by the user e.g. compared to a camera slider. Nevertheless, even in the case of the camera slider, the user needs to trust the manufacturer that it has not embedded hidden sensors in the device. Note that the reconfigurable front-end can be separated from the baseband processor allowing at least for some verification of correctly implemented hardware controls by external experts e.g. from regulatory bodies.

Although a hardware switch can be seen as excellent privacy control, given it can completely disable the sensing capabilities, it will not support fine-grained access control concerning sensing data. Therefore, it will fall short of supporting applications which require certain sensing capabilities/KPIs.

### B. Software-based control of the sensing capabilities

In order to mitigate the shortcomings mentioned above we propose to introduce hardware/software components which allow more fine-grained control of the front-end. This would

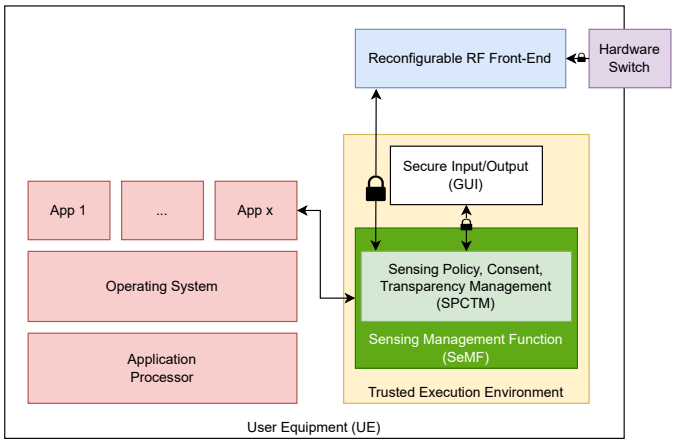


Fig. 4. UE architecture for utilizing software/hardware controlled reconfigurable front-end for privacy control.

enable to support applications which require sensing data while respecting the privacy policy of the user.

The overall architecture is depicted in Fig. 4. It is an extension/refinement of the architecture presented in [6]. The access to the sensing data is governed by the Sensing Policy, Consent, and Transparency Management (SPCTM). To enable a trustworthy, software-based control of the front-end, we would need several requirements:

- We need *Trusted Execution Environments (TEEs)* which provides means for strong separation with respect to the execution of software components. Here, for example, strong separation refers to the fact, that the software running inside the trusted execution environment cannot be manipulated by other software components running on the device including the operating system. TEEs can be realized e.g. with the help of separate processing units/chips, hardware-based separation concepts like the ones proposed by the $M^3$ architecture [29] or through TEEs provided by existing hardware (designs) like ARM TrustZone or Apples Secure Enclave Processor.
- We need a *trusted output component* which can signal the current status of the front-end, i.e. the sensing capabilities without being influenced by potentially malicious software components (including the operating system). This output component can be as simple as a multicolour LED signalling the sensing status by different colours or a hardware/software component which allows to display of information on the screen without being affected by malicious software components running on the device. This can be realised, for example, using secure Graphic User Interface (GUI) concepts presented in [30].
- We need a *trusted input component*, which allows the user to configure their privacy policy with respect to the sensing. This input component can be a (simple) hardware device or or more sophisticated component e.g. based on the secure GUI concept mentioned above.
- We need *trusted/trustworthy paths* between the involved components. This can be achieved by dedicated cabling (among hardware components) or local attestation (among software components).

The architecture depicted in Fig. 4 will enable the user to configure their privacy policy regarding sensing for local applications as well as the case where the UE acts as a sensing device being part of the 6G system. Overall this is very similar to the currently existing rights management systems e.g. with respect to access control regarding the camera, microphone or geographic location.

Note that the policies configured by the user will not only cover the allowed sensing KPIs, e.g. with which frequency and which resolution the sensing might happen. It could also cover dynamic aspects, e.g. that the allowed sensing KPIs are time or location-dependent. For example, this could be used to express that sensing is allowed outside (in the public) but not inside the home/property of the user; or that sensing is allowed during the daytime but not at night etc.

Once the policy is set by the user, the related app will receive a credential (a cryptographic token) from SPCTM. The app needs to use this credential while requesting sensing information to prove that the user has been granted the corresponding rights to access the sensing data with the requested KPIs. While the sensing is going on, SPCTM signals this using the trusted output. Moreover, SPCTM allows to display of additional transparency information (e.g. which application accesses which sensing information for which purposes etc.).

## V. Reconfigurable Front-End for gNB-based Sensing

Although our focus in this paper is on UE-based sensing, we briefly want to discuss the usage of reconfigurable front-ends as privacy and security control in the case of gNB-based sensing.

Regarding the following considerations, we assume a certain level of trustworthiness with respect to the MNO, since a malicious MNO could roll out an independent sensing infrastructure which is solely under its control. This is comparable to the trust we need to have concerning the device manufacturer in the case of UE-based sensing. Nevertheless, we need to assume, that e.g. state-level attackers can manipulate (parts of) the 6G system e.g. with the help of supply-chain-based attacks or by attacking the deployed system.

