PUBLIC SUBMISSION

Received: May 29, 2025
Tracking No. mb9-x3h9-azno
Comments Due: May 28, 2025 **Submission Type:** Web

Docket: NSF-2025-OGC-0001
NITRD_FRDOC_0001

Comment On: NSF-2025-OGC-0001-0001
Request for Information: Development of a 2025 National Artificial Intelligence Research and Development Strategic Plan

Document: NSF-2025-OGC-0001-DRAFT-0273
Comment on FR Doc # 2025-07332

Submitter Information

Government Agency Type: State **Government Agency:** Texas Tech University

General Comment

See attached file(s)

Attachments

TTU RFI response Docket id No NSF-2-25-OGC-001 - AI RD Strategic Plan

Open ISAC to enable dual use parallel innovation for critical infrastructure and national security use cases May 29

CRITICAL INFRASTRUCTURE SECURITY INSTITUTE
TEXAS TECH
Research & Innovation

Texas Tech University Response to Request for Information on the Development of a 2025 National Artificial Intelligence (AI) Research and Development (R&D) Strategic Plan.

Docket ID No. NSF-2025-OGC-0001

Disclaimer: The views expressed in this RFI response are solely those of the content creator and do not necessarily reflect the views of Texas Tech University.

Goal of RFI:

United States can secure its position as the unrivaled world leader in artificial intelligence by performing R&D to accelerate AI-driven innovation, enhance U.S. economic and national security, promote human flourishing, and maintain the United States' dominance in AI while focusing on the Federal government's unique role in AI research and development (R&D) over the next 3 to 5 years.

Texas Tech University Response:

Texas Tech University (TTU) performs AI research with national security relevance e.g., Integrated Sensing and Communications (ISAC) to dome and protect critical infrastructure using private telecommunications networks enhanced with innovative secure Open ISAC processing interfaces. Open ISAC interfaces are critical to enable Artificial Intelligence (AI) sensing R&D for national security interests and critical infrastructure operational efficiencies that are more immediate than normal commercial maturation of the telecommunications Open ISAC feature appears to prioritize. Critical Infrastructure national security context is used to provide a practical understanding of the business case for the ISAC private cellular network as well as the need for parallel innovation to accelerate time to value.

Attached is a paper, “Open Integrated Sensing and Communications Acceleration via Parallel Innovation for Critical Infrastructure and National Security Use Cases” which elaborates on the use of AI R&D for National Security use case acceleration.

Open Integrated Sensing and Communications Acceleration via Parallel Innovation for Critical Infrastructure and National Security Use Cases

Brenda Connor , PhD, CISSP
Department of Electrical and Computer Engineering.
Texas Tech University
Lubbock, Texas
https://orcid.org/0009-0002-9603-0644

Abstract— This applied research seeks to inform and inspire government focus and funding to accelerate the time to value for Integrated Sensing and Communications (ISAC) to dome and protect critical infrastructure using private telecommunications networks enhanced with innovative secure Open ISAC processing interfaces. Open ISAC interfaces are critical to enable Artificial Intelligence (AI) sensing R&D for national security interests and critical infrastructure operational efficiencies that are more immediate than normal commercial maturation of the telecommunications Open ISAC feature appears to prioritize. Critical Infrastructure context is used to provide a practical understanding of the business case for the ISAC private cellular network as well as the need for parallel innovation.

Keywords—ISAC, ISaC, sensing, dome of protection, national security, critical infrastructure

I. INTRODUCTION

Contextual research aims to set a context for the research that includes the commercial value for a specific customer base. The benefit of this approach is the focus on providing holistic value for the context aligned with a business case for adoption which may be broader than motivated by targeted technology alone. This is a prioritization for the research and is not a statement of the lack of value in the other contexts for other stakeholders.

Standardization is important for multivendor interoperability. For the telecommunications Integrated Sensing and Communications (ISAC) technology, 3GPP and O-RAN are the main standards bodies relevant in this research however for Open ISAC processing interfaces, O-RAN is prioritized in this analysis. This paper has been published prior to the standards groups focusing on solving the Open ISAC processing interfaces challenges. In this paper the minimal changes to current state O-RAN architecture is assumed and elaborated. The standards community will decide the final architecture rendering.

