

ISAC Overview and UK Position

An overview of ISAC, the UK position and its use in counter-drone technologies.

Dr Daniel Burt

Introductions

Plexal is the innovation and growth company helping to strengthen the UK's technology capabilities through collaboration. With teams in London, Manchester and Cheltenham, we work closely with government, industry, startups and academia to drive economic growth and reinforce national security.

Plexal delivers four core services: creating workspaces for innovators, running innovation programmes and consultancy, building regional tech clusters and helping SMEs scale strategically.

By closing the gap between early-stage and established organisations – across the public and private sectors at home and abroad – we've impacted over 1,200 businesses, added £731m to the UK economy and helped create 9,400 jobs

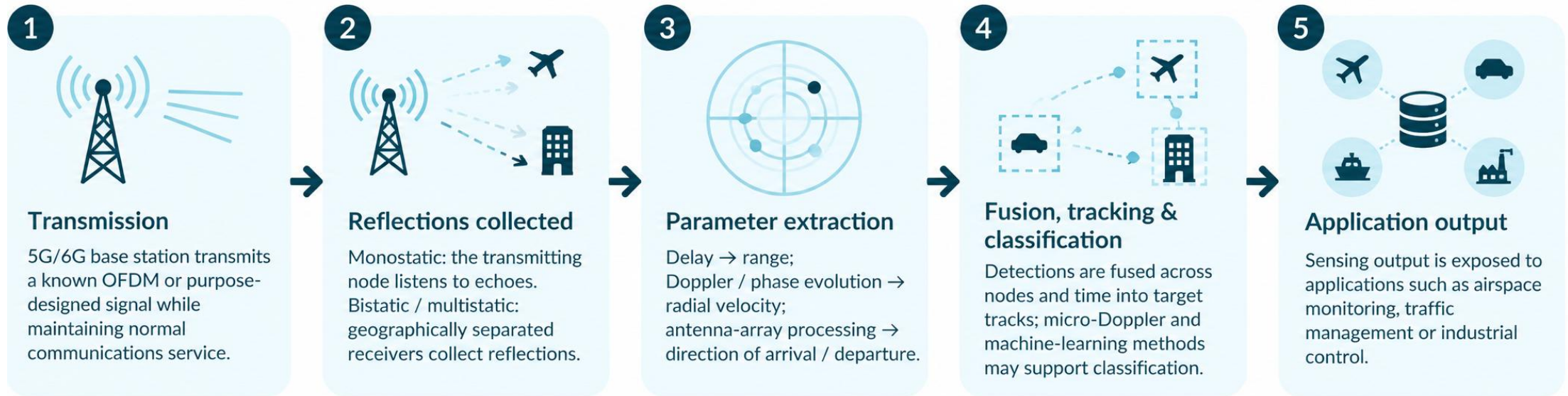


Integrated Sensing and Communication (ISAC)

?

Integrated Sensing and Communication (ISAC) is a design paradigm in which radio infrastructure, spectrum, hardware and, at the deeper levels of integration, the same transmitted waveforms are used **both to exchange data and to sense the physical environment**.

Overview of Operation and Applications



Autonomous Vehicles



Drones



Smart Cities



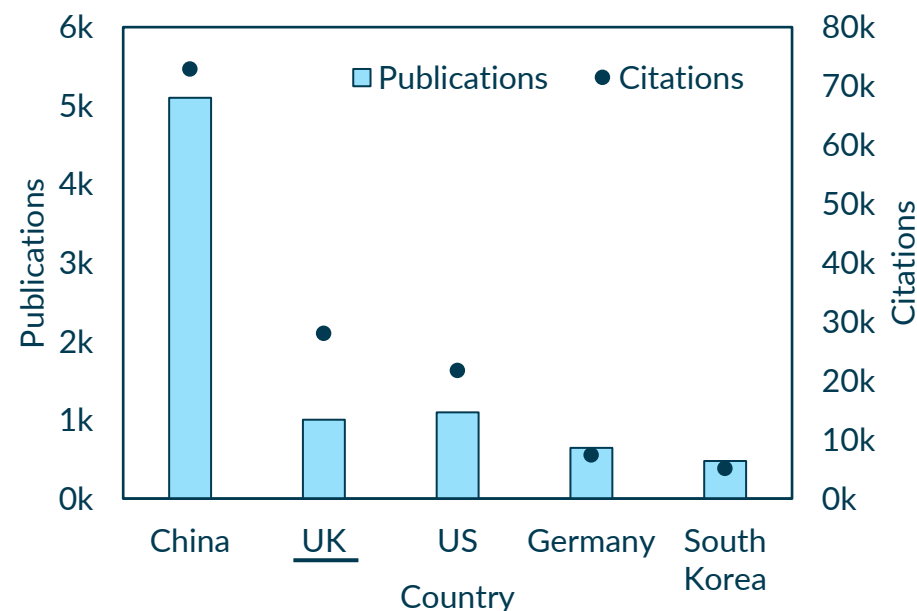
Smart Factories



Healthcare

UK ISAC Research Capability

The UK is a **world leader for ISAC research** in terms of both conference and journal publication number and citations, ranking 3rd and 2nd globally and respectively. There are numerous world-class research institutions with some highlighted below.