The deployment of reconfigurable front-ends accompanied by means of establishing a trustworthy path to access them, e.g. using remote attestation would allow the MNO or external third parties (e.g. regulatory bodies such as data protection authorities) to verify that the actual sensing capabilities are in line with the expected configuration based on the desired privacy policies.

Thinking of more extreme cases (e.g. war-like situations) it could allow the disablement of the sensing capabilities irreversible ("kill-switch") while maintaining the communication capabilities. The first would hinder the enemy from misusing the sensing capabilities, while the latter allows to preserve means to inform the public or to enable emergency calls.

## VI. Conclusion

In this paper, we introduced the concept of reconfigurable front-end usage to influence the sensing KPIs while maintaining the communication capabilities. Such reconfigurable front-end with hardware switch and software based controls can be used towards privacy control as part of an overall security and privacy architecture for joint/integrated communication and sensing in 6G systems. It is especially a useful building block which gives trustworthy control with respect to privacy to the UE users. Here, we especially need to deal with situations, where the UE and its software components might be subverted by the attacker.

Given the highly sensitive nature of radar sensing data, it is of utmost importance that the necessary privacy controls are embedded into the overall system before its mass deployment starts. As a future work, particular front-end controls and their impact on overall system performance will be further investigated along with the requirements in higher layers to enable such privacy switches/controls in the RF domain.

## Acknowledgment

This work is financed on the basis of the budget passed by the Saxon State Parliament. The authors would like to acknowledge the contribution of Tim Hentschel to this work.

## References

[1] C. De Lima, D. Belot, R. Berkvens, A. Bourdoux, D. Dardari, M. Guillaud, M. Isomursu, E.-S. Lohan, Y. Miao, A. N. Barreto, M. R. K. Aziz, J. Saloranta, T. Sanguanpuak, H. Sarieddeen, G. Seco-Granados, J. Suutala, T. Svensson, M. Valkama, B. Van Liempd, and H. Wymeersch, "Convergent communication, sensing and localization in 6G systems: An overview of technologies, opportunities and challenges," *IEEE Access*, vol. 9, pp. 26902–26925, 2021.

[2] ITU-R, "Framework and overall objectives of the future development of IMT for 2030 and beyond," Recommendation ITU-R M.2160-0, ITU-R, Nov. 2023.

[3] F. Liu, C. Masouros, A. P. Petropulu, H. Griffiths, and L. Hanzo, "Joint radar and communication design: Applications, state-of-the-art, and the road ahead," *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3834–3862, 2020.

[4] Hexa-X-II project, "Deliverable D3.3 Initial analysis of architectural enablers and framework." https://hexa-x-ii.eu/wp-content/uploads/2024/04/Hexa-X-II_D3.3_v1.0.pdf, Apr. 2024.

[5] 3GPP, "Feasibility Study on Integrated Sensing and Communication (Release 19)," Tech. Rep. TR 22.837 V19.4.0, 3GPP, 2024.

[6] P. Dass, S. Ujjwal, J. Novotny, Y. Zolotavkin, Z. Laaroussi, and S. Köpsell, "Addressing Privacy Concerns in Joint Communication and Sensing for 6G Networks: Challenges and Prospects," in *Privacy Technologies and Policy*, pp. 87–111, Springer Nature Switzerland, 2024.

[7] A.-K. Seifert, A. M. Zoubir, and M. G. Amin, "Detection of gait asymmetry using indoor doppler radar," in *2019 IEEE Radar Conference (RadarConf)*, pp. 1–6, IEEE, 2019.

[8] S. Ivashov, V. Razevig, A. Sheyko, and I. Vasilyev, "Detection of human breathing and heartbeat by remote radar," in *Progress in Electromagnetic Research Symposium*, vol. 2004, 2004.

[9] Z. Wang, K. Saho, H. Tomiyama, and L. Meng, "Gender classification of elderly people using doppler radar images based on machine learning," in *2019 International Conference on Advanced Mechatronic Systems (ICAMechS)*, pp. 305–310, IEEE, 2019.

[10] S. George, P. Sen, and C. Carta, "Realizing joint communication and sensing rf receiver front-ends: A survey," *IEEE Access*, vol. 12, pp. 9440–9457, 2024.

[11] P. Sen, A. Harutyunyan, M. Umar, and S. Kamal, "Joint communication and radar sensing: RF hardware opportunities and challenges — a circuits and systems perspective," *Sensors*, vol. 23, no. 18, 2023.

[12] J. Gong, L. Zhao, Q. Hao, F. Hu, and X. Hong, "A reconfigurable hardware platform for cognitive sensor networks towards behavioral biometrics," in *SENSORS, 2012 IEEE*, pp. 1–4, 2012.