Cellular Telecommunications RAN sensing technologies aim at acquiring information about a remote object or environment and its characteristics without contacting it. The perception data of the object and its surroundings can be utilized for analysis, so that meaningful information about the object or environment and its characteristics can be obtained.

This applied research seeks to inform and inspire government focus and funding to accelerate the time to value for Integrated Sensing and Communications (ISAC) to dome and protect critical infrastructure using private telecommunications networks enhanced with innovative secure Open ISAC processing interfaces. Open ISAC interfaces are critical to enable Artificial Intelligence (AI) sensing R&D for national security interests and critical infrastructure operational efficiencies that are more immediate than normal commercial maturation of the telecommunications Open ISAC feature appears to prioritize. Critical Infrastructure context is used to provide a practical understanding of the need for parallel innovation.

Parallel innovation is facilitated by the scope of the Notice of Funding Opportunity (NOFO) grant opportunities available via government funding agencies. The need for parallel innovation to accelerate critical infrastructure value is elaborated via the National Telecommunications and Information Association (NTIA) Public Wireless Supply Chain Innovation Fund (PWSCIF) [1] NOFO example. NOFO scope followed a logical progression as illustrated in Fig. 1:

- NOFO 1: Open front haul testing between the Radio (O-RU) and the Baseband (O-DU),
- NOFO 2: then O-RU product innovation and commercialization in the US, and
- NOFO 3: then vertical industry solutions (including critical infrastructure solutions) enabled by the open service management and orchestrion (SMO) platform RAN Intelligent Controller (RIC).

The result is roughly 5 to 6 years for the time to value for vertical industry solutions (including critical infrastructure solutions). Parallel Innovation enablement refers to the request for NOFO scope to include both RAN innovations and programming interfaces enabling Vertical Industry Solutions with each NOFO.

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.

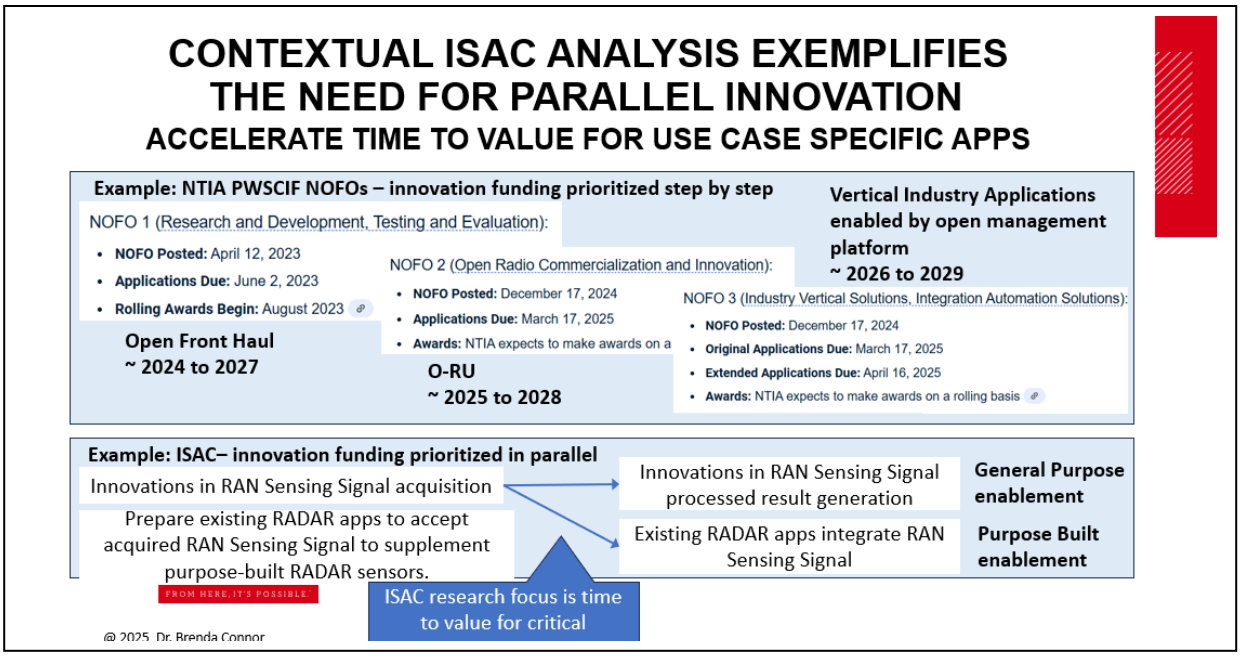

Fig. 1. Example to illustrate need for parallel innovation

Fig. 1 bottom half illustrates the parallel innovation request. Each NOFO scope should include funding for innovation in the RAN sensing signal acquisition (Air to RAN (radio unit and baseband)) and funding for sensing signal interpretation preparation. Fig. 1 lower right shows two sensing signal interpretation paths:

- General Purpose enablement – this path embodies the telecommunications network processing to expose sensing processed results via standard interfaces such as rAPP R1 and or xAPP Y1. See Fig. 6 interface 2.
- Purpose Built enablement – this path embodies the exposure of the sensing data set stream for integration with existing or new AI enabled RADAR applications. See Fig 6 interface 1.

For Critical Infrastructure security use cases, including for national security, Purpose Built enablement is prioritized to take advantage of existing RADAR applications to extend purpose built RADAR reach and to feed new AI enabled use cases. Acceleration of this Open ISAC secure processing area is a research priority.

II. Qualitative need for ISAC Processing Interface Acceleration

Critical Infrastructure Sector's context and emerging ISAC standards are leading considerations for Open ISAC AI enabled national security use cases evaluation.

A. Critical Infrastructure Sector Context

The following Critical Infrastructure Sectors identified by the Cybersecurity & Infrastructure Security Agency (CISA) [2], Energy, Water and Wastewater Systems, and Food and Agriculture Sector, e.g., animals for food production, were analyzed with a focus given to the dual use applicability for critical infrastructure operations including national security and for potential DOD relevance. Example use cases for ISAC included:

- Oil & Gas: ISAC used for object detection and tracking, e.g., vehicle. A report from NewsWest9 Midland, TX in Feb 2024 reported over 30,000 barrels of Oil were stolen from the Permian Basin since Oct 2022 [3]. At $70 to $100 a barrel, detection of unidentified vehicles in an oilfield is valuable and oil is not the only asset being stolen.
- Ranching (animals for food production): ISAC for Pattern of Life analysis e.g. to map livestock normal and abnormal behavior. A threat is Biosecurity Predation. If a predator, e.g., a coyote enters the grazing area of livestock, their behavior changes. The ability to detect normal and abnormal behavior can help reduce herd loss.
- Many other object detection and tracking use cases, e.g. drone detection and pattern of life analysis e.g., to detect animal parturition behavior were considered in selecting these two main patterns of interest in the selected critical infrastructure sectors.

West Texas critical infrastructure context, e.g. oilfield, ranch, was considered in selecting the private cellular network design approach. Any solution must be easy to deploy and modular for deployment in an energy challenged harsh environment which may have spotty public cellular network coverage and scarcity of humans to motivate public telecommunications network

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.

investment. A private cellular telecommunication network with network-based ISAC was selected to defocus policies related to public cellular ISAC use e.g. privacy considerations and to broaden cellular network capability configuration flexibility.

The analysis included consideration for what business case was needed for critical infrastructure operators to motivate adoption of ISAC, a 6th generation cellular telecommunications network feature. Business case motivation required a holistic approach for enabling Critical Infrastructure Security and Operational Efficiency with Private Cellular Telecom Capabilities which is summarized via the following three value streams:

1. Dome Critical Infrastructure – AI enhanced object detection & tracking and pattern of life analysis for protection, safety, and operational efficiency is a high value research area for critical infrastructure operators, for National Security and for DOD.
2. SCADA input/output (AI enabled) automations – Private telecommunications network enables critical infrastructure operators to utilize the telecom network's out-of-band SCADA management capability for operational efficiency.
3. Private Cellular Network has the same capability as a public cellular network enabling communications where public network may be spotty. Critical infrastructure operators leverage off the shelf capability for safety and operational efficiency.

The triple bottom line of ISAC AI enabled value, SCADA input/output automations value, and communications reach in challenged environment provide the business case for deploying ISAC using a private cellular network for critical infrastructure national security benefit. Object detection and tracking, pattern of life analysis, and SCADA IO automation are also of perceived value to the DOD.

B. Standards are Emerging

Standardization is important for multivendor interoperability. In the telecommunications space, 3GPP and O-RAN are the main standards bodies for network based telecommunications ISAC. This paper has been published prior to the standards groups prioritizing the Open ISAC programming interfaces. This paper assumes the minimal changes to current state O-RAN architecture; the standards community will decide the final architecture rendering.