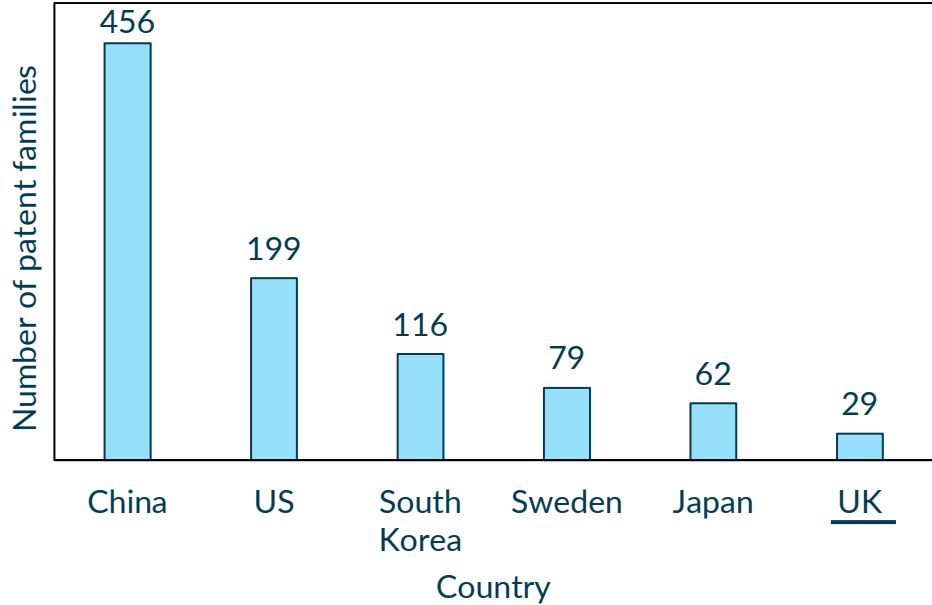
The number of ISAC journal and conference publications and citations between 2021 and 2026 for the top countries (Source: SCOPUS)

Organisation	Description
University College London (UCL)	Institute of Communications and Connected Systems (ICCS) has a long legacy and the most publications.
Queen Mary University London	Centre for Wireless Innovation (CWI) has the second highest number of publications.
Queen’s University Belfast	2026 project on Resilient Distributed Integrated Sensing and Communication Networks
University of Surrey	Institute for Communication Systems / 6GIC is the fourth biggest publisher in this space.
University of Southampton	Long-standing JRC activity. Fifth highest number of publications.

Huge range of other organisations: Innovate UK, dstl, NPL. Imperial College London, University of Glasgow, University of Bristol, University of Manchester, University of Sussex, University of Edinburgh, Kings College London, University of Huddersfield, Herriot-Watt University.

UK ISAC Commercial Capability

The UK has a **limited ISAC intellectual property** footprint, with far fewer patents than leading countries, suggesting challenges in translating research excellence into commercial outcomes. Few UK companies are emerging in this space, though this likely reflects ISAC’s early stage.



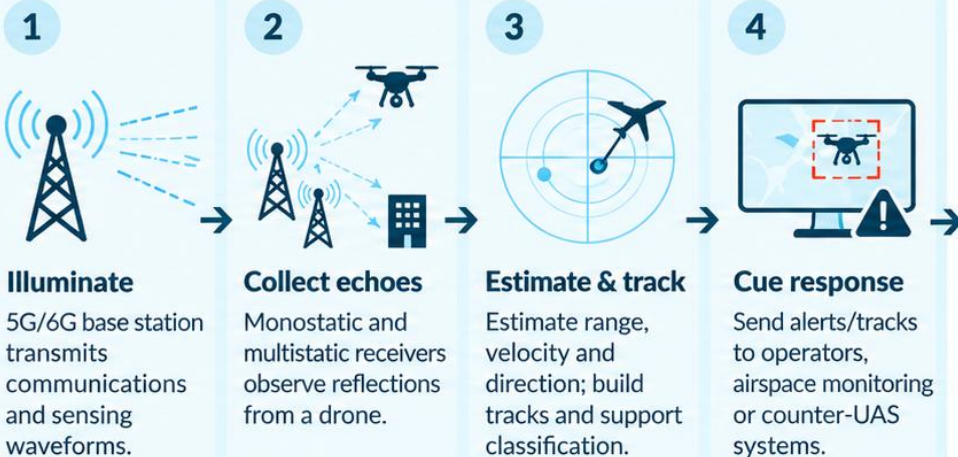
The number of ISAC patents between 2021 and 2026 for the top countries
(Source: Espacenet)

Organisation	Description
Ericsson UK	Works with various academic and industrial partner. Has demonstrated cellular UAV sensing.
Keysight	Named UK supporting organisation in ETSI's ISAC use-case work.
Samsung Electronics	UK partner in ISAC-NEWTON and named participant/supporter in ETSI ISAC work on use cases.
Rohde & Schwarz UK	ISAC lab test platform.