[13] C. Li, X. Yu, C.-M. Lee, D. Li, L. Ran, and J. Lin, "High-sensitivity software-configurable 5.8-GHz radar sensor receiver chip in 0.13-$\mu$ m CMOS for noncontact vital sign detection," *IEEE Transactions on Microwave Theory and Techniques*, vol. 58, no. 5, pp. 1410–1419, 2010.

[14] H. Wymeersch, D. Shrestha, C. M. De Lima, V. Yajnanarayana, B. Richerzhagen, M. F. Keskin, K. Schindhelm, A. Ramirez, A. Wolfgang, M. F. De Guzman, *et al.*, "Integration of communication and sensing in 6G: A joint industrial and academic perspective," in *2021 IEEE 32nd Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, pp. 1–7, IEEE, 2021.

[15] C. D. Lima et. al., "6g white paper on localization and sensing."

[16] R. B. Yishay and D. Elad, "A compact frequency-tunable VGA for multi-standard 5G transceivers," in *2020 IEEE/MTT-S International Microwave Symposium (IMS)*, pp. 325–328, 2020.

[17] D. Guermandi, Q. Shi, A. Medra, T. Murata, W. Van Thillo, A. Bourdoux, P. Wambacq, and V. Giannini, "19.7 A 79GHz binary phase-modulated continuous-wave radar transceiver with TX-to-RX spillover cancellation in 28nm CMOS," in *2015 IEEE International Solid-State Circuits Conference - (ISSCC) Digest of Technical Papers*, pp. 1–3, 2015.

[18] M. Skolnik, *Introduction to Radar Systems*. Electrical engineering series, McGraw-Hill, 2001.

[19] Y. Cho, W. Lee, H.-c. Park, B. Park, J. H. Lee, J. Kim, J. Lee, S. Kim, J. Park, S. Park, K. H. An, J. Son, and S.-G. Yang, "A 16-element phased-array CMOS transmitter with variable gain controlled linear power amplifier for 5G new radio," in *2019 IEEE Radio Frequency Integrated Circuits Symposium (RFIC)*, pp. 247–250, 2019.

[20] D. Pan, Z. Duan, L. Sun, S. Guo, L. Cheng, and P. Gui, "A 76-81 GHz CMOS PA with 16-dBm PSAT and 30-dB Amplitude Control for MIMO automotive radars," in *ESSCIRC 2019 - IEEE 45th European Solid State Circuits Conference (ESSCIRC)*, pp. 329–332, 2019.

[21] S. George, P. Sen, and C. Carta, "A multi-mode direct conversion receiver for joint communication and radar sensing," in *2024 15th German Microwave Conference (GeMiC)*, pp. 229–232, 2024.

[22] D. Cracan, M. Sanduleanu, and M. A. Gebremicheal, "A 0.7-1.5ghz tunable papoulis all-pole low-pass filter in 22nm cmos fdsoi," in *2021 IEEE International Symposium on Circuits and Systems (ISCAS)*, pp. 1–5, 2021.

[23] Y. Yao, J. Wei, M. Li, S. Ma, F. Ye, and J. Ren, "A 256mhz analog baseband chain with tunable bandwidth and gain for uwb receivers," in *2019 IEEE 13th International Conference on ASIC (ASICON)*, pp. 1–4, 2019.

[24] R. S. Thoma, C. Andrich, G. D. Galdo, M. Dobereiner, M. A. Hein, M. Kaske, G. Schafer, S. Schieler, C. Schneider, A. Schwind, and P. Wendland, "Cooperative passive coherent location: A promising 5g service to support road safety," *IEEE Communications Magazine*, vol. 57, no. 9, pp. 86–92, 2019.

[25] P. Zhang, J. Lu, Y. Wang, and Q. Wang, "Cooperative localization in 5G networks: A survey," *Ict Express*, vol. 3, no. 1, pp. 27–32, 2017.

[26] J. He, H. Wymeersch, T. Sanguanpuak, O. Silvén, and M. Juntti, "Adaptive beamforming design for mmwave ris-aided joint localization and communication," in *2020 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, pp. 1–6, IEEE, 2020.

[27] H. Liu, X. Liu, X. Xie, X. Tong, T. Shi, and K. Li, "Application-oriented privacy filter for mmWave radar," *IEEE Communications Magazine*, 2023.

[28] X. Chen, Z. Feng, J. A. Zhang, Z. Wei, X. Yuan, and P. Zhang, "Sensing-aided uplink channel estimation for joint communication and sensing," *IEEE Wireless Communications Letters*, vol. 12, no. 3, pp. 441–445, 2022.

[29] N. Asmussen, S. Haas, A. Lackorzyński, and M. Roitzsch, "Core-local reasoning and predictable cross-core communication with $M^3$," in *2024 IEEE 30th Real-Time and Embedded Technology and Applications Symposium (RTAS)*, pp. 199–211, IEEE, 2024.

[30] N. Feske and C. Helmuth, "A Nitpicker's guide to a minimal-complexity secure GUI," in *21st Annual Computer Security Applications Conference (ACSAC'05)*, pp. 85–94, Dec. 2005. ISSN: 1063-9527.