In Fig. 2, where is the sensing signal processing input source e.g., at the DU, at the CU, at both, at neither? Is the existing O1 interface extended or is a new interface needed? The control loop timing [4], shown on the left of Fig 2 and the needs of the critical infrastructure use case for the decision loop is a driver for where the processing input source is needed e.g., from DU, from CU, or from SMO. Namely, if the critical infrastructure use case needs the information for its processing as follows:

- > 1 s –the sensing signal may be provided by the SMO (non-real time RIC).
- >10 ms to 1 sec – the sensing signal may be provided by the CU or near-RT RIC.
- ~10 ms – the sensing signal may be provided by the DU.
- <10 ms – Purpose built radar sensor may be required.

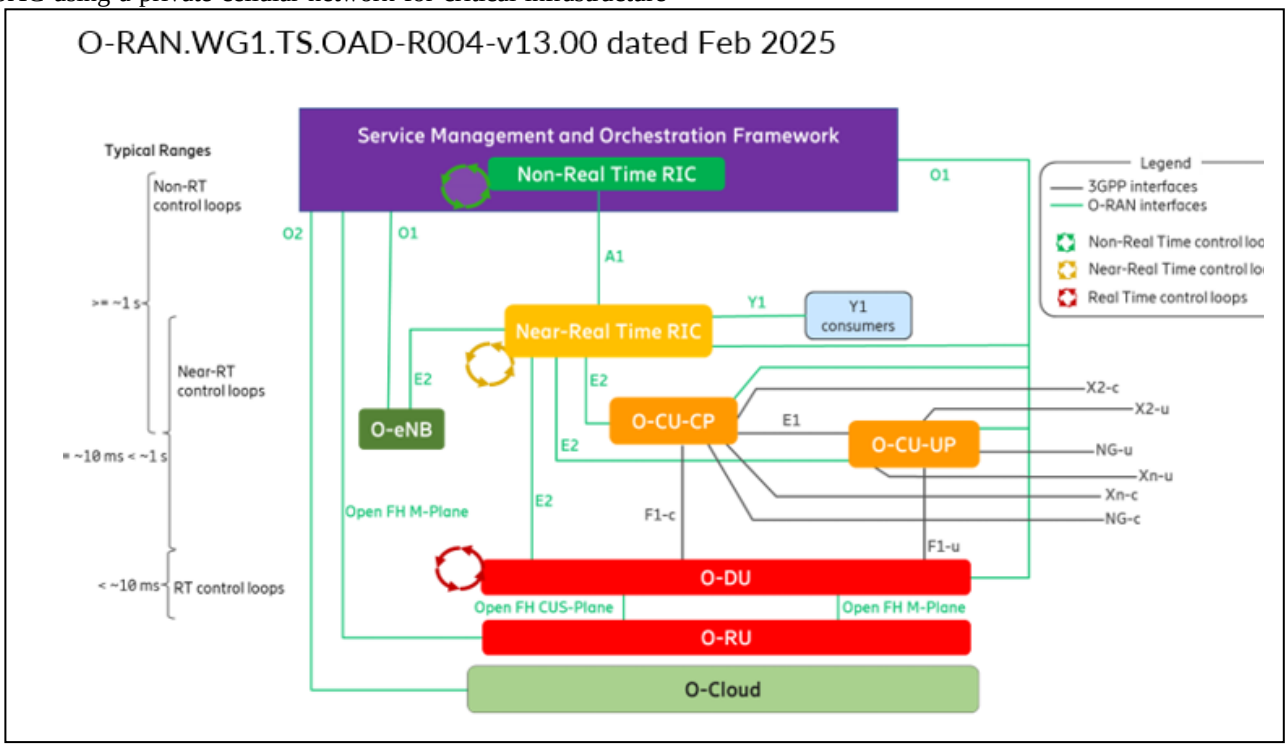

Fig. 2. Example sensing signal processing topic to standardize

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.