ISAC for Counter Drone Applications

ISAC offers a promising additional layer for counter-drone detection and tracking by leveraging existing mobile infrastructure, but its technical limitations and maturity mean it must be integrated with radar, RF, acoustic and EO/IR sensors to deliver robust, layered protection.

1 How ISAC is used



2 Advantages and drawbacks

Advantages

- Uses existing sites, arrays and backhaul
- Can detect non-cooperative or radio-silent drones
- Multistatic geometry can improve localisation
- Complements night or low-light sensing

Drawbacks

- Small, low-altitude drones and clutter remain hard
- Sensing competes with communications resources
- Geometry, bandwidth and self-interference limit performance
- Classification maturity, privacy and security issues remain

3 Layered counter-drone approach required



Memory Vulnerability in Modern Connectivity

A brief overview of memory-vulnerability in modern connectivity and implications for 6G.

Dr Daniel Burt

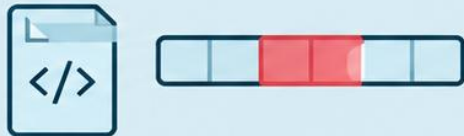


Memory vulnerabilities in advanced connectivity

As 5G and 6G networks become increasingly software-defined, distributed and interconnected, memory vulnerabilities present a growing cybersecurity risk, potentially enabling malicious code execution, data breaches and disruption to critical connectivity services.

1 Memory vulnerabilities

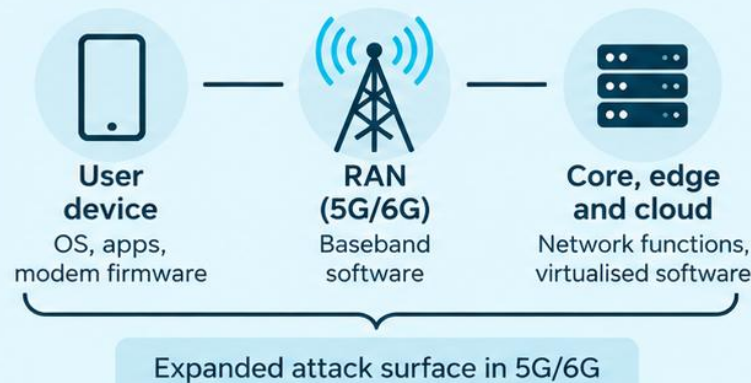
Memory vulnerabilities occur when software does not properly check memory access, allowing malicious actors to read, modify or execute data they should not. This can bypass intended security controls.



e.g. buffer overflow
or use-after-free

2 In modern connectivity and 6G

These vulnerabilities can exist across the connectivity stack – from device firmware and baseband software to network functions in 5G/6G cores, edge and cloud.



3 Potential impact

Exploiting memory vulnerabilities can allow attackers to run malicious code, steal or modify data, disrupt network services or gain persistent access, affecting users, network operators and critical services.



Execute malicious code
(e.g. remote access)



Access or modify sensitive data



Disrupt services and
network availability

CHERI

CHERI addresses a major class of memory vulnerabilities through hardware-enforced memory protection, offering a promising foundation for more secure, resilient and trustworthy 5G/6G infrastructure. We are working with DCMS, PA Consulting and BT to accelerate the adoption of CHERI in advanced connectivity.

1 How CHERI works

CHERI adds hardware-enforced capabilities to pointers, so memory accesses are checked automatically and constrained to authorised memory regions.



Bounds checking



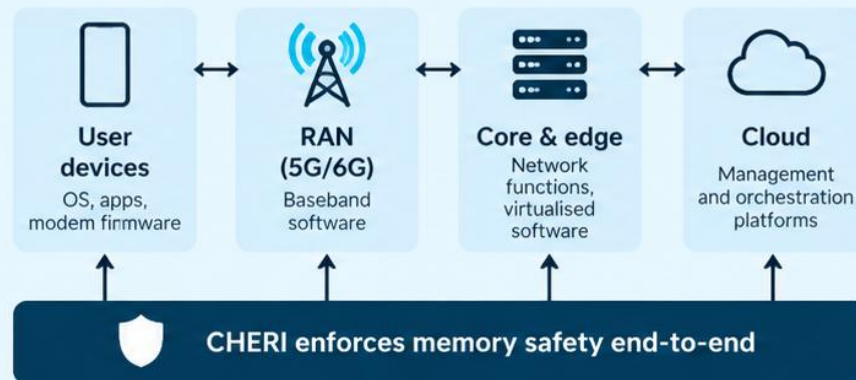
Access permissions



Capability tags

2 Protects the connectivity and 6G stack

Prevents memory-based attacks across layers of the connectivity stack – from device firmware and baseband software to network functions in 5G/6G cores, edge and cloud.



3 Key benefits and impact



Blocks memory-based exploits

Prevents attackers from reading, modifying or executing unauthorised memory, stopping common attack vectors (e.g. buffer overflows, use-after-free).



More resilient connectivity and 6G

Helps secure devices, base stations and network functions, reducing the risk of remote code execution, data theft and service disruption.



Enables safer innovation

Provides a stronger foundation for 6G and future services by reducing a major class of software vulnerabilities.

Thank you