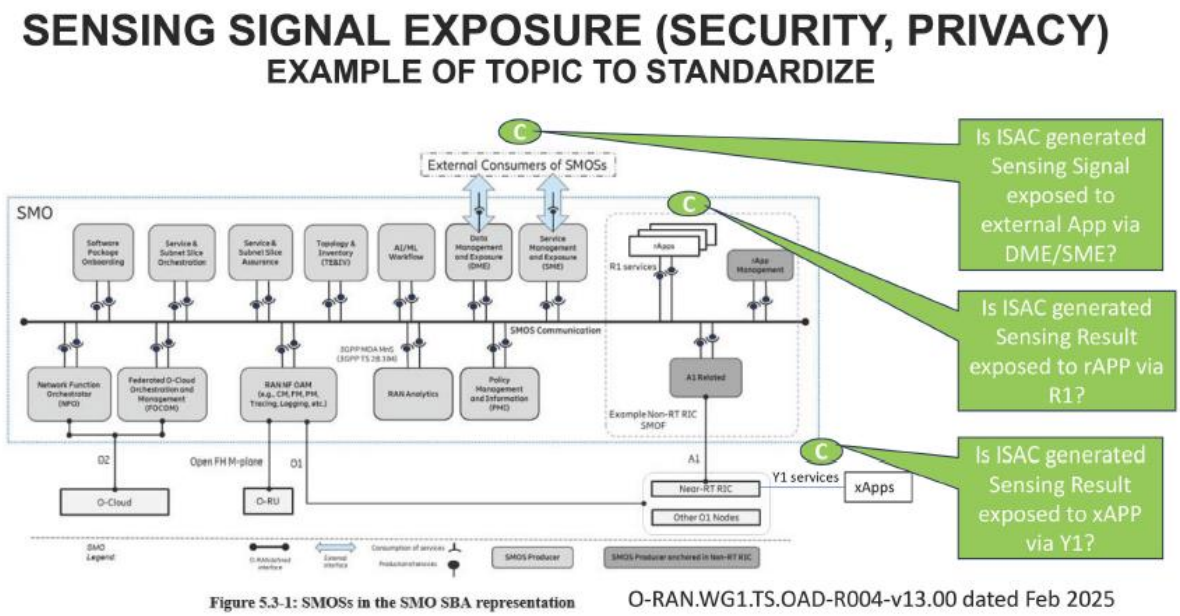

Fig. 3. Illustrative example of considerations for standardization committees

In addition to the critical infrastructures need for the sensing signal decision loop timing, there are other factors involved with sensing signal source selection such as the sensing topology.

For example, the traditional radar topology is monostatic meaning the same node has both the transmitter and the receiver while the ISAC signal may use monostatic sensing topology, bistatic sensing topology or multistatic sensing topology[5]. Bistatic and multistatic sensing topology means that the transmitter and the receiver are on different nodes which requires a fusion function with tighter time and frequency synchronization than may be need for cellular communications thus over-the air RAN node synchronization is preferred.

III. Open ISAC Processing Interfaces for Private Cellular Telecommunications

To further elaborate on Open ISAC processing interfaces for private cellular telecommunications networks, a model for Open ISAC interfaces, an interface to accelerate AI innovation, an ecosystem incubator for Open ISAC processing is elaborated.

A. Model for Open ISAC processing interfaces

The model for Open ISAC processing interface includes consideration for the existing exposure interfaces, the sensing data stream metadata descriptors, and the ability to use existing RAN architecture.

Sensing signal exposure [4] for Open ISAC processing must support security and privacy considerations, Fig. 3. The O-RAN exposure interfaces include:

- Y1 interface from near real time (RT)- RAN Intelligent Controller (RIC)
- R1 interface from non-real time RIC
- External Consumers: Data Management and Exposure (DME)/ Service Management and Exposure (SME) interface

Security and privacy designed specifically for Sensing Signal stream is critical to ensuring the fidelity and trustworthiness of Sensing Signal-processed results, including the impact of data fusion from multi-static nodes.

Metadata standardization is necessary to effectively and efficiently identify characteristics of Sensing Signal stream to allow for multi-vendor interoperability and application digestibility. Sensing Signal stream metadata will require unique, comprehensive security and privacy architectures associated with the sensing data stream e.g., information flow.

In this analysis, the “Integrated” in Integrated Sensing and Communications (ISAC) assumes the same RAN HW is used for both telecommunications and sensing purposes enabling the sharing of 5G New Radio (NR) Stand-alone (SA) hardware, spectrum, and sites [5]. Fig. 4 “Reuse of the waveform” e.g., orthogonal frequency division multiplexing (OFDM) would require changes to the RAN by the RAN vendor to accomplish thus “reuse of the waveform” is not considered in this analysis; “reuse of waveform” is a 6th generation cellular topic.

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.

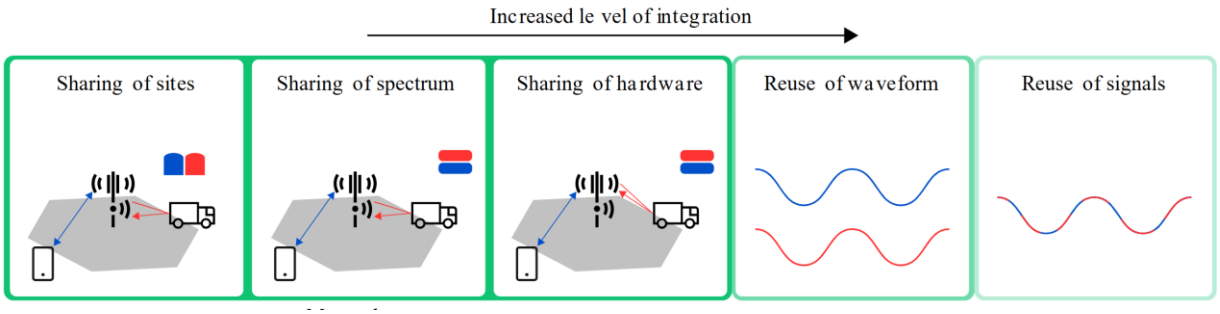

Fig. 4. Level of ISAC integration [5]

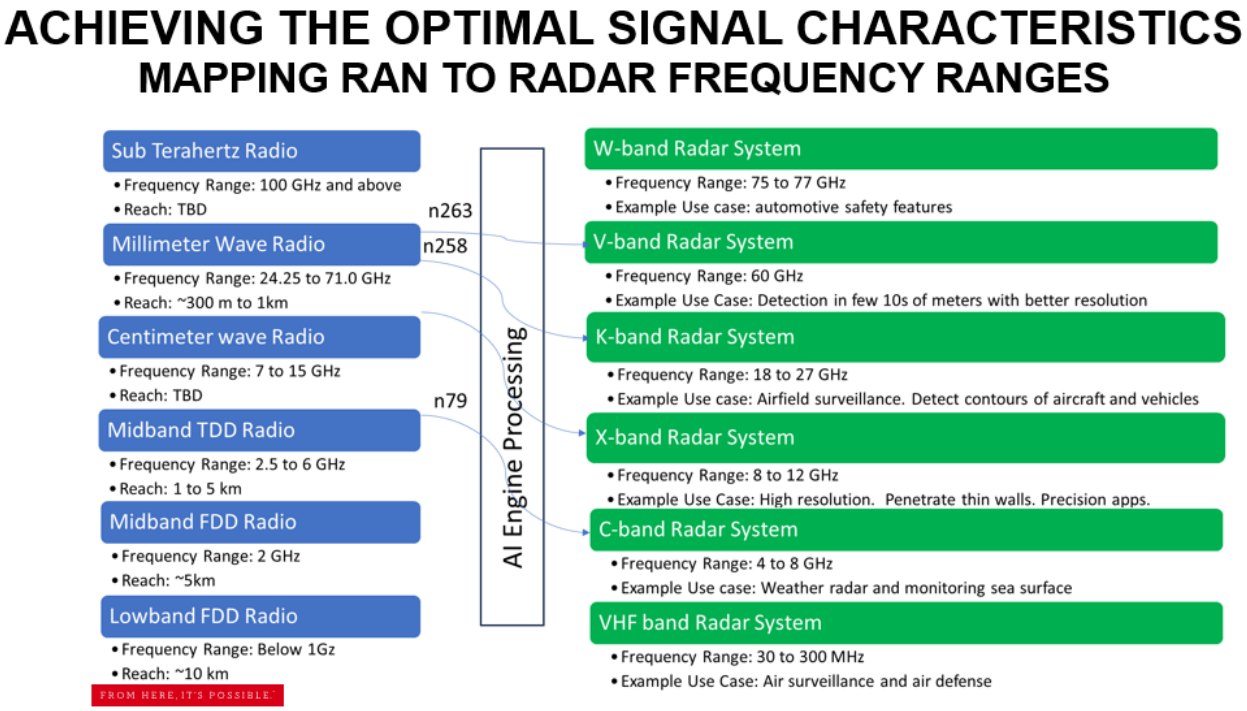

Fig. 5. Mapping 3GPP frequency ranges to IEEE RADAR frequency ranges

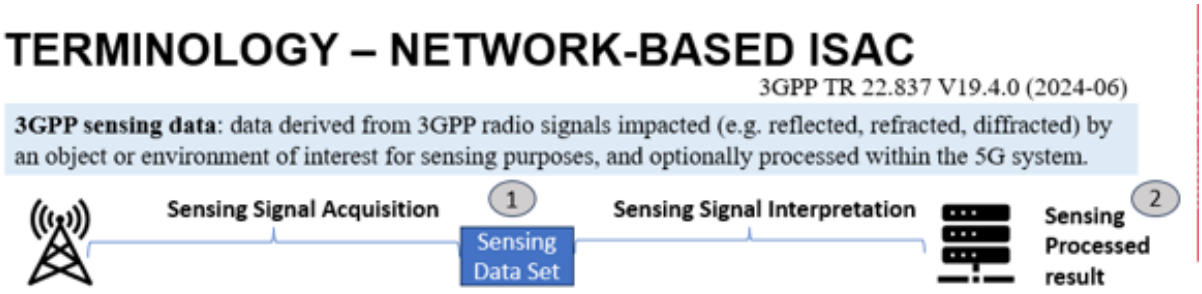

Fig. 6. Open ISAC Interfaces to enable Parallel Innovation

However, "reuse of signals" implies one can use the same signal that is transmitted and received for communications to sample for sensing. "Reuse of signal" for sensing works if the communications signal has the correct properties for the intended use case. If standard 3GPP NR 5G SA HW can be used for private network ISAC with shared HW and "reuse of signal" then the deployment of ISAC may be feasible via a SW upgrade.

Fig. 5 illustrates the relationship between the cellular frequency ranges defined by 3GPP and the RADAR frequency ranges defined by Institute of Electrical and Electronic

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.

Engineers (IEEE). An AI Engine Processing node is shown in the center to illustrate the potential for an Open ISAC processing interface to input sensing data set stream into an AI engine for enhancement.

To enable the "3GPP sensing data" [6] included in Fig. 6 to be "optionally processed in the 5G system", Open ISAC interfaces for sensing signal interpretation must be defined which also implies standardizing the Sensing Data Set shown as a component of interface 1 in Fig. 6. Interface 2 would likely be standardized as an O-RAN interface for an rAPP R1 and/or an xAPP Y1. Interface 1 is needed asap for parallel innovation by independent entities and to accelerate the time to value for critical infrastructure use cases. The Sensing Data Set stream will feed the AI model and algorithms to achieve the sensing signal interpretation necessary for the critical infrastructure object detection and tracking and the pattern of life analysis use cases. The sensing data set must be standardized in the Open ISAC interface 1 standardization.

B. AI as the Engine for Replication to Adjacent Context Use

Architectural considerations for ISAC AI enablement standardization include:

- the presence of distributed and independent AI engines in a telecommunications network e.g., in the RAN, in the fusion layer, in the sensing signal processing path,
- interfaces designed for multivendor scalability, security, and privacy and
- Sensing Signal data set streams are information flow entities with metadata descriptors.

The requirements on the sensing signal processing highlight the need to also have metadata to describe the sensing dataset stream such as, sensing data set stream's decision loop granularity, sensing topology used, sensing signal acquisition frequency, sensing signal acquisition bandwidth.

Security capabilities such as authentication and authorization are typically associated with a node. With Sensing Signal data streams, authentication and authorization must be attached to the sensing data set stream e.g., who is allowed to access the stream. Thus, authentication and authorization attributes are also metadata. In addition, supply chain security attributes such as vendor of node may be relevant to track injection threats in AI models.

Multivendor environment is assumed and thus interface standards that include metadata is prioritized in addition to the sensing data set.

As indicated in Fig. 1, AI may be able to extend the applicability of the acquired sensing signal to adjacent RADAR use cases by incorporating other information into the AI Model and algorithms.

The reuse potential for AI is tremendous. For example, a pattern of life AI model developed using livestock may be reusable to other pattern of life use cases. By leveraging pre-trained and customizable AI models and algorithms developed for critical infrastructure national security purpose, DOD may be able to import and enhance AI models and algorithms with DOD unique development and deployment needs to streamline time to value for national security and national defense.

One potential future includes an AI-Enabled application using metadata to request a sensing data stream via the Open ISAC processing interface. Under the hood, the Open ISAC interface would use the metadata to identify an existing ISAC data stream with suitable characteristics and, if no existing sensing data stream was available, an appropriate sensing data stream would be created on-demand assuming the AI-enabled application was authorized and able to authenticate to obtain access to the sensing data stream.

C. Open ISAC Ecosystem Incubator to facillitate partnership with Industry, Academia and National Security entities.

Standardization of secure open interfaces is needed for commercialization and interoperability. However, national security needs capability in a timeframe that is relevant, and that timeline is driven by external threat actors. Therefore, an ISAC technology evaluation environment to incubate and mature the ecosystem in many areas in parallel is needed. The lessons learned in the ISAC ecosystem incubator must enable researchers to actively contribute relevant finding into standardizations efforts. The motivation for private entities to prioritize Fig 6, interface 1 is lacking and thus investment from government is needed. A private cellular 5G NR SA Telecommunications ecosystem incubator protecting critical infrastructure in harsh energy challenged environments is an ideal proving ground for critical infrastructure holistic value that includes the business case considerations required to motivate critical infrastructure operator deployment. Open ISAC ecosystem incubators are important to test the limits and feasibility of ISAC technologies in real world environments.

IV. Conclusion

By using Critical Infrastructure sector context to provide a practical understanding of the business case for ISAC deployment, prioritizing a private cellular telecommunications network and network based ISAC was discussed. In addition, the need for parallel innovation was presented including Open ISAC processing interfaces with metadata descriptors as critical to enable Artificial Intelligence (AI) sensing R&D for national security interests and critical infrastructure operational efficiencies that are more immediate than normal commercial maturation of the telecommunications Open ISAC feature appears to prioritize.

This applied research seeks to inform and inspire government focus and funding to accelerate the time to value for Integrated Sensing and Communications (ISAC) to dome and protect critical infrastructure using private telecommunications networks enhanced with innovative secure AI enabled Open ISAC processing interfaces. The use cases discussed for object detection and tracking and pattern of life analysis are perceived to be of dual use value for DOD. The benefit of focusing dual use on critical infrastructure first is to leverage the breadth of academic and commercial entities to accelerate the protection of critical infrastructure for national security.

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.

ACKNOWLEDGMENT

Many thanks to Texas Tech University Critical Infrastructure Security Institute for inspiration and for the Critical Infrastructure Telecom Ecosystem Incubator support.

REFERENCES

[1] National Telecommunications and Infromation Association, "Public Wireless Supply Chain Innovation Fund". [Online] https://www.ntia.gov/funding-programs/public-wireless-supply-chain-innovation-fund

[2] America's Cyber Defense Agency, "Critical Infrastructure Sectors". [Online]. Available https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors.

[3] T. Dupnik, "Oilfield theft continues to impact producers in the Permian Basin". [Online]. Available https://www.newswest9.com/article/news/local/oilfield-theft-continues-to-impact-producers-in-the-permian-basin/513-7244c048-3070-4d0a-9f69-78a5b7b26057#:~:text=Thieves%20are%20getting%20onto%20oil,stealing%20more%20than%20just%20oil.&text=ECTOR%20COUNTY%2C%20Texas%20%E2%80%94%2030%2C000%20barrels,to%20a%20representative%20from%20ConocoPhillips.

[4] O-RAN Alliance. O-RAN Work Group 1 (Use Cases and Overall Architecture) O-RAN Architecture Description. O-RAN.WG1.TS.OAD-R004-v13.00, [Online]. Available: https://specifications.o-ran.org/download?id=789

[5] R. Baldemair, "Integrated Sensing and Communications". [Online]. Available: https://www.ericsson.com/en/blog/2024/6/integrated-sensing-and-communication

[6] 3GPP, Feasibillity Study on Integrated Sensing and Communication (Release 19). TR 22.837 V19.4.0 (2024-06). [Online]. Available https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=4044

© 2025 Brenda Ann Connor, PhD, CISSP. Texas Tech University. All rights reserved.